

**ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM
2223 E. WELLINGTON AVENUE, SUITE 100
SANTA ANA, CALIFORNIA**

**AUDIT COMMITTEE MEETING
TUESDAY, FEBRUARY 11, 2025
9:00 A.M.**

Members of the Committee

Adele Lopez Tagaloa, Chair
Shari Freidenrich, Vice Chair
Charles Packard, Member
Iriss Barriga, Member

Members of the public who wish to observe and/or participate in the meeting may do so (1) from the OCERS Boardroom or (2) via the Zoom app or telephone (information below) from any location.

OCERS Zoom Video/Teleconference information	
<p>Join Using Zoom App (Video & Audio)</p> <p>Join Zoom Meeting https://ocers.zoom.us/j/83406721126</p> <p>Meeting ID: 834 0672 1126 Passcode: 512283</p> <p>Go to https://www.zoom.us/download to download Zoom app before meeting Go to https://zoom.us to connect online using any browser.</p>	<p>Join by Telephone (Audio Only)</p> <p>Dial by your location</p> <p>+1 669 900 6833 US (San Jose) +1 253 215 8782 US (Tacoma) +1 346 248 7799 US (Houston) +1 929 436 2866 US (New York) +1 301 715 8592 US (Germantown) +1 312 626 6799 US (Chicago)</p> <p>Meeting ID: 834 0672 1126 Passcode: 512283</p>
<p>A Zoom Meeting Participant Guide is available on OCERS' website Board & Committee Meetings page</p>	

AGENDA

This agenda contains a brief general description of each item to be considered. The Committee may take action on any item included in the agenda; however, except as otherwise provided by law, no action shall be taken on any item not appearing on the agenda. The Committee may consider matters included on the agenda in any order, and not necessarily in the order listed.

OPEN SESSION

1. CALL MEETING TO ORDER AND ROLL CALL
2. BOARD MEMBER STATEMENT REGARDING PARTICIPATION VIA ZOOM (IF NECESSARY)
(Government Code section 54953(f))
3. PUBLIC COMMENTS

Members of the public who wish to provide comment during the meeting may do so by “raising your hand” in the Zoom app, or if joining by telephone, by pressing * 9 on your telephone keypad. Members of the public who participate in the meeting from the OCERS Boardroom and who wish to provide

comment during the meeting may do so from the podium located in the OCERS Boardroom. When addressing the Committee, please state your name for the record prior to providing your comments. Speakers will be limited to three (3) minutes.

At this time, members of the public may comment on (1) matters not included on the agenda, provided that the matter is within the subject matter jurisdiction of the Committee; and (2) any matter appearing on the Consent Agenda.

In addition, public comment on matters listed on this agenda will be taken at the time the item is addressed.

CONSENT AGENDA

C-1 AUDIT COMMITTEE MEETING MINUTES

Audit Committee Meeting Minutes

December 12, 2024

Recommendation: Approve the minutes.

ACTION ITEMS

NOTE: Public comment on matters listed in this agenda will be taken at the time the item is addressed, prior to the Committee’s discussion of the item. **Members of the public who wish to provide comment in connection with any matter listed in this agenda may do so by “raising your hand” in the Zoom app, or if joining by telephone, by pressing * 9, at the time the item is called. Persons attending the meeting in person and wishing to provide comment on a matter listed on the agenda should fill out a speaker card located at the back of the Boardroom and deposit it in the Recording Secretary’s box located near the back counter.**

A-1 INDIVIDUAL ACTION ON ANY ITEM TRAILED FROM THE CONSENT AGENDA

A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

Introduction by Philip Lam, Director of Internal Audit

Presentations by Chris Kalafatis, CPA, Baker Tilly; Mike Del Giudice, Principal, Crowe LLP; and Alfred Ko, Risk Consultant, RSM.

Recommendation: Staff recommends awarding the contract (subject to satisfactory negotiation of terms) to perform co-sourced IT audits, to one of the three finalists, based on the firm’s presentation, responsiveness to the Audit Committee’s questions, and the written proposal submitted.

A-3 CONSIDERATION OF 2025 RISK ASSESSMENT AND AUDIT PLAN

Presentation by Philip Lam, Director of Internal Audit, and Mark Adviento, Senior Internal Auditor

Recommendation: Approve the 2025 Risk Assessment and Audit Plan.

WRITTEN REPORTS

The following are written reports that will not be discussed unless a member of the Committee requests discussion.

R-1 REPORTING OF INTERNAL AUDIT KEY PERFORMANCE INDICATORS

Written Report

R-2 MANAGEMENT ACTION PLAN VERIFICATION REPORT

Written Report

R-3 AUDIT COMMITTEE REVIEW OF ACTIVITIES

Written Report

COMMITTEE MEMBER COMMENTS

CHIEF EXECUTIVE OFFICER/STAFF COMMENTS

COUNSEL COMMENTS

ADJOURNMENT

NOTICE OF NEXT MEETINGS

**DISABILITY COMMITTEE MEETING
FEBRUARY 19, 2025
8:30 A.M.**

**ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM
2223 E. WELLINGTON AVENUE, SUITE 100
SANTA ANA, CA 92701**

**REGULAR BOARD MEETING
FEBRUARY 19, 2025
9:30 A.M.**

**ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM
2223 E. WELLINGTON AVENUE, SUITE 100
SANTA ANA, CA 92701**

AVAILABILITY OF AGENDA MATERIALS - Documents and other materials that are non-exempt public records distributed to all or a majority of the members of the OCERS Board or Committee of the Board in connection with a matter subject to discussion or consideration at an open meeting of the Board or Committee of the Board are available at the OCERS' website: <https://www.ocers.org/board-committee-meetings>. If such materials are distributed to members of the Board or Committee of the Board less than 72 hours prior to the meeting, they will be made available on the OCERS' website at the same time as they are distributed

Orange County Employees Retirement System
February 11, 2025
Audit Committee Meeting

Page 4

to the Board or Committee members. Non-exempt materials distributed during an open meeting of the Board or Committee of the Board will be made available on the OCERS' website as soon as practicable and will be available promptly upon request.

It is OCERS' intention to comply with the Americans with Disabilities Act ("ADA") in all respects. If, as an attendee or participant at this meeting, you will need any special assistance beyond that normally provided, OCERS will attempt to accommodate your needs in a reasonable manner. Please contact OCERS via email at adminsupport@ocers.org or call 714-558-6200 as soon as possible prior to the meeting to tell us about your needs and to determine if accommodation is feasible. We would appreciate at least 48 hours' notice, if possible. Please also advise us if you plan to attend meetings on a regular basis.

**ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM
2223 E. WELLINGTON AVENUE, SUITE 100
SANTA ANA, CALIFORNIA**

**AUDIT COMMITTEE MEETING
THURSDAY, DECEMBER 12, 2024
9:30 A.M.**

MINUTES

OPEN SESSION

Chair Packard called the meeting to order at 9:35 a.m.

Recording Secretary administered the Roll Call attendance.

Attendance was as follows:

Present: Charles Packard, Chair; Adele Lopez Tagaloa, Vice Chair; Chris Prevatt; Board Member; Shari Freidenrich, Ex-Officio Member

Also Present: Steve Delaney, Chief Executive Officer (via Zoom); David Kim, Assistant CEO of External Operations, Brenda Shott, Assistant CEO of Internal Operations; Manuel Serpa, General Counsel; Philip Lam, Director of Internal Audit, Cynthia Hockless, Director of Human Resources; Kwame Addo, Chief Compliance Officer; Mark Adviento, Senior Internal Auditor; Jenny Davey, Internal Auditor; Esther Hong, Internal Auditor; Anthony Beltran, Audio Visual Technician; Marielle Horst, Recording Secretary.

PUBLIC COMMENT

None.

CONSENT AGENDA

C-1 APPROVE AUDIT COMMITTEE MEETING MINUTES

Audit Committee Meeting Minutes

October 9, 2024

C-2 INTERNAL AUDITOR'S INDEPENDENCE AND ETHICS STATEMENT

Recommendation: Receive and File.

MOTION by Mr. Prevatt, **seconded** by Ms. Lopez Tagaloa, to approve the Consent Items.

The motion passed **unanimously**.

Orange County Employees Retirement System
December 12, 2024
Audit Committee Meeting

ACTION ITEMS

A-1 INDIVIDUAL ACTION ON ANY ITEM TRAILED FROM THE CONSENT AGENDA

None.

A-2 CONTINUOUS AUDIT OF FINAL AVERAGE SALARY CALCULATIONS (Q3 2024)

Presentation by Philip Lam, Director of Internal Audit, and Mark Adviento, Senior Internal Auditor

Recommendation: Receive and File.

Mr. Lam presented the report noting there was one observation:

In the test sample where six FAS calculation Excel files did not have formal evidence of a secondary QA (Quality Assurance) review performed by staff. After the discussion of the implementation of changes and timeline, the Committee Members were comfortable with the Management Action Plan.

MOTION by Ms. Freidenrich, **seconded** by Ms. Lopez Tagaloa, to receive and file.

The motion passed **unanimously**.

A-3 AUDIT REPORT - OCERS EMPLOYER AUDIT

Presentation by Philip Lam, Director of Internal Audit, and Mark Adviento, Senior Internal Auditor

Recommendation: Receive and File.

Mr. Lam presented the report noting the following two observations:

The first observation was the Personnel Action Notice (PAN) form was not completed to document the employee's return to their original position after a temporary promotion ended. The Committee questioned if there are policies and procedures in place, and if there is someone actively checking the reports to prevent extra help and temporary employees from working extra hours. Ms. Hockless confirmed that they receive monthly reports from the County.

The second observation was that the OCERS Direct Employee Handbook lacks a section detailing the premium pay items available to OCERS Direct employees. Mr. Serpa noted that the OCERS Direct Handbook is currently being revised, and the changes will be incorporated in 2025. The Audit Committee directed staff to bring the OCERS Direct Employee Handbook as an Information Item to the Personnel and Audit Committees.

MOTION by Ms. Freidenrich, **seconded** by Mr. Prevatt, to receive and file.

The motion passed **unanimously**.

Orange County Employees Retirement System
December 12, 2024
Audit Committee Meeting

A-4 AUDIT REPORT - ORANGE COUNTY HEALTH CARE AGENCY EMPLOYER AUDIT

Presentation by Philip Lam, Director of Internal Audit, and Mark Adviento, Senior Internal Auditor

Recommendation: Receive and File.

Mr. Adviento presented the findings of the Audit Report to the Committee, noting the following five observations:

The first observation was the Retroactive pay reported for two employees was incorrect.

The second observation was the Internal Audit identified 125 HCA members with an incorrect status in the OCERS Pension Administration System (PAS).

Ms. Freidenrich asked if this reconciliation includes the entire headcount. Mr. Adviento noted, that yes, this was inclusive of the entire headcount and produced a 5% error rate. During each audit, it is standard practice to reconcile the agency's members with OCERS PAS.

The third observation was the HCA HR does not use Extra Help Position Request Forms for contract Extra Help employees, as it consistently does with non-contract Extra Help employees.

The fourth observation was for 5 of the 10 Extra Help employees sampled, the total hours reported by approved timecards did not match the total hours reported on the HCA Extra Help Employees Hours Worked report.

Mr. Prevatt commented the fourth observation should have been categorized as a "Priority" rather than "Important". Mr. Adviento noted in the 2-year sample reports they did not find employees having exceeded 1600 hours which would make them an employee, therefore the risk level was labeled as "Important".

Ms. Lopez Tagaloa questioned if OCERS asks the employer to hire or release the employee once they reach 1600 hours. Mr. Adviento confirmed we do not.

Mr. Packard questioned whether an extra help employee exceeds 1600 hours in the first year, does the employer have to pay OCERS for that first year? Is this a loophole where we are not receiving all the pensions we should be receiving? Mr. Delaney responded that there was an unintentional loophole. However, OCERS is working with the employers on a policy change, which will be brought to the Board.

Ms. Freidenrich questioned if there was any employee who violated the policies in this audit. Mr. Adviento confirmed there were no violations found.

The fifth observation was the Extra Help Employees Hours Worked reports HCA uses for monitoring hours worked by Extra Help does not report hours worked by staff who have been hired as regular employees or were separated.

Orange County Employees Retirement System
December 12, 2024
Audit Committee Meeting

Mr. Prevatt expressed concern that the Audit report was not forwarded to the proper Directors and the CEOs.

Ms. Freidenrich directed Mr. Lam to get in contact with the County's Director of Internal Audit, Aggie Alonso.

MOTION by Mr. Prevatt, **seconded** by Ms. Freidenrich, to receive and file.

The motion passed **unanimously**.

INFORMATION ITEM

I-1 INTERNAL AUDIT TRANSITION

Presentation by Philip Lam, Director of Internal Audit

Mr. Lam presented his vision for the fourth quarter of 2024 through the first quarter of 2025. This includes finalizing the Final Average Salary, OCERS Employer, and HCA Audit Reports, closing out the LAFCO Audit and the Alameda Audit, assessing the internal audit team, performing and finalizing risk assessment, obtaining buy-in from stakeholders, and executing the 2025 Audit Plan.

Mr. Packard referenced the HCA audit and audits going forward. Mr. Packard encouraged an assessment of current internal operations communication and directed staff to improve communication with key decision-makers.

I-2 BIENNIAL REPORT ON THE OPERATION AND EFFECTIVENESS OF THE OCERS COMPLIANCE PROGRAM

Presentation by Kwame Addo, Chief Compliance Officer

Mr. Addo presented the Compliance Program Update and Roadmap for 2025-2026. Ms. Freidenrich questioned when the Audit Committee would be receiving reports.

Mr. Serpa explained his goal is to provide a Comprehensive Compliance Program. The priority is to complete the remaining two program documents. Currently, four out of six are finished. Mr. Serpa would like to implement the Compliance program as quickly as possible. They are building out the program, and had intended to get the fundamental system in place before submitting reports; however, Mr. Serpa and Mr. Addo agreed that reports can be provided in the interim.

The Audit Committee directed the Compliance Department to provide quarterly reports.

Mr. Packard expressed concern that staff is not educated in Compliance and would like there to be more training provided by the Department. Mr. Prevatt emphasized that staff needs to be evaluated after the training to ensure they retain the knowledge of the training. Mr. Addo informed the Committee there is a plan to have a provider conduct training.

Orange County Employees Retirement System
December 12, 2024
Audit Committee Meeting

Mr. Prevatt directed the Compliance Department to provide an annual Work Plan at the first Audit Committee of the year. The work plan should provide a list of reports that will be presented within the year.

Mr. Prevatt inquired if the Compliance Department monitors the filings of Form 700. Mr. Serpa informed the committee of the Form 700 review process, which is conducted by the CIO and General Counsel, and then reported to the CEO. Mr. Prevatt directed the General Counsel to provide the Form 700 Report annually to the Audit Committee as an Information Item.

WRITTEN REPORTS

The following are written reports that will not be discussed unless a member of the Committee requests discussion.

R-1 MOSS ADAMS, LLP PERFORMANCE SURVEY REPORT

Written Report

R-2 MANAGEMENT ACTION PLAN VERIFICATION REPORT

Written Report

R-3 STATUS UPDATE OF 2024 AUDIT PLAN

Written Report

COMMITTEE MEMBER COMMENTS

Ms. Lopez Tagaloa asked the members of the Audit Committee for their availability in the upcoming year and confirmed February 11th and March 25th for the first two meetings.

STAFF/COUNSEL/CHIEF EXECUTIVE OFFICER COMMENTS

None.

ADJOURNMENT

Chair Packard adjourned the meeting at 12:06 p.m.

Submitted by:

Submitted by:

Approved by:

Philip Lam
Committee Liaison

Steve Delaney
Secretary to the Board

Adele Lopez Tagaloa
Chair



Memorandum

DATE: February 11, 2025
TO: Members of the Audit Committee
FROM: Philip Lam, Director of Internal Audit
SUBJECT: IT AUDIT CONSULTANT FINALIST INTERVIEWS

Recommendation

Staff recommends awarding the contract (subject to satisfactory negotiation of terms) to perform co-sourced IT audits, to one of the three finalists, based on the firm's presentation, responsiveness to the Audit Committee's questions, and the written proposal submitted.

Background/Discussion

At the October 9, 2024 meeting, the Audit Committee was informed that a Request for Proposal (RFP) to initiate a search for an IT Audit and Consulting services vendor would be issued. The current vendor has reached the sixth year of its contract, and the OCERS Procurement and Contracting Policy (Section II.D) specifies that contract terms cannot exceed six years without going through an RFP process.

The Audit Committee Charter states that the Audit Committee's key areas of responsibility include the oversight of external auditors, including conducting the solicitation, selection and appointment for an external auditor (other than the financial auditor and the actuarial auditor) engaged for the purpose of issuing an independent audit report or performing other independent audits, reviews, or attest services.

Selection Process

In October 2024, the RFP for IT Audit and Consulting services was posted on OCERS' website and released to various affiliates. OCERS received seven proposals in response to the RFP from the following vendors:

- Baker Tilly
- Bullet Proof
- Crowe
- Global
- RSM
- Securance
- Weaver



Memorandum

All proposals received were reviewed for responsiveness based on the following criteria:

Pricing & Value	30%
Team Quality & Experience	20%
Experience (Years in business)	20%
RFP Proposal Quality/Presentation	10%
Quality of Work Product/Samples	20%

The review panel, consisting of four staff members reviewed all proposals and scored them on each criterion. Based on the total score from all panelists, the firms were ranked and the top three proposers who scored above the others were determined to be the most qualified to provide OCERS with IT Audit and Consulting services and were selected to interview with OCERS' Audit Committee:

- Baker Tilly
- Crowe
- RSM

Please note that all references to the finalists in this memorandum and the documents that follow are in alphabetical order based on firm names.

Interview Process

The interviews will take place at the February 11, 2025 Audit Committee meeting. The planned procedure is for an approximately 45-minute interview with each firm as follows:

- Each candidate will be given 10-15 minutes to make a general presentation about their firm.
- The Audit Committee will ask each firm the same questions which will not be provided to the candidates ahead of time.
- The Audit Committee may ask the candidate additional or follow-up questions.
- Presentation to conclude with candidate summary.

The interview process will be explained to the candidates prior to the date of the Audit Committee. The finalist firm not being interviewed will be excused from the meeting during the other firm's interviews. The firms will be excused from the meeting once the interview is complete. OCERS will then communicate the decision to the firms of the finalist to be awarded the contract the following day.



Memorandum

Summary of the RFP Responses

The summary below was based solely on staff’s review and understanding of the firms’ RFP responses and was not reviewed by the firms prior to inclusion with the Audit Committee materials.

Category	Baker Tilly	Crowe	RSM
Total Fees	\$60,000	\$80,000	\$57,500
Retirement Plan Experience	<ul style="list-style-type: none"> • NYC Board of Education Retirement System 	<ul style="list-style-type: none"> • San Diego County Employees Retirement Association • Ohio Public Employees Retirement System • Indiana Public Retirement System • School Employees Retirement System of Ohio 	<ul style="list-style-type: none"> • OCERS • State Employees’ Retirement System of Illinois • Utah Retirement Systems • State of Hawaii Employee’s Retirement System • Cook County Pension Fund • 11 additional retirement systems audited nationwide

The full proposals provided by each of the finalists in response to the RFP and the scoring summary are attached to this memorandum.

Submitted by:



PL- Approved

Philip Lam
Director of Internal Audit

Orange County Employee Retirement System

I.T. Audit & Consulting Services RFP - 2024

Date: **December 17, 2024**

OCERS strictly prohibits activities or relationships that create a conflict of interest or even the appearance of a conflict of interest. An OCERS employee is prohibited from scoring a vendor/contractor if they know or have reason to know they have any financial interest in a candidate for the contract or the outcome of the selection. A financial interest means any financial interest, direct or indirect, which might interfere with the employee's unqualified devotion to their duty to OCERS. Additionally, an employee scoring a vendor/contractor must notify the responsible executive of any pre-existing relationship with a candidate, whether familial, friendly, or professional.

Instructions: We will be combining all the reviewer's spreadsheets to derive an aggregated result. Therefore, do not add or modify any cell size or location

Instructions: Make an entry for all areas highlighted in Yellow

Instructions: Enter a score (0 to 4) in each of the evaluation criteria as referenced below (in whole numbers. No decimals):

- 4: A school rating of an "A" - Outstanding. Far exceeds minimum requirements in most areas
- 3: A school rating of an "B" - Above average, exceeds minimum requirements in many areas
- 2: A school rating of an "C" - Average, meets minimum requirements, my exceed minimum requirements in some areas
- 1: A school rating of an "D" - Below average, only meets minimum requirements
- 0: A school rating of an "F" - Does not meet minimum requirements

Note: The Pricing fields are pre-filled as they are static responses that are not open to interpretation

Note: Only change items scoring fields highlighted in Yellow.

		Finalist x		Finalist x		Finalist x		
		BakerTilly		Crowe		RSM		
	Weighting %	Total	Weighted Score	Total	Weighted Score	Total	Weighted Score	
Q1	Experience (Years in business)	20%	5.0	1.0	5.0	1.0	5.0	1.0
Q2	Support team quality/experience	20%	4.0	0.8	4.0	0.8	4.0	0.8
Q3	Pricing / Value	30%	3.0	0.9	2.5	0.8	4.0	1.2
Q4	Quality of work product / samples	20%	3.0	0.6	3.5	0.7	4.0	0.8
Q5	Proposal Presentation	10%	4.0	0.4	4.0	0.4	5.0	0.5
Q6	Not Scored - Price		\$60,000		\$80,000		\$57,500	
			0.00		0.00		0.00	
			3.70		3.65		4.30	
	100%		A		A		A	

Rejects sent 12/19/2024
Finalists awards sent 12/19/2024

Information Technology Audit & Consulting Services

Request for Proposal

October, 2024

Orange County Employees Retirement System (OCERS)
2223 E Wellington Avenue Suite 100
Santa Ana, CA 92701 USA
1-(714)-558-6200
<http://www.ocers.org>

Contents

Section 1: Introduction	3
Section 2: Background	3
Section 3: Scope of Services.....	3
Section 4: General Conditions	4
Section 5: Point of Contact	4
Section 6: Response to Request for Proposal.....	5
Section 7: Proposal Requirements.....	6
Section 8: Evaluation Criteria.....	7
Section 9: Non-Discrimination Requirement	7
Section 10: Notice Regarding the California Public Records Act	8
Section 11: Contract Negotiations.....	8
Section 12: Reservations by OCERS	9
Section 13: Facility Tour.....	10
Exhibit A: Intent to Respond.....	11
Exhibit B: Scope of Services.....	12
Exhibit C: Minimum Qualifications Certification	13
Exhibit D: Proposal Cover Page and Checklist	14
Exhibit E: Services Agreement Template	15

Section 1: Introduction

The Orange County Employees Retirement System (“OCERS”) is requesting proposals from qualified firms interested in providing Information Technology Audit & Consulting services.

Questions about this RFP must be submitted in writing by **5:00 pm, PT, November 1, 2024** to Jim Doezie, Contracts, Risk & Performance Administrator, by email at jdoezie@ocers.org.

Those who wish to be considered must submit their completed proposal by **5:00 p.m., PT, November 22, 2024**. Specific instructions for proposal submissions are contained in Section 7 of this RFP.

Section 2: Background

OCERS was established in 1945 under the County Employees Retirement Law of 1937, providing members with retirement, disability, death, and cost-of-living benefits. There are approximately 50,000 members served by OCERS, of which over 19,000 are retirees. OCERS is governed by a nine-member Board of Retirement (“Board”), which has plenary authority and fiduciary responsibility for the investment of moneys and administration of the retirement system. OCERS has over one hundred employees, and the Board appoints a Chief Executive Officer responsible for the agency’s management. For additional information about OCERS, please refer to the OCERS website at ocers.org.

Section 3: Scope of Services

The detailed scope of services for this engagement is outlined in the attached Exhibit “A” (“Scope of Services”). The primary objectives are to provide OCERS with Information Technology Audit & Consulting services.:

The firm selected for this engagement will be expected to meet requirements that include, but are not limited to, the following:

1. The firm must have all necessary permits and licenses to perform the requested services and must be bonded where applicable.
2. Minimum insurance coverage must include the following items, and proof of such insurance must be provided to OCERS prior to the commencement of work, on an annual basis, and upon request:
 - Commercial General Liability: \$1M per occurrence, \$2M aggregate
 - Automobile Liability: \$1M per occurrence
 - Workers Compensation: \$1M per occurrence
 - Umbrella/Excess Liability: \$5M per occurrence, \$5M aggregate
 - Professional Liability: \$1M per occurrence, \$2M aggregate

OCERS must be listed as an additional insured on the above policies.

3. The firm shall provide all personnel, equipment, tools, materials, vehicles, supervision, and other items and services necessary to perform all services, tasks, and functions as requested in this RFP.

4. The initial term of the contract awarded pursuant to this RFP will be for three years (36 monthly periods), with OCERS retaining the option to renew the contract, on an annual basis, for up to an additional three years. The total term of the contract will not exceed six years.
5. All work under the contract awarded shall be performed and all equipment furnished or installed in accordance with applicable safety codes, ordinances, and other regulations, including the regulations of the State of California, Division of Industrial Safety and the provisions of the California Labor Code.
6. Minimum Qualifications
All respondents are required to sign and return the "Minimum Qualifications Certification," attached as Exhibit "B."

Section 4: General Conditions

All terms, conditions, requirements, and procedures included in this RFP must be met for a proposal to be qualified. A proposal that fails to meet any material term, condition, requirement, or procedure of this RFP may be disqualified. OCERS reserves the right to waive or permit the cure of non-material errors or omissions. OCERS reserves the right to modify, amend, or cancel the terms of this RFP at any time.

OCERS may modify this RFP before the date fixed for submission of a proposal by posting, mailing, emailing, or faxing an addendum to the respondents known to be interested in submitting a proposal. However, failure of a respondent to receive or acknowledge receipt of any addendum shall not relieve the respondent of the responsibility for complying with the terms thereof.

A respondent's proposal shall constitute an irrevocable offer for the 120 days following the deadline for submission of proposals. Reference to a certain number of days in this RFP shall mean calendar days unless otherwise specified.

All proposals submitted in response to this RFP will become the exclusive property of OCERS. Therefore, proposals will not be returned to respondents.

By submitting a proposal, the respondent acknowledges that it has read this RFP, understands it, and agrees to be bound by its requirements unless clearly and specifically noted in the proposal submitted.

Section 5: Point of Contact

A quiet period will be in effect from the date of issuance of this RFP until announcement of the candidate(s) selected. During the quiet period, respondents are not permitted to communicate with any OCERS staff member or Board Member regarding this RFP except through the Point of Contact named herein. Respondents violating this quiet period may be disqualified at OCERS' discretion. In addition, respondents having current business with OCERS must limit their communications to the subject of such business.

OCERS' regular business hours are from 08:00 to 17:00, Monday through Friday, except for federal and state holidays.

The Point of Contact for all matters relating to this RFP is:

Name:	Jim Doezie
Title:	Contracts, Risk & Performance Administrator
Physical Address:	OCERS 2223 E Wellington Ave., Suite 100 Santa Ana, CA 92701
Mailing Address:	OCERS P.O. Box 1229 Santa Ana, CA 92701
Telephone:	(714) 569-4884
Email:	jdoezie@ocers.org
OCERS Website:	www.OCERS.org
Status:	See the OCERS website for status of the RFP and announcements. These items can also be found here: http://www.ocers.org/rfp/requestforproposal.htm

Section 6: Response to Request for Proposal

Proposals must be submitted to the Point of Contact identified in [Section 5](#) and delivered by the due date and time stated below in the RFP Schedule.

OCERS will accept electronic submissions only. Proposals may be submitted electronically in Microsoft Word or Adobe Acrobat PDF format to the email address noted in [Section 5](#). Submission may also be submitted to the PlanetBids site using this link: [PlanetBids Link](#)

RFP Schedule

The following timetable constitutes a tentative schedule for this RFP process. OCERS reserves the right to modify this schedule at any time.

Deliverable	Date	Time
Release of RFP	Tuesday, 10/15/2024	
Submission of RFP Questions to OCERS	Friday, November 1	5:00 p.m. PT
RFP Answers Posted	Friday, November 8	5:00 p.m. PT

RFP Submission Deadline	Friday, November 22	5:00 p.m. PT
OCERS Review of RFP Submissions	November 25 to December 16	
Selection of Finalists	December 20, 2024	
Interviews of Finalists	To be determined	
Service Award [or recommendation to the Board]	To be determined	

Section 7: Proposal Requirements

Proposals must include the following information:

1. The "Minimum Qualifications Certification," attached as Exhibit "B."
2. The "Proposal Cover Page and Check List," attached as Exhibit "C."
3. An executive summary that provides the respondent's background, experience, and other qualifications to provide the services included in the Scope of Services.
4. A description of the respondent including:
 - a. Brief history, including year the respondent firm was formed.
 - b. Ownership structure.
 - c. Office locations.
 - d. Organization chart.
 - e. Number of employees.
 - f. Annual revenues.
 - g. Scope of services offered.
 - h. Respondent's specialties, strengths, and limitations.
5. The names and qualifications of the staff that will be assigned to OCERS work, including a detailed profile of each person's background and relevant individual experience.
6. At least three (3) references for which the respondent has provided services similar to those included in the Scope of Services. Please include for each reference the individual point of contact, a summary of the work performed, and the length of time the respondent provided each service.
7. Copies of any pertinent licenses required to deliver respondent's product or service (e.g., business license).
8. An explanation of the pricing proposal for the scope of work, including pricing of fees and costs, billing practices, and payment terms that would apply. OCERS does limit the pricing approach to pricing and will consider alternative pricing methods for the scope of work, or portions of it. This section of the response should include an explanation as to how the pricing approach(es) will be managed to provide the best value to OCERS. The respondent should represent that the pricing offered to OCERS is, and will remain, equivalent to or better than that provided to other public

pension fund or institutional investor clients or explain why this representation cannot be provided. All pricing proposals should be “best and final,” although OCERS reserves the right to negotiate on pricing.

9. An explanation of all actual or potential conflicts of interest that the respondent may have in contracting with OCERS.
10. A description of all past, pending, or threatened litigation, including malpractice claims, administrative, state ethics, disciplinary proceedings, and other claims against respondent and/or any of the individuals proposed to provide services to OCERS.
11. Any other information that the respondent deems relevant to OCERS’ selection process.

Section 8: Evaluation Criteria

Responses will be evaluated based upon the following:

1. Experience and reputation of the respondent.
2. Quality of the team proposed to provide services to OCERS, including staffing depth, experience, turnover, and compensation.
3. Pricing and value.
4. Delivery and payment terms.
5. Compliance with technical standards contained in this RFP.
6. The organization, completeness, and quality of the proposal.
7. Information provided by references.
8. Other factors OCERS determines to be relevant.

The factors will be considered as a whole, without a specific weighting.

OCERS may require one or more interviews with or personal presentations by finalists to be conducted with staff or members of the Board of Retirement.

If the proposal’s information is deemed to be insufficient for evaluation, OCERS may request additional information or reject the proposal outright at OCERS’ sole discretion. In addition, false, incomplete, or unresponsive statements in connection with a proposal may result in rejection of the proposal.

Section 9: Non-Discrimination Requirement

By submitting a proposal, the respondent represents that it and its subsidiaries do not and will not discriminate against any employee or applicant for employment based on race, religion, color, national origin, ethnic group identification, mental disability, physical disability, medical condition, genetic information, marital status, ancestry, sex, gender, sexual orientation, gender identity, gender expression, age, or military and veteran status.

Section 10: Notice Regarding the California Public Records Act

The information submitted in response to this RFP will be subject to public disclosure pursuant to the California Public Records Act (California Government Code Section 6250, et. seq., the "Act"). The Act provides that all records relating to a public agency's business are open to public inspection and copying unless exempted explicitly under one of several exemptions set forth in the Act. If a respondent believes any portion of its proposal is exempt from public disclosure under the Act, the respondent must provide a full explanation and mark such portion "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY," and make it readily separable from the balance of the response. Proposals marked "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY" in their entirety will not be honored, and OCERS will not deny public disclosure of all or any portion of proposals so marked.

By submitting a proposal with material marked "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY," a respondent represents it has a good faith belief that the material is exempt from disclosure under the Act; however, such designations will not necessarily be conclusive, and a respondent may be required to justify in writing why OCERS should not disclose such material under the Act. Fee and pricing proposals are not considered "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY."

If OCERS receives a request pursuant to the Act for materials that a respondent has marked "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY," and if OCERS agrees that the material requested is not subject to disclosure under the Act, OCERS will either notify the respondent so that it can seek a protective order at its own cost and expense, or OCERS will deny disclosure of those materials. OCERS will not be held liable for inadvertent disclosure of such materials, data, and information or for disclosure of such materials if deemed appropriate in OCERS' sole discretion. OCERS retains the right to disclose all information provided by a respondent.

If OCERS denies public disclosure of any materials designated as "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY," the respondent agrees to reimburse OCERS for, and to indemnify, defend, and hold harmless OCERS, its Boards, officers, fiduciaries, employees, and agents from and against:

1. Any and all claims, damages, losses, liabilities, suits, judgments, fines, penalties, costs, and expenses, including, without limitation, attorneys' fees, expenses, and court costs of any nature whatsoever (collectively, "Claims") arising from or relating to OCERS' non-disclosure of any such designated portions of a proposal; and
2. Any and all Claims arising from or relating to OCERS' public disclosure of any such designated portions of a proposal if OCERS determines disclosure is required by law, or if disclosure is ordered by a court of competent jurisdiction.

Section 11: Contract Negotiations

OCERS will propose a contract to the successful respondent, which will contain such terms as OCERS, in its sole discretion, may require. In addition, the selected firm will agree that this RFP and the firm's proposal will be incorporated into any resulting contract.

This RFP is not an offer to contract. Acceptance of a proposal neither commits OCERS to award a contract to any respondent nor does it limit OCERS' right to negotiate the terms of a contract in OCERS' best interest, including the addition of terms not mentioned in this RFP. The final contract must, among other terms and conditions required by OCERS, allow OCERS to terminate the contract a) for OCERS' convenience, b) if funds are not appropriated for the services, or c) for default.

The general form of the contract OCERS intends to use is included as Exhibit "E" ("OCERS Services Agreement"). OCERS reserves the right to make changes to the contract prior to execution, including material changes. The final Scope of Services to be included in the contract will be determined at the conclusion of the RFP process.

By submitting a proposal without comment on the OCERS Services Agreement, respondent will be deemed to have agreed to each term in the OCERS Services Agreement, and to not seek any modifications to it. If respondent objects to any term in the OCERS Services Agreement or wishes to modify or add terms to the OCERS Services Agreement, the proposal must identify each objection and propose language for each modification and additional term sought. A rationale should be included for each objection, modification, or addition.

Section 12: Reservations by OCERS

In addition to the other provisions of this RFP, OCERS reserves the right to:

1. Cancel or modify this RFP, in whole or in part, at any time.
2. Make such investigation as it deems necessary to determine the respondent's ability to furnish the required services, and the respondent agrees to furnish all such information for this purpose as OCERS may request.
3. Reject the proposal of any respondent who is not currently in a position to perform the services, or who has previously failed to perform similar services properly, or in a timely manner, or for any other reason in OCERS' sole discretion.
4. Waive irregularities, to negotiate in any manner necessary to best serve the public interest, and to make a whole award, multiple awards, a partial award, or no award.
5. Award a contract, if at all, to the firm which will provide the best match to the requirements of the RFP and the service needs of OCERS in OCERS' sole discretion, which may not be the proposal offering the lowest fees.
6. Request additional documentation or information from respondents, which may vary by respondent. OCERS may ask questions of any respondent to seek clarification of a proposal or to ensure the respondent understands the scope of the work or other terms of the RFP.
7. Reject any or all proposals submitted in response to this RFP.
8. Choose to not enter into an agreement with any of the respondents to this RFP or negotiate for the services described in this RFP with a party that did not submit a proposal.
9. Determine the extent, without limitation, to which the services of a successful respondent are or are not actually utilized.

10. Defer selection of a bidder to a time of OCERS' choosing.
11. Consider information about a respondent other than, and in addition to, that submitted by the respondent.

Exhibit A

Scope of Services

A consultant, under the supervision of OCERS Director of Internal Audit, will be expected to provide the following range of IT audit/consulting services to OCERS regarding (1) IT General Controls (ITGC) and (2) Cybersecurity. The consultant will also provide (3) a high-level review to support Internal Audit IT risk assessment, with the goal of assisting in the development of the IT internal audit plan for the next 1-3 years. The consultant will help build a multi-year IT audit program for OCERS Internal Audit Department based on an IT risk assessment using a format that is consistent with the format used by OCERS' Internal Audit Department.

The frequency and/or rotation of the audits in the audit plan will be tailored and customized based on OCERS' budget constraints and risk appetite. Future IT audits are subject matter specific audits that address specific IT risks and will also be identified in the multi-year audit program. The multi-year audit plan should include only audits typical for organizations the size of OCERS and for common IT risks that such an organization may face. Due to general security concerns, details such as number of servers, types of platforms, number of key applications, databases, data centers and locations, use of outsourced IT functions, Cybersecurity controls, etc. will only be disclosed to the selected vendor.

IT General Controls (ITGC)

- For IT General Controls, build and develop an overall audit policy and audit procedures for in collaboration with OCERS Internal Audit, OCERS management and OCERS external auditor. In addition, develop a risk controls matrix to identify controls that mitigate the corresponding ITGC risks. Build an audit program that tests the design and operating effectiveness of those controls. Key areas for audit may include governance, access controls, change management, backup and recovery, logical and physical security, IT operations, vendor and third-party management, log management, asset management, etc. The consultant will also provide observations and recommendations and inquire with management for their assistance with future remediation.

Cybersecurity

For Cybersecurity, build and develop an overall audit policy and audit procedures in collaboration with OCERS Internal Audit and OCERS management. In addition, develop a risk controls matrix to identify controls that mitigate the corresponding Cybersecurity risks. Build an audit program that tests the design and operating effectiveness of those controls. Key areas for audit may include governance, identity and access management, data protection, data privacy, threat intelligence, vulnerability management, network security, endpoint security, application security, cloud security, incident response, security operations, third-party risk management, etc. The consultant will also provide observations and recommendations, and inquire with management for their assistance with future remediation.

Internal Audit IT Risk Assessment/Audit Program

- Assist in the development of the Internal Audit IT audit plan for the next 1 to 3 years by performing a high-level review in support of the Internal Audit risk assessment. A multi-year IT audit plan with ITGC and Cybersecurity audits would be identified as a result of the IT risk assessment.

In addition to the foregoing, core skills and expertise of the consultant shall include excellent oral and written communication skills, sound judgment, the ability to work well with and maintain the confidence of the Board and staff, and the ability to deliver services in a timely and cost-effective manner.

The selected consultants shall be able to provide all personnel, equipment, tools, materials, vehicles, supervision, and other items and services necessary to perform all services, tasks, and functions as defined in this RFP.

Proposals must include the following information:

1. A current Curriculum Vitae of the lead consultant(s) must be included in the proposal.
2. The candidate shall submit writing samples for review that demonstrate the candidate's ability to create an adequate IT Risk Assessment, IT audit plan, and Cybersecurity audit plan.
3. The candidate shall provide as much information as possible about past experience as an IT Auditor/Consultant with direct experience relevant to the scope of work identified.
4. The candidate shall provide an affirmative statement that if he/she is selected to serve as a consultant, he/she will be independent of OCERS and not related in any way to OCERS' business operations. The candidate should also provide an affirmative statement that he/she is not currently in litigation with OCERS or any of OCERS plan sponsor agencies.
5. The candidate shall provide an affirmative statement that he/she has not given a gift or political campaign contribution to any officer, Board member, or employee of OCERS within the past twenty-four (24) months.
6. The candidate shall detail any work performed for other retirement systems or pension plans.
7. Any other information that the respondent deems relevant to OCERS' selection process.

Exhibit B

MINIMUM QUALIFICATIONS CERTIFICATION

All firms submitting a proposal in response to this RFP are required to sign and return this attachment, along with written evidence of how the respondent meets each qualification.

The undersigned hereby certifies that it fulfills the minimum qualifications outlined below, as well as the requirements contained in the RFP.

Minimum Qualifications include:

1. The auditor should have professional certifications such as CISA, CIA, CISSP, CRISC, or similar.
2. Minimum 7+ years of IT Audit experience: The auditor should have substantial experience in conducting both ITGC and Cybersecurity audits.
3. Experience in conducting risk-based ITGC audits: The auditor should use a risk-based approach in their audit methodology, focusing on areas with higher risks to the organization.
4. Experience conducting risk-based Cybersecurity audits: The auditor should adopt a risk-based approach, focusing on high-risk areas, critical assets, and potential vulnerabilities.
5. Familiarity with recognized security frameworks: The auditor should be proficient in assessing against the NIST Cybersecurity Framework and CIS Controls.
6. Ability to develop control matrices and test plans: Experience in designing and implementing IT control matrices and audit test plans for IT audits.
7. Proven track record in delivering audit reports: Ability to write clear, concise, and actionable audit reports suitable for presentation to senior management and audit committees.

The undersigned hereby certifies that they are an individual authorized to bind the Firm contractually, and said signature authorizes verification of this information.

Authorized Signature

Date

Name and Title (please print)

Name of Firm

Exhibit C

PROPOSAL COVER PAGE AND CHECK LIST (TO BE SUBMITTED IN FIRM'S LETTERHEAD)

Respondent Name:

Respondent Signature:

Respondent Address:

By submitting this response, the undersigned hereby affirms and represents that they have reviewed the proposal requirements and have submitted a complete and accurate response to the best of their knowledge. By signing below, I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements.

Respondent specifically acknowledges the following:

1. Respondent possesses the required technical expertise and has sufficient capacity to provide the services outlined in the RFP.
2. Respondent has no unresolved questions regarding the RFP and believes that there are no ambiguities in the scope of services.
3. The fee schedule submitted in response to the RFP is for the entire scope of services and no extra charges or expenses will be paid by OCERS.
4. Respondent has completely disclosed to OCERS all facts bearing upon any possible interests, direct or indirect, that Respondent believes any member of OCERS, or other officer, agent, or employee of OCERS presently has, or will have, in this contract, or in the performance thereof, or in any portion of the profits thereunder.
5. Materials contained in the proposal and all correspondence and written questions submitted during the RFP process are subject to disclosure pursuant to the California Public Records Act.
6. Respondent is not currently under investigation by any state or federal regulatory agency for any reason.
7. Except as specifically noted in the proposal, respondent agrees to all of the terms and conditions included in OCERS Services Agreement.
8. The signatory above is authorized to bind the respondent contractually.

Exhibit D

SERVICES AGREEMENT TEMPLATE

ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM

AGREEMENT FOR SERVICES

This Agreement for Services (“Agreement”) is entered into this [REDACTED] day of [REDACTED], 20[REDACTED] (the “Effective Date”) by and between the Orange County Employees Retirement System, (“OCERS”) and [REDACTED] (“Contractor”). OCERS and Contractor are sometimes individually referred to as “Party” and collectively as “Parties.” The Parties hereby agree as follows:

ARTICLE 1

PURPOSE

- 1.1 **Project.** Contractor desires to perform and assume responsibility for the provision of, and OCERS desires to engage Contractor to render, services for **IT Audit & Consulting services** on the terms and conditions set forth in this Agreement and its attached exhibits.

ARTICLE 2

TERMS

- 2.1 **Scope of Services.** Contractor promises and agrees to furnish to OCERS all labor, materials, tools, equipment, services, and incidental and customary work necessary to fully and adequately perform all services contemplated by this Agreement (“Services”), as more particularly described in the attached **Exhibit “A”** (“Scope of Services”). All Services shall be subject to, and performed in accordance with, this Agreement, the exhibits attached hereto and incorporated herein by reference, and all applicable local, state, and federal laws, rules, and regulations. Contractor represents and warrants to OCERS that Contractor will perform the Services in a professional and workmanlike manner, in accordance with best industry standards and practices used in well-managed operations performing services similar to the Services. To the extent necessary to facilitate performance of the Services, OCERS may, in its discretion, make certain of its facilities, assets, and resources available on an “as is, where is” basis to Contractor at Contractor’s request. While on OCERS’ premises, Contractor agrees to comply with OCERS’ access rules and procedures, including those related to safety, security, and confidentiality.
- 2.2 **Term.** The term of this Agreement will commence upon the Effective Date and will continue for thirty-six months from the Effective Date (“Term”), unless earlier

terminated as provided herein. The Parties may, by mutual written agreement, extend the Term for up to thirty-six additional twelve (36) month periods. In no event shall the total term of the Agreement exceed seventy-two (72) months.

2.3 **Consideration.**

- 2.3.1 **Compensation.** Contractor shall receive compensation, including authorized reimbursements, for all Services rendered under this Agreement as set forth in Exhibit “B” (“Fee Schedule”).
- 2.3.2 **Invoices and Payment.** Contractor shall submit to OCERS monthly itemized invoices as required by the Fee Schedule. OCERS shall pay all undisputed charges within net thirty (30) days of receiving such invoice.
- 2.3.3 **Extra Work.** At any time during the term of this Agreement, OCERS may request that Contractor perform Extra Work. As used herein, “Extra Work” means any work which is determined by OCERS to be necessary for the proper completion of the Services, but which the Parties did not reasonably anticipate would be necessary as of the Effective Date. Contractor shall not perform, nor be compensated for, Extra Work without written authorization by OCERS. Extra Work, if authorized by OCERS, will be compensated at the rates and manner set forth in this Agreement.

2.4 **Responsibilities of Contractor.**

- 2.4.1 **Independent Contractor.** Contractor’s relationship with OCERS is that of an independent contractor, and nothing in this Agreement is intended to, or should be construed to, create a partnership, agency, joint venture, or employment relationship between OCERS and any of Contractor’s employees or agents. Contractor is not authorized to make any representation, contract, or commitment on behalf of OCERS. Except as OCERS may agree in writing, Contractor shall have no authority, expressed or implied, to act on behalf of OCERS in any capacity whatsoever as an agent of OCERS. The Services shall be performed by Contractor or by Contractor’s employees under Contractor’s supervision. Contractor will determine the means, methods, and details of performing the Services subject to the requirements of this Agreement. Contractor is an independent contractor and not an employee of OCERS. Any additional personnel performing the Services under this Agreement on behalf of Contractor will also not be employees of OCERS and will at all times be under Contractor’s exclusive direction and control.
- 2.4.2 **No Benefits and Payment of Subordinates.** Contractor (if Contractor is an individual) and Contractor’s personnel will not be entitled to any of the benefits that OCERS may make available to its employees, including, but not limited to, group health insurance, life insurance, or retirement benefits. Contractor will pay all wages, salaries, and other amounts due its personnel in connection with their

performance of Services under this Agreement and as required by law. Contractor shall be responsible for all reports and obligations respecting such additional personnel, including, but not limited to social security taxes, income tax withholding, unemployment insurance, disability insurance, and workers' compensation insurance. Contractor will bear the sole responsibility and liability for furnishing Workers' Compensation benefits to all such personnel for injuries arising from or connected with the Services.

- 2.4.3 Tax. Because Contractor is an independent contractor, OCERS will not withhold or make payments for social security, make unemployment insurance, or disability insurance contributions, or obtain workers' compensation insurance on behalf of Contractor. Contractor is solely responsible for, and will file, on a timely basis, all tax returns and payments required to be filed with, or made to, any federal, state, or local tax authority with respect to the performance of Services and receipt of fees under this Agreement. Contractor is solely responsible for, and must maintain adequate records of, expenses incurred in the course of performing Services under this Agreement. No part of Contractor's compensation will be subject to withholding by OCERS for the payment of any social security, federal, state or any other employee payroll taxes.
- 2.4.4 Licensing. Contractor represents that it, its employees, and subcontractors have all licenses, permits, qualifications, and approvals of whatever nature that are legally required to perform the Services, and that such licenses and approvals shall be maintained throughout the term of this Agreement.
- 2.4.5 Conformance to Applicable Requirements. All Services performed by Contractor shall be subject to the approval of OCERS.
- 2.4.6 Substitution of Key Personnel. Contractor has represented to OCERS that certain key personnel, listed in the attached **Exhibit "C"** ("Key Personnel"), will perform and coordinate the Services under this Agreement. Key Personnel will be available to perform Services under the terms and conditions of this Agreement immediately upon commencement of the term of this Agreement. If one or more of such Key Personnel becomes unavailable, Contractor may substitute other personnel of at least equal competence upon written approval of OCERS. Contractor shall provide OCERS written notification detailing the circumstances of the unavailability of the Key Personnel and designating replacement personnel prior to the effective date of the unavailability of such Key Personnel, to the maximum extent feasible, but no later than five (5) business days after the date of the Key Personnel's unavailability. OCERS will have the right to approve or disapprove the reassignment or substitution of Key Personnel for any reason at OCERS' sole discretion. In the event that OCERS and Contractor cannot agree as to the substitution of Key Personnel, OCERS will be entitled to terminate this Agreement for cause.

- 2.4.7 Removal of Key Personnel. Contractor agrees to remove any Key Personnel from performing Services under this Agreement within twenty-four (24) hours or as soon thereafter as is practicable if reasonably requested to do so by the OCERS.
- 2.4.8 Laws and Regulations. Contractor shall keep itself fully informed of and in compliance with all local, state, and federal laws, rules, and regulations in any manner affecting the performance of the Services, including all Cal/OSHA requirements, and shall give all notices required by law. Contractor shall be liable for all violations of such laws and regulations in connection with Services. If Contractor performs any work knowing it to be contrary to such laws, rules, and regulations, Contractor shall be solely responsible for all costs arising therefrom.
- 2.4.9 Labor Code Provisions.
- A. Prevailing Wages. Contractor is aware of the requirements of California Labor Code Section 1720, et seq., and 1770, et seq., as well as California Code of Regulations, Title 8, Section 16000, et seq. (“Prevailing Wage Laws”), which require the payment of prevailing wage rates and the performance of other requirements on “public works” and “maintenance” projects. If the Services are being performed as part of an applicable “public works” or “maintenance” project, as defined by the Prevailing Wage Laws, and if the total compensation is \$1,000 or more, Contractor agrees to fully comply with such Prevailing Wage Laws. Contractor shall comply with all prevailing wage requirements under the California Labor Code and Contractor shall forfeit as penalty to OCERS a sum of not more than \$200 for each calendar day, or portion thereof, for each worker paid less than the prevailing rates. This penalty shall be in addition to any shortfall in wages paid. OCERS has obtained the general prevailing rate of wages, as determined by the Director of the Department of Industrial Relations (“DIR”), a copy of which is on file in OCERS’s office and shall be made available for viewing to any interested party upon request. Contractor shall make copies of the prevailing rates of per diem wages for each craft, classification, or type of worker needed to execute the Services available to interested parties upon request and shall post copies at Contractor’s principal place of business and at the site where Services are performed.
- B. Registration and Labor Compliance. If the Services are being performed as part of an applicable “public works” or “maintenance” project, then, in addition to the foregoing, pursuant to Labor Code sections 1725.5 and 1771.1, Contractor and all subcontractors must be registered with the DIR. Contractor shall maintain registration for the duration of this Agreement and require the same of any subcontractors. The Services may also be subject to compliance monitoring and enforcement by the

DIR. It shall be Contractor's sole responsibility to comply with all applicable registration and labor compliance requirements, including the submission of payroll records directly to the DIR.

- C. Labor Certification. By its signature hereunder, Contractor certifies that it is aware of the provisions of Section 3700 of the California Labor Code which require every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code and agrees to comply with such provisions before commencing the performance of the Services.

2.4.10 Accounting Records. Contractor shall maintain complete and accurate records with respect to all costs and expenses incurred under this Agreement. All such records shall be clearly identifiable. Contractor shall allow a representative of OCERS during normal business hours to examine, audit, and make transcripts or copies of such records and any other documents created pursuant to this Agreement. Contractor shall allow inspection of all work, data, documents, proceedings, and activities related to the Agreement for a period of four (4) years from the date of final payment under this Agreement. Pursuant to California Government Code Section 8546.7, the parties acknowledge that every contract involving the expenditure of public funds in excess of \$10,000 shall be subject to audit by the California State Auditor.

2.4.11 Business Continuity Plan. Contractor warrants that it has and will maintain throughout the term of this Agreement a written business continuity plan ("BCP") to enable it to recover and resume the Services provided by it to OCERS within one (1) Business Day in the event of any disruptive event. Contractor further represents and warrants that it has tested its BCP and will continue to conduct sufficient ongoing verification testing for the recovery and resumption of services provided to OCERS and will update its BCP at least annually. Contractor will notify OCERS within thirty (30) days of any material alterations to its BCP that would impair its ability to recover and resume any interrupted Services it provides to OCERS. Upon request by OCERS, Contractor will provide to OCERS a description of its BCP procedures as they relate to the recovery and resumption of the Services accompanied by a written certification that the BCP has undergone review and testing to account for any changes to such Services. Contractor shall promptly notify OCERS of any actual, threatened, or anticipated event that does or may disrupt or impact the Services provided by Contractor and will cooperate fully with OCERS to minimize any such disruption and promptly restore and recover the Services.

2.4.12 Inducement. Contractor warrants that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by Contractor or any agent or representative of Contractor, to any officer or employee of OCERS with a view

toward securing this Agreement or securing favorable treatment with respect to any determinations concerning the performance of this Agreement.

- 2.4.13 **No Conflict.** Contractor will refrain from any activity, and will not enter into any agreement or make any commitment, that is inconsistent or incompatible with Contractor's obligations under this Agreement, including Contractor's ability to perform the Services. Contractor represents and warrants that Contractor is not subject to any contract or duty that would be breached by Contractor's entering or performing Contractor's obligations under this Agreement or that is otherwise inconsistent with this Agreement.

2.5 **Representatives of the Parties.**

- 2.5.1 **OCERS' Representative.** OCERS hereby designates **Mark Adviento**, to act as its representative for the performance of this Agreement ("OCERS' Representative"). Contractor shall not accept direction or orders from any person other than the OCERS' Representative.

- 2.5.2 **Contractor's Representative.** Contractor hereby designates **[name or title]**, or their designee, to act as its representative for the performance of this Agreement ("Contractor's Representative"). Contractor's Representative shall have full authority to represent and act on behalf of Contractor for all purposes under this Agreement. Contractor's Representative shall supervise and direct performance of the Services, using their best skill and attention, and shall be responsible for all means, methods, techniques, sequences, and procedures and for the satisfactory coordination of all portions of the Services under this Agreement.

2.6 **Indemnification.**

- 2.6.1 **Indemnity by Contractor.** To the fullest extent permitted by law, Contractor shall indemnify, immediately defend, and hold OCERS, the members of the OCERS Board of Retirement, and OCERS' officials, officers, employees, volunteers, and agents (collectively, "OCERS Indemnitees") free and harmless from and against all Losses (as defined in Section 2.6.4 below) that any OCERS Indemnitee shall suffer, sustain or become subject to in any manner arising out of, pertaining to, or incident to any (i) negligent act, error or omission, or intentional misconduct by Contractor, its officials, officers, employees, subcontractors, contractors, or agents in connection with the performance of the Services or (ii) breach or alleged breach of this Agreement by Contractor. Contractor's duty to indemnify does not extend to the Indemnity Claims caused by OCERS' sole negligence or willful misconduct.
- 2.6.2 **Third-Party Claims.** Contractor shall immediately defend, with legal counsel reasonably agreed to by OCERS and at Contractor's own cost, expense, and risk, any Indemnity Claims; excluding, however, such claims arising from OCERS' sole negligence or willful misconduct. Contractor shall control the defense or settlement

of any such action, except that Contractor will not have the right to settle or compromise the claim without the consent of OCERS. Contractor shall pay and satisfy any judgment, award, or decree that may be rendered against any OCERS Indemnitee as part of any Indemnity Claim(s). Contractor shall also reimburse OCERS for the cost of any settlement paid by any OCERS Indemnitee as part of any Indemnity Claim. Such reimbursement shall include payment for OCERS' attorneys' fees and costs, including expert witness fees.

- 2.6.3 Civil Code Section 2782.8. Notwithstanding the foregoing, to the extent the Services are subject to Civil Code Section 2782.8, the above indemnity and duty to defend shall be limited, to the extent required by Civil Code Section 2782.8, to claims that arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of Contractor.
- 2.6.4 Definition of Losses. As used in this Agreement, "Losses" mean all damages, dues, penalties, fines, amounts paid in settlement, taxes, costs, obligations, losses, expenses, and fees (including court costs and reasonable attorneys' and expert witness fees and expenses), including, as the context may require, any of the foregoing that arise out of or in connection with any actions, suits, proceedings, hearings, investigations, charges, complaints, claims, demands, injunctions, judgments, orders, decrees, or rulings.

2.7 Insurance.

- 2.7.1 Time for Compliance. Contractor shall not commence work under this Agreement until it has provided evidence satisfactory to OCERS that it has secured all insurance required under this Section 2.7. In addition, Contractor shall not allow any subcontractor to commence work on any subcontract until Contractor has provided evidence satisfactory to OCERS that the subcontractor has secured all insurance required under this section. Failure to provide and maintain all required insurance shall be grounds for the OCERS to terminate this Agreement for cause.
- 2.7.2 Minimum Requirements. Contractor shall, at its expense, procure and maintain for the duration of the Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the Agreement by Contractor, its agents, representatives, employees, or subcontractors. Contractor shall also require all its subcontractors to procure and maintain the same insurance for the duration of the Agreement. Such insurance shall meet the following requirements:
- A. Commercial General Liability. Commercial general liability insurance, including bodily injury, personal injury, property damage and productions/completed operations coverage, in the amount not less than one million dollars (\$1,000,000) per occurrence, \$2 million (\$2,000,000) aggregate.

- B. **Automobile Liability.** Business automobile liability insurance insuring all owned, non-owned, and hired automobiles, in the amount not less than one million dollars (\$1,000,000) combined single limit per accident for bodily injury and property damage.
 - C. **Workers' Compensation and Employer's Liability Insurance.** Workers' Compensation insurance as required by the State of California and Employer's Liability Insurance in an amount not less than one million dollars (\$1,000,000) per accident for bodily injury or disease. The insurer shall agree to waive all rights of subrogation against the OCERS Indemnitees for losses paid under the terms of the insurance policy which arise from work performed by Contractor.
 - D. **Professional Liability.** Errors and omissions liability insurance appropriate to their profession covering Contractor's wrongful acts, negligent actions, errors, or omissions in the amount not less than one million dollars (\$1,000,000) per claim, two million (\$2,000,000) aggregate, and covering the period from the effective date of this Agreement until five (5) years following the termination or expiration of this Agreement.
 - E. **Excess Liability.** The limits of insurance required in this Agreement may be satisfied by a combination of primary and umbrella or excess insurance. Any umbrella or excess coverage shall contain or be endorsed to contain a provision that such coverage shall also apply on a primary and non-contributory basis for the benefit of the OCERS Indemnitees (if agreed to in a written contract or agreement) before any OCERS Indemnitee's own primary or self-insurance shall be called upon to protect it as a named insured. The policy shall be endorsed to state that the OCERS Indemnitees shall be covered as additional insured. The coverage shall contain no special limitations on the scope of protection afforded to the OCERS Indemnitees. The coverage shall be in the amount not less than five million dollars (\$5,000,000) per claim and aggregate.
- 2.7.3 **All Coverages; No Contribution.** All insurance which Contractor is obligated to procure and maintain shall include or be endorsed to state that: (1) the OCERS Indemnitees shall be covered as additional insured with respect to work by or on behalf of Contractor, including materials, parts, or equipment furnished in connection with such work; and (2) the insurance coverage shall be primary insurance with respect to the OCERS Indemnitees, or if excess, shall stand in an unbroken chain of coverage excess of Contractor's scheduled underlying coverage. Any insurance or self-insurance maintained by any OCERS Indemnitee shall be excess of Contractor's insurance and shall not be called upon to contribute with it in any way.

- A. The insurance policies required by Section 2.7.2 above shall contain or be endorsed to contain the following specific provisions:
- I. The policies shall contain a waiver of transfer rights of recovery (“waiver of subrogation”) against the OCERS Indemnitees, for any claims arising out of the work of Contractor.
 - II. Policies may provide coverage which contains deductible or self-insured retentions. Such deductible and/or self-insured retentions shall not be applicable with respect to the coverage provided to the OCERS Indemnitees under such policies. Contractor shall be solely responsible for deductible and/or self-insured retention and OCERS, at its sole discretion, may require Contractor to secure the payment of such deductible or self-insured retentions by a surety bond or an irrevocable and unconditional letter of credit. The insurance policies that contain deductibles or self-insured retentions in excess of \$25,000 per occurrence shall not be acceptable without the prior approval of OCERS.
 - III. Prior to start of work under this Agreement, Contractor shall file with OCERS certificate(s) of insurance signed by an authorized representative of the insurer(s) evidencing and certifying to the insurance coverage required by Section 2.7.2.
 - IV. Each insurance policy required by Section 2.7.2 shall contain a cancellation clause that provides such policy shall not be cancelled or otherwise terminated by the insurer or Contractor or reduced in coverage or in limits except after thirty (30) days’ prior written notice by certified mail, return receipt requested, has been given to OCERS, Attention: Jim Doezie
 - V. Insurance required by Section 2.7.2 shall be placed with insurers licensed by the State of California to transact insurance business of the types required herein. Each insurer shall have a current Best Insurance Guide rating of not less than A: VII unless prior approval is secured from OCERS as to the use of such insurer.
 - VI. Contractor shall include all subcontractors as insureds under its policies or shall furnish separate certificates and endorsements for each subcontractor. All coverages for subcontractors shall be subject to all the requirements stated herein.

2.7.4 Reporting of Claims. Contractor shall report to OCERS, in addition to Contractor’s insurer, any and all insurance claims submitted by Contractor in connection with the Services under this Agreement.

2.8 Termination of Agreement.

2.8.1 Termination. OCERS may, by written notice to Contractor, terminate the whole or any part of this Agreement without liability to OCERS if Contractor fails to perform or breaches any of the terms contained herein. In addition, either Party may terminate this Agreement for any reason or for no reason on thirty (30) days' written notice to the other Party. Upon termination, Contractor shall be compensated only for those Services that have been performed and delivered to OCERS' satisfaction, and Contractor shall be entitled to no further compensation.

2.8.2 Survival. The rights and obligations contained in Section 2.4 (Responsibilities of Contractor), Section 2.6 (Indemnification), and Section 2.9 (Ownership of Work Product and Confidentiality) will survive any termination or expiration of this Agreement.

2.9 Ownership of Work Product and Confidentiality.

2.9.1 Ownership of Work Product; Licensing of Intellectual Property. Contractor hereby irrevocably assigns to OCERS all right, title and interest worldwide in and to any and all discoveries, developments, formulae, information, materials, improvements, designs, artwork, content, software programs, other works of authorship, and any other work product created, conceived, or developed by Contractor (whether alone or jointly with others) for OCERS during or before the term of this Agreement, including all copyrights, patents, trademarks, trade secrets, and other intellectual property rights therein (including all rights to priority and rights to file patent applications and/or registered designs) ("Work Product"). Contractor retains no rights to use the Work Product and agrees not to challenge the validity of OCERS' ownership of, or intellectual property rights in, the Work Product. Contractor agrees to execute, at OCERS' request and expense, all documents and other instruments necessary or desirable to confirm such assignment, including without limitation, any copyright assignment or patent assignment provided by OCERS. Contractor hereby irrevocably appoints OCERS as Contractor's attorney-in-fact for the purpose of executing such documents on Contractor's behalf, which appointment is coupled with an interest. At OCERS' request, Contractor will promptly record any such patent assignment with the United States Patent and Trademark Office. OCERS will reimburse Contractor for any reasonable out-of-pocket expenses actually incurred by Contractor in fulfilling its obligations under this section. Contractor will deliver each item of Work Product specified in **Exhibit "A"** and disclose promptly in writing to OCERS all other Work Product.

2.9.2 Other Rights. If Contractor has any rights, including without limitation "artist's rights" or "moral rights," in the Work Product that cannot be assigned, Contractor hereby unconditionally and irrevocably grants to OCERS an exclusive (even as to Contractor), worldwide, fully paid and royalty-free, irrevocable, perpetual license, with rights to sublicense through multiple tiers of sublicensees, to use, reproduce,

distribute, create derivative works of, publicly perform and publicly display the Work Product in any medium or format, whether now known or later developed. In the event that Contractor has any rights in the Work Product that cannot be assigned or licensed, Contractor unconditionally and irrevocably waives the enforcement of such rights, and all claims and causes of action of any kind against OCERS and its affiliates.

- 2.9.3 License to Preexisting IP. Contractor agrees not to use or incorporate into Work Product any intellectual property developed by any third party or by Contractor other than in the course of performing Services for OCERS (“Preexisting IP”) unless the Preexisting IP has been specifically identified and described in **Exhibit “A”**. In the event Contractor uses or incorporates Preexisting IP into Work Product, Contractor hereby grants to OCERS a non-exclusive, worldwide, fully-paid and royalty-free, irrevocable, perpetual license, with the right to sublicense through multiple tiers of sublicensees, to use, reproduce, distribute, digitally transmit, create derivative works of, publicly perform, and publicly display in any medium or format, whether now known or later developed, such Preexisting IP incorporated or used in Work Product.
- 2.9.4 Confidential Information. Any financial, statistical, personal, technical, and other data and information relating to a Party’s operations which are made available to the other Party in order to carry out this Agreement shall be reasonably protected by such other Party from unauthorized use, except to the extent that disclosure thereof is required to comply with applicable law, including the California Public Records Act. Confidentiality does not apply to information which is known to a receiving Party from other sources, which is otherwise publicly available, or which is required to be disclosed pursuant to an order or requirements of a regulatory body or a court.
- 2.9.5 Customer Data. Contractor acknowledges that it may receive confidential information from OCERS or otherwise in connection with this Agreement or the performance of the Services, including personally identifiable information of OCERS’ customers and members (“Customer Data”). Except for information in the public domain, unless such information falls into the public domain by disclosure or other acts of OCERS or through the fault of OCERS, Contractor agrees:
- A. To maintain Customer Data in confidence;
 - B. Not to use Customer Data other than in the course of this Agreement;
 - C. Not to disclose or release Customer Data except on a need-to-know only basis;

- D. Not to disclose or release Customer Data to any third person without the prior written consent of OCERS, except for authorized employees or agents of Contractor;
- E. To promptly notify OCERS in writing of any unauthorized release of confidential information, including Customer Data;
- F. To take all appropriate action, whether by instruction, agreement or otherwise, to ensure that third persons with access to the information under the direction or control or in any contractual privity with Contractor, do not disclose or use, directly or indirectly, for any purpose other than for performing the Services during or after the term of this Agreement, any confidential information, including Customer Data, without first obtaining the written consent of OCERS; and
- G. Upon request by OCERS and upon the termination or expiration of this Agreement for any reason, Contractor shall promptly return to OCERS all copies, whether in written, electronic, or other form or media, of Customer Data in its possession or in the possession of its employees or agents, or securely dispose of all such copies, and certify in writing to OCERS that such Customer Data has been returned to OCERS or disposed of securely.

2.9.6 Disclosure. Except as may be required by applicable law, neither Party shall make any disclosure of any designated confidential information related to this Agreement without the specific prior written approval from the other of the content to be disclosed and the form in which it is disclosed, except for such disclosures to the Parties' financing sources, other secured parties, creditors, beneficiaries, partners, members, officers, employees, agents, consultants, attorneys, accountants, and exchange facilitators as may be necessary to permit each Party to perform its obligations hereunder and as required to comply with applicable laws or rules of any exchange upon which a Party's shares may be traded. Notwithstanding the foregoing, nothing contained herein shall be deemed to restrict or prohibit OCERS from complying with applicable law regarding disclosure of information, including the California Public Records Act and Contractor hereby agrees to release OCERS from any and all Losses related to any such disclosure.

2.9.7 Publicity. Contractor shall not use OCERS' name or insignia, photographs of OCERS property, or any publicity pertaining to the Services in any advertisement, magazine, trade paper, newspaper, television, or radio production, or other similar medium without the prior written consent of OCERS.

2.9.8 Non-Infringement. Contractor represents, warrants, and covenants that it will perform its responsibilities under this Agreement in a manner that does not

infringe, or constitute an infringement or misappropriation of, any patent, copyright, trademark, trade secret, or other proprietary rights of any third-party.

2.10 Subcontracting/Subconsulting.

2.10.1 Prior Approval Required. Contractor shall not subcontract any portion of the work required by this Agreement, except as expressly stated herein, without prior written approval of OCERS. Subcontracts, if any, shall contain a provision making them subject to all provisions stipulated in this Agreement. Contractor will be solely responsible for the payment of all subcontractors and other third parties engaged by or through Contractor to provide, perform, or assist in the provision and delivery of the Services.

ARTICLE 3
GENERAL PROVISIONS

3.1 Notices. All notices permitted or required under this Agreement shall be given to the respective Parties at the following address, or at such other address as the respective Parties may provide in writing for this purpose:

OCERS:

CONTRACTOR:

Orange County Employees Retirement System

2223 E. Wellington Avenue

Santa Ana, CA 92701

Attention: Jim Doezie

e-mail: jdoezie@ocers.org

Such notice shall be deemed made when personally delivered or when mailed, upon deposit in the U.S. Mail, first class postage prepaid and registered or certified addressed to the Party at its applicable address. Actual notice shall be deemed adequate notice on the date actual notice occurred, regardless of the method of service.

3.2 Equal Opportunity Employment. Contractor represents that it is an equal opportunity employer and it shall not discriminate against any subcontractor, employee, or applicant

for employment because of race, religion, color, national origin, ethnic group identification, mental disability, physical disability, medical condition, genetic information, marital status, ancestry, sex, gender, sexual orientation, gender identity, gender expression, age, or military and veteran status. Such non-discrimination shall include, but not be limited to, all activities related to initial employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff, or termination.

- 3.3 Time of Essence. Time is of the essence for each and every provision of this Agreement. The acceptance of late performance shall not waive the right to claim damages for such breach nor constitute a waiver of the requirement of timely performance of any obligations remaining to be performed.
- 3.4 OCERS' Right to Employ Other Contractors. OCERS reserves the right to employ other contractors in connection with the Services.
- 3.5 Successors and Assigns. This Agreement shall be binding on the successors and assigns of the Parties.
- 3.6 Assignment or Transfer. Contractor shall not assign, hypothecate, or transfer, either directly or indirectly (including by operation of law), this Agreement or any interest herein without the prior written consent of OCERS.
- 3.7 Amendment. This Agreement may not be altered or amended except in a writing signed by both Parties.
- 3.8 Waiver. All waivers under this Agreement must be in writing to be effective. No waiver of any default shall constitute a waiver of any other default or breach, whether of the same or other covenant or condition.
- 3.9 No Third-Party Beneficiaries. There are no intended third-party beneficiaries of any right or obligation assumed by the Parties.
- 3.10 Invalidity; Severability. If any portion of this Agreement is declared invalid, illegal, or otherwise unenforceable by a court of competent jurisdiction, the remaining provisions shall continue in full force and effect.
- 3.11 Governing Law; Venue. This Agreement shall be governed by the laws of the State of California. The exclusive venue for any dispute arising out of or relating to this Agreement shall be in Orange County, California.
- 3.12 Injunctive Relief for Breach. Contractor's obligations under this Agreement are of a unique character that gives them particular value; breach of any of such obligations will result in irreparable and continuing damage to OCERS for which there will be no adequate remedy at law; and, in the event of such breach, OCERS will be entitled to injunctive relief and/or a decree for specific performance, and such other and further relief as may be proper (including monetary damages if appropriate).

- 3.13 Attorneys' Fees. If either Party commences an action against the other Party, either legal, administrative, or otherwise, arising out of or in connection with this Agreement, the prevailing party in such litigation shall be entitled to have and recover from the losing party reasonable attorneys' fees and all other costs of such action.
- 3.14 Authority to Enter Agreement. Contractor has all requisite power and authority to conduct its business and to execute, deliver, and perform the Agreement. Each Party warrants that the individuals who have signed this Agreement have the legal power, right, and authority to make this Agreement and bind each respective Party.
- 3.15 Counterparts. This Agreement may be signed in counterparts, each of which shall constitute an original.
- 3.16 Integration. This Agreement represents the entire understanding of OCERS and Contractor as to those matters contained herein. No prior oral or written understanding shall be of any force or effect with respect to those matters covered hereunder. Neither Party shall be deemed to be the drafter of this Agreement and no presumption for or against the drafter shall be applicable in interpreting or enforcing this Agreement.
- 3.17 Interpretation. This Agreement has been negotiated at arm's length and between parties sophisticated and knowledgeable in the matters dealt with in this Agreement. Each Party has been represented by experienced and knowledgeable legal counsel. Accordingly, any rule of law (including, without limitation, California's Civil Code Section 1654) or legal decisions that would require interpretation of any ambiguities in this Agreement against the party that has drafted it shall not be applicable and are hereby waived. The provisions of the Agreement shall be interpreted in a reasonable manner to effectuate the purpose of the Parties and this Agreement.
- 3.18 Headings. Titles or headings are not part of this Agreement, are for convenience of reference only, and shall have no effect on the construction or legal effect of this Agreement.
- 3.19 Precedence. In the event of any conflict, inconsistency, or ambiguity between the terms and conditions in the main body of this Agreement and the terms and conditions in any exhibit, the main body of this Agreement shall control. This Agreement and all attached exhibits will be construed to be consistent, insofar as reasonably possible. When interpreting this Agreement, precedence shall be given to its respective parts and amendments in the following descending order:
- A. Amendments to this Agreement entered into pursuant to Section 3.7 herein.
 - B. This Agreement.
 - C. Exhibit A: Scope of Services, Exhibit B: Fee Schedule, and Exhibit C: Key Personnel.

D. OCERS Request for Proposal dated October, 2024 attached as Exhibit "D".

E. Contractor's Response to OCERS Request for Proposal, attached as Exhibit "E".

IN WITNESS WHEREOF, the Parties hereby have caused this Agreement to be executed on the Effective Date:

APPROVED:

APPROVED:

OCERS

[CONTRACTOR]

By:

By:

Name:

Name:

Title:

Title:

By:

Name:

Title:

EXHIBIT A

Scope of Services

Starting on the Effective Date, and continuing during the Term, Contractor will perform the Services in accordance with the terms of the Agreement. The Services consist of:

A consultant, under the supervision of OCERS Director of Internal Audit, will be expected to provide the following range of IT consulting/audit services to OCERS in regards to (1) IT General Controls (ITGC) and (2) Cybersecurity. The consultant will also provide (3) a high level review to support Internal Audit IT risk assessment, with the goal of assisting in the development of the IT internal audit plan for the next 1-3 years. The consultant will help build a multi-year IT audit program for OCERS Internal Audit Department based on an IT risk assessment using a format that is consistent with the format used by OCERS' Internal Audit Department.

The frequency and/or rotation of the audits in the audit plan will be tailored and customized based on OCERS' budget constraints and risk appetite. Future operational IT audits are subject matter specific audits that address operational IT risks and will also be identified in the multi-year audit program. The multi-year audit plan should include only audits typical for organizations the size of OCERS and for common operational IT risks that such an organization may face.

IT General Controls (ITGC)

- For the IT General Controls audit, build and develop an overall audit policy and audit procedures for IT general controls in collaboration with OCERS Internal Audit, OCERS management and OCERS external auditor. In addition, develop a risk controls matrix to identify controls that mitigate the corresponding ITGC risks. Build an audit program that tests the design and operating effectiveness of those controls, focusing on logical and physical security, IT operations, and software development and change management.

Cybersecurity

- For Cybersecurity, OCERS Director of Cybersecurity is early in the process of incorporating the NIST Cybersecurity Framework and the CIS Controls within OCERS. The consultant would act only in a review and advisory capacity to determine whether the controls established to date or in the near future are sufficiently designed to meet the control criteria and objectives. The consultant will provide observations and recommendations, and inquire with management for their assistance with future remediation.

Internal Audit IT Risk Assessment/Audit Program

- Assist in the development of the Internal Audit IT audit plan for the next 1 to 3 years by performing a high-level review in support of the Internal Audit risk assessment. A multi-year IT audit plan with operational IT audits would be identified as a result of the IT risk assessment.

EXHIBIT B

Fee Schedule*

1. **Fees and Expenses.** Contractor agrees to accept the compensation set forth in this Exhibit B as full payment for performing all Services, including all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the Services, for risks connected with the Services, and for performance by Contractor of all its duties and obligations under the Agreement. OCERS will pay the following fees in accordance with the provisions of this Agreement:
2. *The total compensation shall not exceed XXX Dollars (\$XXX.00) without written approval by OCERS.*
3. *[provision for expense reimbursement]*
4. **Payment Terms – Payment in Arrears:** Invoices are to be submitted in arrears to OCERS unless otherwise directed in this Agreement. Payment by OCERS will be net thirty (30) days after receipt and approval of an invoice in a format acceptable to OCERS.
5. **Payment – Invoicing Instructions:** Contractor will provide an invoice on Contractor’s letterhead for services rendered under this Agreement. Each invoice will have a number and will include the following information:
 - a. Contractor’s name and address
 - b. Contractor’s remittance address, if different from item #1 above
 - c. Contractor’s Taxpayer ID Number
 - d. Name of OCERS Agency/Department
 - e. Delivery/service address
 - f. Agreement number
 - g. Agency/Department’s Account Number
 - h. Date of invoice
 - i. Description and price of services provided
 - j. Sales tax, if applicable
 - k. Freight/delivery charges, if applicable
 - l. Total

Invoice and support documentation are to be forwarded to:

Orange County Employees Retirement System
2223 E. Wellington Avenue
Santa Ana, CA 92701
Attention: Accounts Payable
Email: Accountspayable@ocers.org

EXHIBIT C
Key Personnel

EXHIBIT D
Request for Proposal

EXHIBIT E

Response to Request for Proposal



November 22, 2024

Orange County Employees Retirement System

True transformation reaches far beyond everyday success. Explore IT audit and consulting solutions that move you forward.

Contents

PROPOSAL FORMS	2
EXECUTIVE SUMMARY	6
PROPOSAL REQUIREMENTS	7
FEEES	29
APPENDIX A: WRITING SAMPLES	31
APPENDIX B: CURRICULUM VITAE	91



We really appreciate your support through our journey and ALL that we were able to learn with you coaching and guiding us.

Vice president | Baker Tilly client



The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US, LLP and Baker Tilly Advisory Group, LP and its subsidiary entities provide professional services through an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable laws, regulations and professional standards. Baker Tilly US, LLP is a licensed independent CPA firm that provides attest services to clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and business advisory services to their clients. Baker Tilly Advisory Group, LP and its subsidiary entities are not licensed CPA firms.

Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, are independent members of Baker Tilly International. Baker Tilly International Limited is an English company. Baker Tilly International provides no professional services to clients. Each member firm is a separate and independent legal entity, and each describes itself as such. Baker Tilly Advisory Group, LP and Baker Tilly US, LLP are not Baker Tilly International's agent and do not have the authority to bind Baker Tilly International or act on Baker Tilly International's behalf. None of Baker Tilly International, Baker Tilly Advisory Group, LP, Baker Tilly US, LLP nor any of the other member firms of Baker Tilly International has any liability for each other's acts or omissions. The name Baker Tilly and its associated logo is used under license from Baker Tilly International Limited.



Proposal forms

November 22, 2024

Jim Doezie
Contracts, Risk & Performance Administrator
Orange County Employees Retirement System
P.O. Box 1229
Santa Ana, CA 92701

Baker Tilly Advisory Group, LP
11150 Santa Monica Blvd
Suite 600
Los Angeles, CA 90025
United States of America


T: +1 (310) 826 4474
F: +1 (310) 826 9188

bakertilly.com

Exhibit C

PROPOSAL COVER PAGE AND CHECK LIST (TO BE SUBMITTED IN FIRM'S LETTERHEAD)

Respondent Name: Chris Kalafatis

Respondent Signature: 

Respondent Address: 8219 Leesburg Pike Suite 800 Tysons, VA 22182

By submitting this response, the undersigned hereby affirms and represents that they have reviewed the proposal requirements and have submitted a complete and accurate response to the best of their knowledge. By signing below, I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements.

Respondent specifically acknowledges the following:

1. Respondent possesses the required technical expertise and has sufficient capacity to provide the services outlined in the RFP.
2. Respondent has no unresolved questions regarding the RFP and believes that there are no ambiguities in the scope of services.
3. The fee schedule submitted in response to the RFP is for the entire scope of services and no extra charges or expenses will be paid by OCERS.
4. Respondent has completely disclosed to OCERS all facts bearing upon any possible interests, direct or indirect, that Respondent believes any member of OCERS, or other officer, agent, or employee of OCERS presently has, or will have, in this contract, or in the performance thereof, or in any portion of the profits thereunder.
5. Materials contained in the proposal and all correspondence and written questions submitted during the RFP process are subject to disclosure pursuant to the California Public Records Act.
6. Respondent is not currently under investigation by any state or federal regulatory agency for any reason.
7. Except as specifically noted in the proposal, respondent agrees to all of the terms and conditions included in OCERS Services Agreement.
8. The signatory above is authorized to bind the respondent contractually.

PROPOSAL FORMS

Exhibit B

MINIMUM QUALIFICATIONS CERTIFICATION

All firms submitting a proposal in response to this RFP are required to sign and return this attachment, along with written evidence of how the respondent meets each qualification.

The undersigned hereby certifies that it fulfills the minimum qualifications outlined below, as well as the requirements contained in the RFP.

Minimum Qualifications include:

1. The auditor should have professional certifications such as CISA, CIA, CISSP, CRISC, or similar.
2. Minimum 7+ years of IT Audit experience: The auditor should have substantial experience in conducting both ITGC and Cybersecurity audits.
3. Experience in conducting risk-based ITGC audits: The auditor should use a risk-based approach in their audit methodology, focusing on areas with higher risks to the organization.
4. Experience conducting risk-based Cybersecurity audits: The auditor should adopt a risk-based approach, focusing on high-risk areas, critical assets, and potential vulnerabilities.
5. Familiarity with recognized security frameworks: The auditor should be proficient in assessing against the NIST Cybersecurity Framework and CIS Controls.
6. Ability to develop control matrices and test plans: Experience in designing and implementing IT control matrices and audit test plans for IT audits.
7. Proven track record in delivering audit reports: Ability to write clear, concise, and actionable audit reports suitable for presentation to senior management and audit committees.

The undersigned hereby certifies that they are an individual authorized to bind the Firm contractually, and said signature authorizes verification of this information.

Chris Kalafatis
Digitally signed by Chris Kalafatis
 Date: 2024.11.19 16:15:02
 +05'00'

11/22/2024

Authorized Signature

Date

Chris Kalafatis, Managing Director

Name and Title (please print)

Baker Tilly Advisory Group, LP

Name of Firm

PROPOSAL FORMS



**Secretary of State
Certificate of Qualification / Registration**

I, SHIRLEY N. WEBER, PH.D., California Secretary of State, hereby certify:

Entity Name: Baker Tilly Advisory Group, LP
Entity No.: 202461906539
Registration Date: 04/22/2024
Filing Type: Limited Partnership - Out of State
Formed In: DELAWARE

The above referenced entity complied with the requirements of California law in effect on the Registration Date for the purpose of qualifying to transact intrastate business in the State of California, and that as of the Registration Date, said entity became and now is duly registered, qualified and authorized to transact intrastate business in the State of California, subject however, to any licensing requirements otherwise imposed by the laws of this State and that the entity shall transact all intrastate business within California under the Entity Name as set forth above.

No information is available from this office regarding the financial condition, status of licenses, if any, business activities or practices of the entity.



IN WITNESS WHEREOF, I execute this certificate and affix the Great Seal of the State of California this day of April 29, 2024.

SHIRLEY N. WEBER, PH.D.
Secretary of State

Certificate No.: 205219627

To verify the issuance of this Certificate, use the Certificate No. above with the Secretary of State Certification Verification Search available at bizfileOnline.sos.ca.gov.



November 22, 2024

Jim Doezie
Contracts, Risk & Performance Administrator
Orange County Employees Retirement System

1150 Santa Monica Blvd
Suite 600
Los Angeles, CA 90025
T +1 (310) 826 4474
F: +1 (414) 777 5555
bakertilly.com

Delivered electronically

Dear Mr. Doezie:

You told us you're looking for a firm to provide a range of IT audit and consulting services including IT General Controls (ITGC) and cybersecurity, as well as a high-level review to support internal audit IT risk assessment, with the goal of assisting in the development of the IT internal audit plan for the next 1-3 years. This proposal is the starting point — our vision of how we can protect and enhance your enterprise value as we achieve your immediate goal to work with experienced practitioners who can support your agency's technical resilience.

We understand that for public sector agencies like Orange County Employees Retirement System (OCERS), the pursuit of excellence extends far beyond your mission to provide secure retirement and disability benefits with the highest standards. It also involves creating a robust framework for managing IT risks and safeguarding organizational assets. We're prepared to redefine what excellence means for OCERS, helping you navigate complex landscapes, ensure regulatory compliance using industry best practices and build trust within the communities you serve.

The approach and qualifications we've shared in our proposal show how important OCERS will be to us as a client. We can't wait to get started. Sincerely,

You are ready to step beyond the boundaries of everyday success. It's only natural. Leaders don't live in comfort zones. Neither do we. This is why there's limitless potential ahead of us when we join forces.

Chris Kalafatis, CPA, CIA, CFE, Managing Director
+1 (703) 923 8007 | Chris.Kalafatis@bakertilly.com

Madhu Maganti, CPA, CISA, M.S., Principal
+1 (346) 201 6024 | Madhu.Maganti@bakertilly.com

Executive summary

This is more than a proposal. It's a promise. To serve as your sounding board, your navigator and your second set of eyes on the horizon.

Driving the change you envision, from the word go

Our wheels were in motion from the moment we received your RFP about IT audit and consulting services. Based on what we've learned from you, we understand that OCERS is seeking a firm to provide a range of IT audit and consulting services including IT General Controls (ITGC) and cybersecurity, as well as a high-level review to support Internal Audit IT risk assessment, with the goal of assisting in the development of the IT internal audit plan for the next 1-3 years.

So, let's get to it. Our proposal includes the details of everything we'll bring to OCERS. Here are the highlights:

WE KNOW THE PUBLIC SECTOR

State and local government is an industry of focus at Baker Tilly. Serving organizations like OCERS is central to what we do, and we never rest in our work to take the industry forward. You'll see our public sector team actively engaged with state and national associations to stay at the forefront. This makes us even more effective at helping you implement regulations and adopt new standards, processes or technologies, all while bringing solutions that address the complexities and obligations of government and your unique opportunities within it.

GOING BEYOND IS WHAT WE DO

There's little value in checking boxes. We're driven to make a real difference for OCERS. Expect highly competitive fee estimates and the highest level of service from seasoned principals and managers: Pushing above and beyond your requirements and expectations. Bringing insights. Improving efficiencies. Achieving your objectives. Then identifying even greater possibilities. Every day, you'll experience value-added education and consistent communication that reflects how important your organization is to us.

WE'RE ON THIS JOURNEY TOGETHER

Our industry-focused, advisory-based and communication-centric audit approach is considerate of your internal team at every step. We offer a creative and flexible structure in which the right people perform the right work at the right time — for the right price. Our risk-based model aligns with our deep understanding of OCERS' business, industry, size, ownership structure and internal controls.

Proposal requirements

As your guide, we champion your goals, anticipate your challenges and pioneer new territory together.

A description of the respondent including:

- a. Brief history, including year the respondent firm was formed.*
- b. Ownership structure.*
- c. Office locations.*
- d. Organization chart.*
- e. Number of employees.*
- f. Annual revenues.*
- g. Scope of services offered.*
- h. Respondent's specialties, strengths, and limitations*

Upholding tradition while focusing on what's ahead

Where we've been and where we're going with OCERS

We started by planting strong roots. From there, we never stopped growing. It was in **1931** — the height of the Great Depression — in Waterloo, Wisconsin, where Ed Virchow began providing audits to Midwestern canning companies that helped feed our nation. He built much more than a public accounting firm. He built a culture of innovation where we find new and better ways to work.

Since then, we have grown to encompass 50 different business combinations, each with its own rich history. We have augmented our scope across industries, services and areas of expertise to better serve our clients and have expanded our reach from coast to coast and around the globe.

What hasn't changed? Our dedication. Our values. And our passion for enhancing our clients' organizational impact. That legacy continues with our service to OCERS. **With over 90 years** of experience providing services similar in size and scope to those requested in this RFP, we've honed our skills and adapted to evolving markets.

Detailing our firm's governance and leadership structure

In June 2024, Baker Tilly accepted a strategic investment from private equity firms Hellman & Friedman and Valeas Capital Partners, resulting in an organizational restructuring to ensure compliance with professional regulations. Baker Tilly US, LLP and Baker Tilly Advisory Group, LP and its subsidiary entities provide professional services through an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable laws, regulations and professional standards. Baker Tilly US, LLP is a licensed independent CPA firm that provides attest services to clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and business advisory services to their clients. Baker Tilly Advisory Group, LP and its subsidiary entities are not licensed CPA firms.

Baker Tilly, Advisory Group LP is a limited partnership, and our board and consulting leadership are structured as shown on the following page:

PROPOSAL REQUIREMENTS

Baker Tilly Advisory Group, LP Board



Blake Kleinman
Chair
Hellman & Friedman



Chuck Droege
Chief Operating Officer
Baker Tilly



Jeff Ferro
Chief Executive Officer
Baker Tilly



Fred Jackson
Hellman & Friedman
LLC



Theresa Meiners
Chief Risk Officer and
General Counsel
Baker Tilly



Tarim Wasim
Hellman & Friedman
LLC



Ed Woiteshek
Valeas Capital Partners

BAKER TILLY ADVISORY GROUP'S BOARD

Baker Tilly's top leaders empower our success and support our growth-driven culture.

The organizational structure of our firm's consulting leadership



Angie MacPhee
Managing Principal



Heather Acker
Managing Principal
Risk Advisory



Ann Blakely
Managing Principal
Digital Solutions



Todd Carpenter
Managing Principal
Development &
Community Advisory



Cary Mallandt
Managing Principal
Corporate Finance
& Forensics



Katherine Strong
Senior Executive Assistant



Becky Holmes
Managing Director
Business Management Lead
Corporate Finance
& Forensics &
Risk Advisory



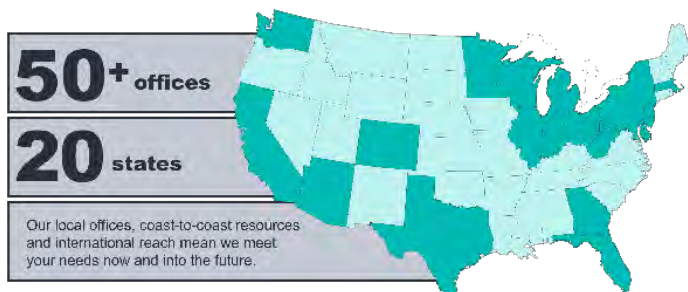
John O'Connor
Managing Director
Business Management Lead
Development & Community
Advisory &
Digital Solutions

Spanning the nation and the globe with our resources for you

OCERS will have access to resources in more than 50 U.S. Baker Tilly office locations across 20 states and international office locations. This means wherever you do business and wherever your business grows — across the nation or around the globe — you'll have a team of specialists who know the

PROPOSAL REQUIREMENTS

landscape and can help you achieve your goals in compliance with the local laws and regulations.



DELIVERING COAST-TO-COAST AND GLOBAL EXPERTISE FOR OCERS

With offices in 20 U.S. states and clients in all 50 states, we provide the right resources to meet any challenge, across the nation and around the globe.

Guiding you with our resources, reputation and reach

Baker Tilly consulting at a glance

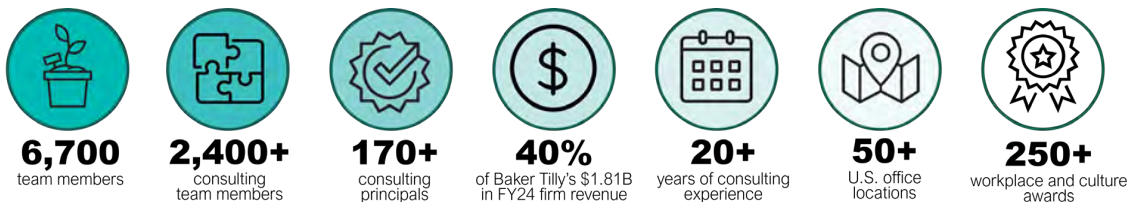
Making decisions today to shape tomorrow is especially challenging in these extraordinary times. OCERS requires a firm with consulting specialists who combine functional experience, industry knowledge and technical expertise to respond to your immediate needs and support you as your agency evolves.

Baker Tilly is that firm. We pay special attention to the intersection of strategy and execution to deliver:

- **Innovative and pragmatic approaches** for assessing changes, adapting quickly, implementing best practices and competing in any environment
- **Services to enhance and protect the enterprise value** you have worked so hard to achieve
- **Strategies** to identify and mitigate potential risks
- **Solutions** for your toughest challenges

When you work with Baker Tilly on your advisory needs, you work alongside an agile team that drives transformation by supporting you with a flexible engagement model “right sized” to your unique culture and circumstances. We dedicate ourselves to delivering industry insights, efficiencies, creativity, flexibility and forward-thinking ideas every step of the way.

More than anything, OCERS will receive an exceptional experience for your management team, governance team, internal process owners and — ultimately — the citizens you serve. Below are some key facts about our consulting practice, including the depth of resources that stand ready to support your core project team:



GIVING YOU THE TOOLS YOU NEED TO NAVIGATE THE FUTURE

Baker Tilly will successfully guide OCERS through changing landscapes with skills, stability and strength as one of the oldest and largest advisory, assurance and tax firms in the United States.

PROPOSAL REQUIREMENTS

Investing our resources in California

Your population is the largest in the United States and growing. You have the fifth-largest economy in the world, boasting a diverse range of industries and businesses. We're proud to be growing right alongside you. For Baker Tilly, expanding client relationships, a burgeoning local presence and an understanding of your state's unique markets are escalating our growth in the Golden State.

Baker Tilly has more than 800 professionals across nine California locations here for you. For OCERS, that means exceptional service from a local team passionate about protecting and enhancing your value and standing ready to draw on our broad national resources as your goals or needs evolve.



COVERING MORE OF THE CALIFORNIA MAP TO SUPPORT OCERS

When OCERS wants a team with an in-depth understanding of economic conditions, knowledge of regional and state regulations and local assistance, you won't have to go far.

Holding a steady financial course, onward and upward

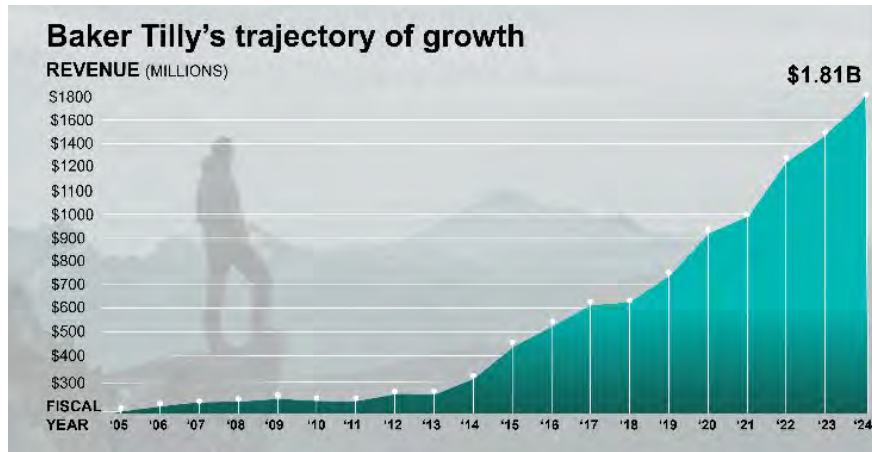
Seeing where a firm has taken itself can be a good indicator of where it can take you. When choosing a firm that you will be able to rely on for the long-term, financial stability and resources are an immense consideration.

Baker Tilly is a privately held company and partnership and does not distribute financial information without a properly signed non-disclosure agreement. In an effort to satisfy financial disclosure requirements for proposals, we do provide five years of consolidated net revenue. This financial information is available publicly and included below. Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, operate under an alternative practice structure and are members of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. Baker Tilly US, LLP is a licensed CPA firm that provides assurance services to its clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and consulting services to their clients and are not licensed CPA firms.

PROPOSAL REQUIREMENTS

Our financial path has been heading steadily in one direction: upward. Consistent growth in revenue and a diversified client base give Baker Tilly the stability and resources to serve OCERS' long-term needs. You can also see our level of financial stability and strength in key facts like these:

- Baker Tilly ranks as the 10th-largest accounting firm in the United States, according to [INSIDE Public Accounting's 2024 list of Top 500 Firms](#)
- Baker Tilly serves tens of thousands of publicly traded and privately held clients ranging in size from \$1 million to billions of dollars in revenues
- Baker Tilly has never filed for bankruptcy



A STEADY AND STRATEGIC CLIMB IN FINANCIAL STRENGTH

Our firm's steady growth through the years has been built both organically and through strategic combinations.

Highlighting the capabilities of our national risk advisory practice

The best way to address risk is to see it coming — and act before it affects your business. That's the mission of our national risk advisory practice, where **more than 370 members** will proactively address organizations' strategic, operational, financial and general business risks.

We collaborate with organizations' management and leaders, internal audit functions, boards and audit committees to address areas of strategic importance, keeping your organization's unique culture in mind. As shown on the following page, our suite of risk advisory services includes:

PROPOSAL REQUIREMENTS



BRINGING OCERS THE POWER OF A FULL RANGE OF RISK ADVISORY SERVICES

We'll collaborate with you to proactively identify organizations' areas of strategic importance, then tailor our services, fortifying your protection on every front. Attest services are provided by Baker Tilly US, LLP, a licensed independent CPA firm, and tax and advisory services are provided by Baker Tilly Advisory Group, LP.

IT audit capabilities

Decades of serving the public sector with IT audit and cybersecurity consulting support have allowed us to become familiar with the IT risks and threats that agencies like OCERS face. You can rely on our experience to help you reduce IT and cybersecurity risk to acceptable levels and ensure that your technology investments are secure, reliable, and effective in meeting the organization's needs. More than 850 clients of all sizes have leveraged our work to:

- Identify opportunities and manage risks associated with IT and cybersecurity
- Understand root causes of control deficiencies and implications of various remediation plans
- Identify the IT and cybersecurity risks relevant to their business and technical environments
- Align financial management requirements with technology investments
- Evaluate the confidentiality, processing integrity, and availability risks related to a wide variety of deployed technologies
- Better position IT and cybersecurity initiatives, processes, and systems to add value
- Develop dashboards to measure key performance metrics and identify trends
- Facilitate critical discussions about technology and cybersecurity risks with management and boards

PROPOSAL REQUIREMENTS

When recommending an IT solution for OCERS, expect us to carefully consider your culture, complexity, and strategic growth goals, assuring your team of right-sized, actionable recommendations to remedy known deficiencies and capitalize on opportunities for improvement. Our work as cybersecurity specialists and IT auditors has helped clients to attain benefits, including:

- More secure, reliable IT infrastructure and operations
- Increased operational efficiency and effectiveness
- Streamlined internal controls and reduced duplication in IT processes
- Enhanced internal controls emphasizing risk detection and risk mitigation
- Reduction of the potential for a single-point failure
- Optimized technology investments
- Quicker issue resolution
- Better strategic decision-making about IT and cybersecurity risk mitigation

Our professionals have served clients in a wide range of IT risk and cybersecurity engagements:

COMMON IT AUDIT AREAS	
<ul style="list-style-type: none"> • Application security IT governance and oversight • Architectural reviews IT internal controls testing • Breach response and preparedness IT operations • Board training IT risk assessment • Change management • Mobile device management and security • Cloud computing • Policies and procedure enhancement • Contract compliance security and network integration • Cybersecurity assessment • Data clarification server administration • Data security and privacy • Server configuration review 	<ul style="list-style-type: none"> • Disaster recovery, business continuity, and incident response • System access control • End point management • System backup and recovery • End user support • System development • Enterprise mobility • System implementations, changes, and upgrades • Identity and access management • Targeted phishing assessments • Incident and problem management • Vulnerability and patch management • Information privacy (including GDPR, HIPAA) • Vulnerability and penetration testing • Industry-specific compliance requirements • Web application testing

PROPOSAL REQUIREMENTS

Benefit from a highly credentialed and experienced team

More than **100 professionals** nationally at Baker Tilly specialize in providing cybersecurity and IT risk-related services to clients of all industries and sizes. Our team members perform over **100,000 hours** of technology and cybersecurity-related assessments annually, translating into a deep understanding of IT as a business enabler and experience that will inform our efforts to help OCERS in creating synergy and security for the agency.



Beyond hands-on experience, members of our larger Baker Tilly team have attained diverse relevant certifications which demonstrate the depth of their skills and qualifications to serve your cybersecurity and IT needs, including:

HIGHLIGHTING OUR TEAM MEMBERS' CREDENTIALS	
Certified Information Systems Auditor (CISA)	Certified Information Privacy Technologist (CIPT)
Certified Information Systems Security Professional (CISSP)	Certified Payment-Card Industry Security Manager (CPISM)
Certified Information Privacy Professional (CIPP)	National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) Certified Professional
Certified Cloud Security Professional (CSSP)	Symantec Certified Specialist (SCS +) for DLP
Certificate of Cloud Security Knowledge (CCSK)	International Organization for Standardization (ISO) Lead Auditor
Certified in Risk and Information Systems Control (CRISC)	International Organization for Standardization (ISO) Lead Implementer
Common Security Framework (CSF) Certified Professional	Certified Fraud Examiner (CFE)
Certified Information Technology Professional (CITP)	Certified Internal Auditor (CIA)
HITRUST Certified CSF Practitioners (CCSFP)	Certified Public Accountant (CPA)

PROPOSAL REQUIREMENTS

WHAT DO WE BRING TO THE TABLE?



A cohesive team with cybersecurity and IT audit expertise: OCERS will have a team of highly specialized resources to assess and test your information security infrastructure, risks and controls. Baker Tilly's **more than 100** qualified cybersecurity and IT risk professionals have combined technical training with hands-on experience in completing cybersecurity, IT audit and consulting engagements for clients in diverse industries. Demonstrating their expertise, team members also hold a variety of certifications, as detailed above.



Complementary industry and technical experience: In helping companies like OCERS identify vulnerabilities and inefficiencies and mitigate IT-related risks, we draw from a deep understanding of the transportation and extensive experience in working with similar companies to more effectively manage cybersecurity risks and reduce the likelihood and impact of an exposure.



An understanding of security risks in the context of your business: Effective cybersecurity management requires a holistic perspective on potential threats and associated risks across the entire company — beyond just the IT department. As experienced consultants and auditors, we understand how to address security risk within the context of business risk. We start by working with your personnel to gain a complete picture of their unique operations, cybersecurity control environment and applicable regulatory requirements. Then we provide practical guidance based on lessons learned and **leading cybersecurity frameworks** such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27000/27001 and many more.



Practical and cost-effective strategies to mitigate risk: Our services focus on proactively identifying risk mitigation strategies that are pragmatic, actionable and cost-effective. We understand the importance of “right-sizing” our approach and recommendations to meet your unique staffing and budgetary constraints. Our integrated cybersecurity management approach helps clients safeguard information assets by reinforcing protection while ensuring critical business operations are not disrupted.

PROPOSAL REQUIREMENTS

Additional qualifications: our work in the public sector

Baker Tilly has served state and local governments since our establishment more than 90 years ago. We are one of the few advisory, tax and assurance firms with a practice dedicated entirely to serving governmental clients.

Unlike many other firms, Baker Tilly is organized by industry, not service line. What does this mean for OCERS? It means you will be served by a carefully selected team that blends our government-focused professionals with experienced specialists in the activities of your agency. OCERS will work with a knowledgeable team that understands your specific challenges and provides innovative solutions to help you overcome them.



State and local government is a complex, unique environment shaped by fiscal, regulatory and operational considerations not found in other industries. Recognizing this complexity and eager to serve as a true valued advisor to the public sector, Baker Tilly formalized its dedicated public sector specialization more than 50 years ago. **Today, more than 350 Baker Tilly professionals — including nearly 30 principals** — focus directly on serving governments and provide hundreds of thousands of client service hours annually to agencies like OCERS.

Nationwide, our public sector practice serves nearly **4,000 state and local governmental entities**, including counties, municipalities, school districts, utilities, transit organizations, airports and special authorities. Several of these client groups are now served by dedicated specialists in distinct sub-practices.

Public sector: Experience that matters



4,000 public sector clients



90+ years of industry experience



Serving clients nationwide

COMMITMENT TO THE PUBLIC SECTOR

Baker Tilly has been in business for more than 90 years, and public sector entities were some of our first clients.

PROPOSAL REQUIREMENTS

Serving large governmental entities

Baker Tilly will bring OCERS deep experience serving large governments across the nation. The following is a representative list of our recent audit and advisory clients, which includes a diverse array of high-profile public-sector entities — state agencies, local governments, public utilities, transits and K-12 school districts.

REPRESENTATIVE LIST OF OUR PUBLIC-SECTOR CLIENTS

- | | | |
|--|---|---|
| <ul style="list-style-type: none"> • Anaheim Public Utilities, CA • Austin Energy, TX • Baltimore County, MD • Burbank Water and Power, CA • Champaign County, IL • City of Baltimore, MD • City of Burbank, CA • City of Chicago, IL • City of Dallas, TX • City of Fort Worth, TX • City of Highland Park, IL • City of Houston, TX • City of Kansas City, MO • City of Long Beach, CA • City of Madison, WI • City of Milwaukee, WI • City of Minneapolis, MN • City of Rochester, NY • City of San Antonio, TX • City of Santa Clara, CA • City of Seattle, WA • City of St. Paul, MN • City Public Service of San Antonio, TX • Colorado Springs Utilities, CO • Dallas Independent School District, TX • Detroit Water and Sewerage Department, MI | <ul style="list-style-type: none"> • DuPage County, IL • Forest Preserve District of Cook County, IL • Great Lakes Water Authority, MI • Hennepin County, MN • Illinois Department of Commerce & Economic Opportunity • Illinois Department of Technology and Innovation • Illinois Housing Development Association • Illinois Racing Board • Illinois Tollway • Independence Power & Light, MO • Kane County, IL • Lake County, IL • Las Vegas Valley Water District, NV • Long Island Power Authority, NY • Los Angeles Unified School District, CA • Lower Colorado River Authority, TX • McHenry County, IL • Memphis Light, Gas and Water, TN • Metra (Chicago transit), IL | <ul style="list-style-type: none"> • Milwaukee County, WI • New York City Board of Education Retirement System • Northern California Public Power Agency • Oklahoma Municipal Power Authority • Orlando Utilities Commission, FL • Pace Suburban Bus, IL • Pasadena Water & Electric, CA • Rockford Public Schools, IL • Sacramento Municipal Utility District, CA • San Antonio Water System, TX • San Diego Gas & Electric, CA • Seattle City Light, WA • State of California • State of Illinois • State of Indiana • State of Maryland • State of Ohio • State of Oregon • State of Virginia • State of Wisconsin • University of Illinois • University of Wisconsin • Will County, IL • Yolo County, CA |
|--|---|---|

Many of our senior-level practice professionals bring a combination of large-firm consulting and industry-based experience to your engagement. We combine their diverse expertise in a personalized delivery model for OCERS, working side by side with your team and your unique culture. While our consulting practice brings you significant depth of public sector expertise, we also draw on leading practices gained across many other industry segments. We provide proven, practical solutions through comprehensive, firmwide resources, benefiting OCERS in the following ways:

PROPOSAL REQUIREMENTS

- **Specialized training and continuing education:** OCERS can rely on a team with the necessary knowledge and skills you desire to provide professional services.
- **Dedication to state and local government:** Baker Tilly team members live and breathe government, working in your industry year-round. This translates into insights only experience can bring. Our team effectively communicates with public-sector entities and private-sector organizations, enabling collaboration between all stakeholders.
- **Knowledge sharing with OCERS:** We keep our public-sector clients informed with crucial thought leadership in the form of webinars, workshops, articles, regular newsletters, our CommunitIES podcasts and a diagnostic tool for government clients.
- **Regular consultations at no additional cost:** Throughout our relationship, we will be available for routine meetings and calls for technical questions, connecting you with recommendations and ideas to address any operational issues that may arise.

Demonstrating our ability via similar projects

By highlighting our expertise through comparable projects, Baker Tilly assures OCERS that we will utilize this knowledge to understand your distinct culture and needs, delivering customized and adaptable IT audit and consulting services.

IT AUDIT AT A HOUSING SERVICES ORGANIZATION	
Our client's need	A not-for-profit organization sought a risk assessment of its IT function and operating environment. Specifically, they wanted a review of their current state systems and processing environment and consultative feedback that identified areas of risk and recommended opportunities for improvement.
Baker Tilly solution	Our two-phased approach was tailored to the organization's operating environment and needs. First, Baker Tilly worked with the client to perform a thorough evaluation of their infrastructure, interviewing key personnel and reviewing documentation to gain a high-level understanding of IT systems. Then, we analyzed results and risks were grouped into key areas, which were then prioritized based on importance to the organization.
Results achieved	Once the analysis was completed, Baker Tilly issued a report to the client that broke down the strengths and weaknesses of the then-IT governance model. Areas for improvement included data management, information security, security awareness and training. Based on the client's resources and objectives, Baker Tilly also developed a prioritized remediation roadmap with costs was presented for board approval. The first remediation project, a comprehensive policy update project, is now underway.
IT AUDIT	
Our client's need	When a county's information technology (IT) director retired, the municipality needed assistance identifying and hiring a replacement. Once the new IT director was hired, the county had to turn its attention to addressing IT controls that had not been prioritized during previous years' audits.

PROPOSAL REQUIREMENTS

IT AUDIT	
Baker Tilly solution	Baker Tilly had previously served the county and was familiar with the challenges the IT department faced and with management's vision for its future. We helped the county enhance its executive recruitment process and hire a qualified and experienced IT director. Thereafter, Baker Tilly's public sector and cybersecurity specialists supported the new director by completing a cybersecurity assessment to evaluate the county's people, tools and processes and determine whether they were meeting the county's needs and objectives. We then built a cybersecurity program to address cyber risks realized in the assessment.
Results achieved	Within three months, the county had a smoothly operating cybersecurity program to identify risk and prevent cyber-attacks. The county now has a strong IT environment.

CYBERSECURITY ASSESSMENT FOR A STATE AGENCY	
Our client's need	A state-run tollway needed assistance in performing a variety of cybersecurity and compliance assessments, including reviewing their overall cybersecurity program, performing penetration testing to evaluate the effectiveness of their IT processes, and performing a readiness assessment to ensure they were compliant with payment card industry (PCI) security practices.
Baker Tilly solution	<p>Baker Tilly worked with the tollway to perform a cybersecurity assessment utilizing the NIST Cybersecurity Framework (CSF). The assessment included interviews with the tollway's IT and security team members to review current capabilities across people, process, and technology. Deliverables included a detailed report describing our observations and recommendations and three-year roadmap and security strategy.</p> <p>In addition to the cybersecurity assessment, Baker Tilly performed external penetration testing and internal vulnerability scanning against the tollway's segmented networks. The goal of these tests was to validate that the tollway's IT operations were effectively patching and remediating known vulnerabilities among networking devices, servers, and end user computers. Our report provided a high-level overview of our testing activities, observations, and recommendations as well as detailed technical findings and recommended remediation steps.</p> <p>Finally, Baker Tilly performed a PCI readiness assessment to ensure the tollway was following the control requirements set forth in the PCI Council's Data Security Standards. Baker Tilly performed interviews, gathered relevant documentation, and identified gaps between current control processes and PCI requirements. Our report outlined our observations, identified gaps, and provided recommendations to support the tollway in closing those gaps in order to maintain PCI compliance.</p>
Results achieved	The tollway was able to identify a variety of improvement areas to its IT and security programs to ensure its environment remains secure and the services it provides are available when needed.

PROPOSAL REQUIREMENTS

NIST FRAMEWORK MATURITY ASSESSMENT	
Our client’s need	A company wanted an assessment of its current information security processes, controls and infrastructure, specifically regarding its compliance with key regulations, standards and frameworks, including NIST.
Baker Tilly solution	Baker Tilly sought to gain an understanding of the company’s current security posture. This entailed an in-depth document review, including 32 published policies, standards and procedures, as well as more than 40 interviews with key personnel.
Results achieved	Findings from the research phase were used to develop a roadmap, which included a defined set of projects to treat risk areas and improve security posture at the company. Baker Tilly’s recommendations included a deeper integration of data protection into operations, improvements to the communication of cybersecurity risks and the creation of an incident response strategy. Recommendations were broken into a series of key tasks and a suggested timetable for executing these recommendations — based on the company’s resources — were also offered.

CITY-WIDE CYBERSECURITY ASSESSMENT AGAINST NIST CSF	
Our client’s need	A large organization sought an assessment of their cybersecurity environment to identify risks. Additionally, the client needed guidance to optimize their future cybersecurity and IT investments and help with identifying recommended future audits.
Baker Tilly solution	Baker Tilly performed a cybersecurity governance assessment to review the organization’s activities as compared to leading practices, business objectives and regulatory requirements. Using the NIST CSF Framework as a foundation for our assessment, we comprehensively examined the cybersecurity environment, examining budget, staffing, policies and procedures, data risk management and third-party/vendor risks. Working with the chief internal auditor, we reviewed documentation and conducted interviews with relevant staff to understand the governance approach and identify gaps relative to NIST. Based on our cyber governance and NIST gap assessments, we also developed recommended future audits for an audit plan.
Results achieved	The client received a report condensing Baker Tilly’s findings, analysis and recommendations. In summary, we concluded that the organization had made positive strides in recent years by investing in cybersecurity leadership and tools. However, the current governance structure did not meet the standards of NIST CSF or of comparable organizations, so we recommended an array of improvements. Specifically, we advised the client to define its cybersecurity priorities more clearly, to invest in a security information and event management (SIEM) system and two-factor authentication applications, and to create new positions in the Information Security Office focused on governance, risk management and compliance.

Specialties, strengths and weaknesses


As demonstrated above, we are confident in our ability to meet the requirements of your RFP without any limitations. As seen below in our [service expertise](#), we assure OCERS that we have the capabilities and resources necessary to achieve your goals today, tomorrow and in the future.

PROPOSAL REQUIREMENTS

The names and qualifications of the staff that will be assigned to OCERS work, including a detailed profile of each person's background and relevant individual experience.



Providing information technology audit and consulting support and uncovering opportunities along the way

Meet the IT audit and consulting support team we've assembled to achieve everything you envision. Led by our public sector leader, **Chris Kalafatis**, this team was selected intentionally for OCERS' goals, is backed by our specialized resources and is comprised of collaborative and multidisciplinary individuals. Their passion for the public sector industry will make them an unstoppable force on your behalf. You'll find their bios below, and Curriculum Vitae in **Appendix B**.

INTENTIONALLY SELECTED ENGAGEMENT TEAM FOR OCERS		
	Chris Kalafatis, CPA, CIA, CFE— Managing director	
	Engagement role: Public sector leader	Experience
	<p>Chris has 25+ years of audit and consulting experience and leads Baker Tilly's public sector industry within the firm's Risk Advisory practice. Chris and his team's primary service offerings include internal audit, IT audit, and other process improvement or IT consulting projects.</p>	<ul style="list-style-type: none"> • Has directly served 50+ public sector entities • Leverages extensive familiarity with and understanding of state and local government agency operations to support engagement teams in quickly and thoroughly addressing engagement objectives and tailoring service delivery to the agencies' unique operating constraints


PROPOSAL REQUIREMENTS


INTENTIONALLY SELECTED ENGAGEMENT TEAM FOR OCERS

Madhu Maganti, CPA, CISA, M.S. — Principal		
	Engagement role: Engagement principal	Experience
	<p>Madhu is a goal-oriented cybersecurity/IT advisory leader with more than 20 years of comprehensive experience leading high-performance teams with a proven track record of continuous improvement toward objectives. He will oversee the entire engagement to ensure OCERS receives a seamless and well-planned engagement process, valuable solutions and technically accurate final deliverables to achieve your goals. Madhu is committed to the OCERS' success and satisfaction with our services; he will collaborate with you and the team to meet your deadlines and exceed expectations.</p>	<ul style="list-style-type: none"> Principal-in-charge on risk-based engagements, including cybersecurity risk assessments, HIPAA compliance, GDPR/CCPA compliance, SOX compliance, business process improvement, international restructuring, SOC-2 attestation and other information security related services Managed end-to-end NIST/ISO assessments for clients in energy, healthcare, finance, higher education and technology As a fractional CISO, streamlined operations and developed a robust information security environment for several SMBs
Peter Tsengas, CISA, CISM — Senior manager		
	Engagement role: Engagement manager	Experience
	<p>Peter will lead IT audits for OCERS. He has 25+ years of IT audit and IT risk and compliance consulting experience with three top 10 firms, and industry experience in the public sector and Fortune 500. He stays current on new industry technologies, risks, and regulatory compliance requirements and is dedicated to helping public sector clients identify, prioritize and remediate technology and cybersecurity-related risks.</p>	<ul style="list-style-type: none"> Led and supervised IT risk and compliance projects with 40+ public sector entities, including IT security audits for sensitive systems and independent assessments for third-party cloud hosted sensitive systems, to assess compliance with industry best practice standards such as NIST (Publication 800-53 and NIST Cybersecurity Framework) Led and supervised multiple annual IT audits for internal audit outsourced public sector clients

PROPOSAL REQUIREMENTS



INTENTIONALLY SELECTED ENGAGEMENT TEAM FOR OCERS

	Stacey Gill, CIA, CISA — Senior manager	
	Engagement role: Relationship manager	Experience
<p>Stacey has 15 years of experience providing risk advisory, business process improvement and compliance-based consulting services to public sector clients. Leveraging her expertise in internal audit and risk management, she supports clients by collaboratively executing audit activities including enterprise risk assessment, annual audit plan development, audit execution, remediation follow-up and reporting to audit committees. Stacey will support Madhu and the team in ensuring an efficient, value-driven engagement for OCERS.</p>	<ul style="list-style-type: none"> • Extensive service to public sector organizations, including state agencies, utilities and municipal governments • Leads outsourced and co-sourced internal audit services including financial audits, compliance audits, operational audits, information technology audits, performance audits and advisory projects • Manages business process and IT general controls reviews 	

	Andrew Kennedy, CISA — Manager	
	Engagement role: Engagement manager	Experience
<p>Andrew will oversee audit activities and tasks to assist the team in delivering timely, valuable outcomes for OCERS. He specializes in compliance-based and risk-driven assessments with a strong focus on cybersecurity and data privacy, collaborating with clients, delivering high-quality results and valuable insights, and providing long-term strategies that benefit the organization holistically as well as operationally. Andrew's experience encompasses service to entities in a wide variety of industries.</p>	<ul style="list-style-type: none"> • Supports clients developing sound IT management policies and practices • Provides recommendations to enhance financial and IS internal control environments • Leads process improvement and control implementation projects • Supports compliance and risk mitigation efforts 	

PROPOSAL REQUIREMENTS

INTENTIONALLY SELECTED ENGAGEMENT TEAM FOR OCERS

	Valentine Acqua — Senior Consultant	
	Engagement role: Testing specialist	Experience
	Valentine as experience in compliance and risk advisory engagements related to information systems and internal controls over financial reporting. He will assist with day-to-day IT audit tasks such as controls testing, documentation reviews, interviews and walkthroughs, drafting reports and ensuring timely communication and collaboration.	<ul style="list-style-type: none"> Executes NIST cybersecurity assessments and provides recommendations for improvement Assists with controls testing and audit planning Evaluates internal controls for IT risks that could impact financial reporting, system security and/or IT operations
	Staff and subject matter specialists, as needed	
	Baker Tilly staffs a deep bench of practitioners with extensive, direct experience in each of the audit areas in scope. As needed, we will identify and assign appropriate resources to support specific engagement objectives.	

OCERS WILL RECEIVE TANGIBLE RESULTS WITH BAKER TILLY

All engagement team members are committed to the OCERS' success. Their industry experience and business process controls expertise translate into tangible results

At least three (3) references for which the respondent has provided services similar to those included in the Scope of Services. Please include for each reference the individual point of contact, a summary of the work performed, and the length of time the respondent provided each service.

Demonstrating that we've been down this path before

The experiences of our clients speak more to Baker Tilly's capabilities than any proposal ever could. That's why we encourage you to talk with our clients. Here are a few individuals who welcome the opportunity to share their Baker Tilly experience.

NYC BOARD OF EDUCATION RETIREMENT SYSTEM

Name	Iyekeze Ada Ezefili	Title	Internal Audit Director
Phone	+1 (929) 305 3861	Email	iezeffili@bers.nyc.gov
Services	Baker Tilly assisted in internal audit start-up, including drafting an internal audit charter, drafting job descriptions, compiling internal audit policies, and researching internal audit technology. Baker Tilly performed the initial risk assessment, drafted a multi-year internal audit plan and thereafter has performed all audits within the audit plan.		
Project dates	Multi-year engagement, ended in 2024		

MAXI-LIFT, INC.

Name	Jim Rowell	Title	CFO
Phone	+1 (469) 801 2131	Email	jrowell@maxilift.com

PROPOSAL REQUIREMENTS

MAXI-LIFT, INC.	
Project description	NIST CSF assessment, external penetration test, internal vulnerability scan, a review of the credit card processing security against PCI requirements, a review of the BC/DR capabilities, and a review of the cloud architecture and security controls.
Project dates	Ongoing

LANDMARK MANAGEMENT GROUP			
Name	Pradeep Nair	Title	CTO/CIO
Phone	+1 (972) 202 4345	Email	pradeep.nair@landmarktx.com
Project description	Cybersecurity strategic consulting services, including cyber risk assessments, data flow mapping, penetration testing, and network security assessments.		
Project dates	Ongoing		

SOUTHERN UTE INDIAN TRIBE			
Name	Brian Bex	Title	Director of Internal Audit
Phone	+1 (970) 563-2310	Email	bbex@southernute-nsn.gov
Project description	Internal audit outsourced services, including IT and cybersecurity assessment services.		
Project dates	Ongoing		

EXPERIENCE MATTERS. ESPECIALLY THE EXPERIENCE OUR CLIENTS RECEIVE
Connect with our clients to learn more. Additional references are available by request.

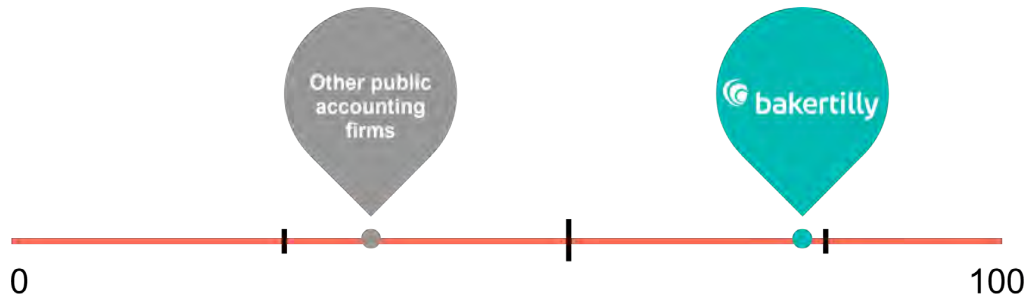
Don't just take our word for it; explore our industry-leading client satisfaction scores. When done right, exceptional service earns exceptional recognition. The proof of our client service quality lies in our metrics.

Net Promoter Score (NPS) is a metric used to gauge customer loyalty by asking how likely customers are to recommend a company to others. An NPS of over 50 is considered "excellent." In the accounting industry, the average benchmark is 41 according to a 2023 report by [ClearlyRated](#). **Baker Tilly consistently receives an NPS of greater than 65.** While that's unexpected in the advisory, tax and assurance world, it's what OCERS can expect from us — an experience that goes beyond what other firms deliver.

Your feedback is not a nice to have — it's necessary

With your feedback, we can make "our good better and our better best."

PROPOSAL REQUIREMENTS



LEADING BY EXAMPLE FOR THE CITY WITH OUR ABOVE-AVERAGE NPS

The ClearlyRated industry NPS benchmark for U.S. accounting firms is 41. Baker Tilly far surpasses this benchmark.

Client Satisfaction Score (CSAT) is another well-known metric. We consistently score well above the industry average of 82 (published by Retently - retently.com/blog/customer-satisfaction-score-csat/). This means that we bring the City one of the highest overall satisfaction scores in our industry.

Finally, in our annual client survey, 90% of respondents stated that Baker Tilly is a firm they trust; 88% acknowledged the relevance and consistency of our guidance; and 87% recognized our support in helping them navigate alternatives and avoid negative outcomes.

PROPOSAL REQUIREMENTS

Copies of any pertinent licenses required to deliver respondent's product or service (e.g., business license).

A copy of our business license can be found in the [proposal forms](#) section of our response.

An explanation of all actual or potential conflicts of interest that the respondent may have in contracting with OCERS.

Valuing independence — and ensuring it

The validity of the work we do for OCERS and the reputation of our firm all depend on one thing: upholding the independence standards that govern our profession.

This is a responsibility we hold paramount. We use multiple guard rails in the form of quality control policies and procedures to monitor our compliance. Each year, every staff member completes and signs representations on their compliance with independence policies and procedures.

Selected principals and managers verify compliance with independence requirements. We conduct firmwide conflict checks prior to accepting attest work for publicly traded companies. We also maintain a real-time list of companies where investments may be prohibited.

As part of OCERS' engagement planning process, we confirm the independence of your engagement team members, management-level personnel and other applicable individuals in the firm.

A description of all past, pending, or threatened litigation, including malpractice claims, administrative, state ethics, disciplinary proceedings, and other claims against respondent and/or any of the individuals proposed to provide services to OCERS.

Like most large accounting firms, Baker Tilly is periodically party to litigation and government inquiries but does not publicly disclose or discuss pending matters. However, we can affirm that we are not currently in litigation with OCERS or any of OCERS plan sponsor agencies. Additionally, we can also affirm that Baker Tilly has not given a gift or political campaign contribution to any officer, board member or employee of OCERS within the past twenty-four (24) months.

PROPOSAL REQUIREMENTS

Any other information that the respondent deems relevant to OCERS' selection process.

Working beyond your IT audit and consulting goals

We understand that the primary goal of this RFP is to provide IT audit and consulting services. However, our team is well positioned to support OCERS future needs as they continue to evolve. Our additional service offerings include:



Our service expertise
Our expertise extends beyond traditional consulting, accounting, tax and assurance

Tax

- Federal tax
- International tax
- State and local tax
- Transfer pricing
- Unclaimed property
- Research and development credits
- Tax advocacy and controversy services

Transactions

- Capital sourcing
- Investment banking
- Mergers and acquisitions
- Transaction advisory services
- Due diligence
- Project finance
- Strategy and management consulting

Assurance

- Employee benefit plan audit
- International audit
- Public company audit
- ASC 606 revenue recognition
- Lease accounting (ASC 842 and GASB 87)
- Sarbanes-Oxley (SOX) compliance
- Financial statement audit
- Internal audit
- IT audit solutions
- Outsourcing and managed services
- System and organization controls
- Single audits and federal

Consulting

- Bankruptcy and restructuring
- Corporate renewal and turnaround
- Complex disputes and litigation
- Fraud and forensic investigations
- Human capital
- Insurance qualification
- Staffing, recruiting and executive search
- Valuations
- CFO advisory and support
- Development advisory
- Forensic accounting
- Municipal advisory
- Government contracting

Risk advisory

- Board and audit committee governance
- Construction risk management
- Business continuity
- Cybersecurity
- Cybersecurity maturity model certification
- Privacy
- Relief funding assistance
- Disaster recovery
- Enterprise risk management
- Fraud and forensic investigations
- Internal audit
- IT audit solutions
- Grants administration and

International

- International audit
- International tax
- Transfer pricing
- Japanese services
- Chinese services
- Nearshoring services
- U.S. inbound services
- Global trade management

Digital services

- Application development
- Data solutions
- Enterprise solutions
- Cloud infrastructure
- Digital transformation

Private wealth

- Charitable giving and philanthropy
- Wealth management
- Family office
- Private client
- Ownership transition and exit strategies

Fees

When we say value, we mean achieving your objectives and imagining new ones. We mean sharing industry insights, gaining efficiencies and directing our best resources to OCERS.

An explanation of the pricing proposal for the scope of work, including pricing of fees and costs, billing practices, and payment terms that would apply.

Sharing our transparent fee estimate

OCERS fee estimate is based on what we've learned is important to you. We'll go beyond what's expected to deliver a return on your investment.

SERVICES FOR THE DEPARTMENT	FEES
Our scope of services will include the following:	
<ul style="list-style-type: none"> IT General Controls (ITGC) Audit 	
<ul style="list-style-type: none"> Cybersecurity Audit 	\$60,000.00
<ul style="list-style-type: none"> IT Risk Assessment / Audit Program Assistance 	
TOTAL FOR ALL SERVICES	\$60,000.00

OUR TRANSPARENT, FAIR FEE ESTIMATE

OCERS can expect a competitive fee arrangement and continuous value.

No unnecessary charges

You won't see add-on charges for routine calls, emails or quick consultations. They're included in our fees because we're here to earn your trust. If your need is out of scope, we'll never perform additional work unless you give us the go-ahead. Our final billing will always be based on the value we deliver to you.

Key assumptions

We based our fee estimate on your needs. If any of the assumptions below change, we'll share any new requirements, budgetary considerations and options.

ASSUMPTIONS	
<ul style="list-style-type: none"> Adequate support, preparedness, cooperation and feedback from management Administrative/technology fee (5% of the total fee amount) will be added to fees; you will not receive any hidden charges 	<ul style="list-style-type: none"> Fees based on current standards No major changes in scope or organizational structure, including mergers or expansions Organized books and records

Bringing you exceptional service and predictable invoicing

We're here for the long term, and we work hard to make sure the only surprises we bring you are good ones. It's why we won't bill you for routine phone calls, emails, questions or concerns. Instead, you'll receive regular, predictable and transparent billing. Baker Tilly proposes to invoice OCERS **every 30 days**, with invoice amounts due within 30 days of their submittal.

Taking intentional next steps toward your goals

You've reviewed our proposal. You've seen our passion for the public sector and OCERS' success.

When you choose Baker Tilly as your IT audit and consulting services provider, here's where we'll go next:

TOGETHER, FORWARD

1. Provide OCERS with an engagement letter, tentative transition plan and request lists
2. Hold a kickoff meeting to align expectations
3. Complete transition and begin client service plan
4. Build a lasting relationship and shape the future

YOUR TRANSITION WILL BE SMOOTH SAILING

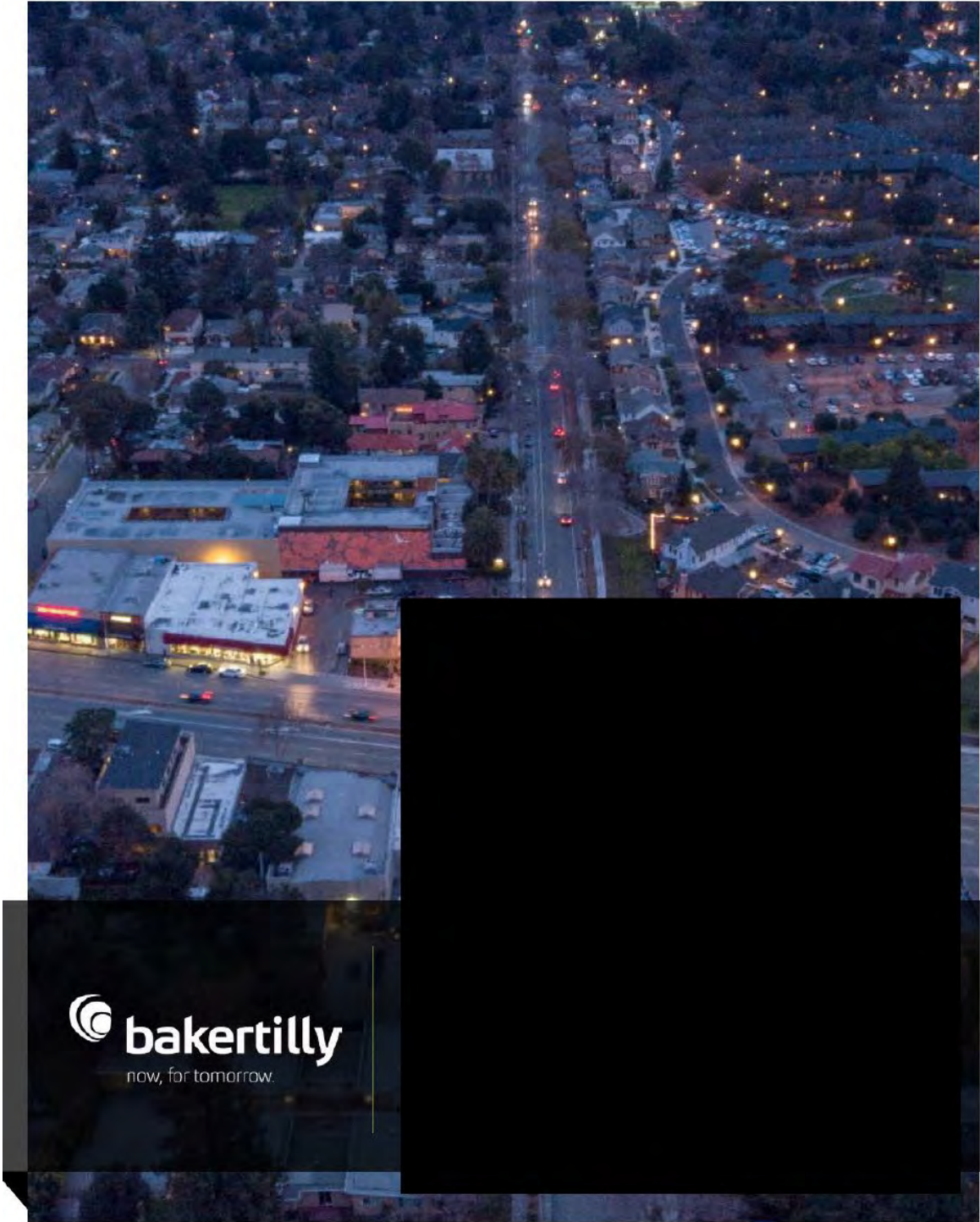
We bring a wealth of experience transitioning similar agencies and waive transition fees to minimize the impact on OCERS' time and resources.

Our dedication to OCERS starts now. If you need more information, call us any time. We'll gladly schedule time for your questions, your feedback and to help make your decision-making process easy.



Appendix A: Writing samples

APPENDIX A: WRITING SAMPLES



APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Audit Activity Types

OCA will conduct performance audits and perform financial/operational analyses of any City department, program, service, or activity as approved by the City Council in accordance with the Baker Tilly agreement.

Performance Audits

According to the Government Auditing Standards ([GAO-18-568G](#), Section 1.21 and 1.22, page 10-12), performance audits provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight with, among other things, improving program performance and operations, reducing costs, facilitating decision making by parties responsible for overseeing or initiating corrective action, and contributing to public accountability. Performance audits may include the following four (4) audit objectives:

- Program effectiveness and results
- Internal control design and effectiveness
- Compliance with laws, regulations, and policies
- Prospective analysis

Audit Planning Considerations

While maintaining its independence and objectivity in accordance with standards, the City Auditor considers a variety of matters when developing the Annual Audit Plan, including but not limited to:

- Risk assessment – OCA performed a risk assessment and summarized the results in a separate report (Task #2). Generally speaking, audit activities target high(er) risk areas. The results are shown the following page.
- Ability to add value – audit seeks to add value through independent and objective analysis.
- City Council – the City Auditor reports to the City Council and seeks input on audit priorities.
- Coverage and Prior Audits – the City Auditor considers prior audits conducted by OCA, the financial audit, and other audit and consulting reports recently issued.
- “Ripeness” and On-Going Initiatives – certain risk areas may be addressed through operational activities, which could mean they are not be ripe for audit to add value.
- Scheduling – the City Auditor takes into consideration the timing of an audit and other on-going initiatives that directly relate. Putting an undue burden on City staff may exacerbate the risk at hand or other interrelated risks.

APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Risk Assessment Results

The OCA performed a citywide risk assessment to plan for FY22 and FY23 audit activities and documented the methodology and the detailed results in a separate Risk Assessment Report. In summary, we identified the following areas rated as High or High-Moderate risks. In determining the audit activities to be performed in FY22 and in FY23, we further reviewed these risks and functional areas and considered the matters listed in the previous page.

Functional Area	Title	Likelihood (1-5)	Impact (1-5)	Score
City Wide	COVID-19 Response	5	5	50
Org Wide	Employee Retention & Succession Planning	5	4	46
Planning and Development Services	Long Range Planning	5	4	46
Information Technology	Disaster Recovery Preparedness and Testing	3	5	44
Information Technology	Host Intrusion and Malware Defense	3	5	44
Information Technology	Problem Management and Incident Response	3	5	44
Transportation	Contract Management	3	5	44
Org Wide	Workforce	4	4	42
Org Wide	Citywide Risk Management	4	4	42
Administrative Services	Procurement	4	4	42
Fire	Emergency Medical Service	4	4	42
Human Resources	High Cost Claims	4	4	42
Human Resources	Workload	4	4	42
Information Technology	Mobile Device Management	5	3	40
Information Technology	Strategy and Governance	5	3	40
Public Works	Secondary Treatment Upgrades	2	5	38
Public Works	ADA Compliance Upgrade	2	5	38
Administrative Services	Investments, Debt, and Cash Management	2	5	38
Information Technology	Information Security	2	5	38
Information Technology	Operations and Monitoring	2	5	38
Information Technology	Physical and Environmental Controls	2	5	38
Information Technology	Ransomware	2	5	38
Police	Use of Force and Officer Conduct	2	5	38
Org Wide	Governance	3	4	36
Org Wide	Organizational Culture	3	4	36
Administrative Services	ERP System Upgrade	3	4	36
City Wide	Sustainability and Climate Action Plan	3	4	36
Administrative Services	Accounts Receivable	3	4	36
Fire	Fire Suppression	3	4	36
Fire	Fire Prevention - [REDACTED] Foothills & Wildland Fire Risk	3	4	36
Public Works	Public Services - Fleet	3	4	36
Public Works	Wastewater Treatment Plant Operations	3	4	36
Public Works	Public Services -Facilities	3	4	36
Utilities	AMI (Advanced Metering Infrastructure) Project	3	4	36
Utilities	Rates and Rate Adjustments	3	4	36

APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Proposed Audit Activities for FY2022-2023

Included in the tables below are the proposed audit activities for the remainder of FY2022 and FY2023. Each audit activity corresponds to a risk rated as High or Moderate in the Risk Assessment Report and selected based on other factors outlined on page 3.

The preliminary audit objectives are described for each audit listed. These objectives and scope of each audit activity will be further defined based on the result of a project planning risk assessment processes performed at the beginning of each activity.

Audits are planned in three overall phases – note that the timing may differ slightly for each audit activity:

- **Phase I** – Activities projected to start before March 2022 and end by June 2022
- **Phase II** – Activities projected to start in March 2022 and end by December 2022
- **Phase III** – Activities projected to start in June 2022 or January 2023 and end by June 2023

Amendments to the proposed audit plan will be proposed either as needed or after conducting an annual risk assessment and update the audit plan, as needed, during FY23. Amendments may be proposed in response to changes in the City's environment such as organizational structure, operations, risks, systems, and controls. Please note that the City Auditor will actively manage projects and overall budgets and workload in its execution of the workplan.

For each audit activity, a task order is submitted to the City Council for approval before the work is commenced. We have prepared and attached to this report multiple task orders that correspond to audit activities we have prioritized (e.g., those in Phase I). Those audit activities for are marked with an "X" in the 'Seeking Approval' column of the table below, and the Task Orders are included in the Appendix.

APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Phase I Activities

Seeking Approval	Function	Project Title	Audit Objectives	Timeline	Estimated Hours	FY22 Cost	FY23 Cost (*)	Total Cost FY21+22+23
	Administrative Services	Economic Recovery Advisory (Task Order 4.7)	<ul style="list-style-type: none"> Review the City's long-term financial planning model and offer recommendations for improvement. Identify and evaluate key revenue sources categories that present long term risk to the City's financial sustainability. Perform scenario analysis and advise in the development of long term financial projections. 	March - December 2021	400	\$04,063		\$04,063
	Public Works	Public Safety Building - Construction Audit (Task Order 4.8)	<ul style="list-style-type: none"> Monthly invoice review Change order testing Contingency and allowance testing Lien waiver control Compliance with insurance requirements 	March 2021 - June 2023	420	\$26,633	\$26,633	\$51,266
	Planning and Development Services	Building Permit & Inspection Process Review (Task Order 4.9)	<ul style="list-style-type: none"> Identify highest impact area to focus the assessment (e.g., specific permit type(s), specific sub-processes, etc.). Document corresponding process(es) and evaluate for efficiency and effectiveness. Benchmark operational performance against industry practices and established standards. 	April - September 2021	360	\$48,300		\$48,300
	Citywide	Nonprofit Agreements Risk Management Review (Task Order 4.10)	<ul style="list-style-type: none"> Evaluate controls in place to ensure that nonprofit organizations are properly vetted prior to selection and monitored through the life of an agreement. Assess the performance monitoring process against the best practice. Follow up on relevant audit findings from past audit work. 	May - September 2021	400	\$55,246		\$55,246
	Utilities	Utility Work Order & Process Review (Task Order 4.11)	<ul style="list-style-type: none"> Determine whether adequate controls are in place and working effectively around the work order process Assess the work order process against best practices 	January - December 2022	400	\$81,400		\$81,400
	Administrative Services / Information Technology	Wire Payment Process and Controls (Task Order 4.12)	<ul style="list-style-type: none"> Determine whether adequate controls are in place and working effectively to ensure that all disbursements are valid and properly processed in compliance with City's policies and procedures Determine whether end user security awareness training is sufficient to prevent erroneous payments caused by phishing 	February - June 2022	270	\$54,550		\$54,550
Phase I Sub Total					2,250	\$329,792	\$26,633	\$355,425

* For the purpose of audit plan preparation, OCA used the FY22 budget amount for FY23

APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Phase II Activities

Seeking Approval	Function	Project Title	Audit Objectives (preliminary objectives for audits not currently subject to approval)	Timeline	Estimated Hours	FY22 Cost	FY23 Cost (*)	Total Cost
X	Human Resources	Remote and Flexible Work Study	<ul style="list-style-type: none"> Assess employee and management perspectives for long-term remote and flexible work viability and associated challenges Evaluate positive outcomes and challenges for managing a mixed location workforce Identify policies, processes, management practices and work culture improvements that may improve the City's ability to manage a remote workforce 	March - December 2022	285	\$50,000	\$10,000	\$60,000
X	Information Technology	Cybersecurity Assessment	<ul style="list-style-type: none"> Map current state security capabilities to the NIST Cybersecurity Framework and evaluate the maturity of current security processes Identify current risks related to weaknesses in the City's cybersecurity program Identify target state objectives utilizing the Capability Maturity Model (CMMI) and develop recommendation to meet the objectives 	March - December 2022	525	\$90,000	\$20,000	\$110,000
X	Public Works	Wastewater Treatment Plant Agreement Audit	<ul style="list-style-type: none"> Evaluate whether direct and indirect costs incurred by the City are properly allocated to the operation of the Wastewater Treatment Plant. Review whether costs are properly allocated to the various parties to the Wastewater Treatment Plant Agreement. 	March 2022 - December 2022	400	\$60,000	\$2,250	\$62,250
Phase II Sub Total					1,210	\$194,000	\$38,250	\$232,250

* For the purpose of audit plan preparation, OCA used the FY22 budget amount for FY23

APPENDIX A: WRITING SAMPLES

FY2022/2023 Audit Plan

Phase III Activities

Seeking Approval	Function	Project Title	Preliminary Audit Objectives	Timeline	Estimated Hours	FY22 Cost	FY23 Cost (*)	Total Cost
	Transportation	Contract Management ALPR Technology	<ul style="list-style-type: none"> Determine whether policies and procedures are implemented effectively to protect the privacy of personal information gathered using ALPR technology for the City's parking management. Determine whether the City monitors the vendor's performance to ensure the compliance with contract terms and applicable laws and regulations related to data privacy. 	June 2022 - January 2023	400		\$82,500	\$82,500
	Administrative Services	Investment Management	<ul style="list-style-type: none"> Determine whether adequate controls are in place and operating effectively to ensure that investments are managed in accordance with the investment management and other relevant policies. Assess the organizational structure and operations of the investment portfolio management function against best practice. 	June 2022 - January 2023	350		\$61,550	\$61,550
	Information Technology	Disaster Recovery Preparedness	<ul style="list-style-type: none"> Determine whether a formal disaster recovery plan exists and aligns with the City's needs for business continuity Determine whether a disaster recovery plan is periodically tested and updated to ensure a successful recovery 	January - June 2023	400		\$87,500	\$87,500
	Administrative Services	Procurement Process	<ul style="list-style-type: none"> Determine whether adequate controls are in place and working effectively to ensure that the appropriate vendors are selected properly to achieve desired objectives Identify the opportunities to improve the efficiency and effectiveness of the procurement process 	January - June 2023	350		\$61,550	\$61,550
	Planning and Development Services	Long Range Planning	<ul style="list-style-type: none"> Review progress against intended goals and identify any gaps Determine whether an effective control environment exists for the Long Range Planning group to maintain City's Comprehensive Plan Determine whether adequate controls are in place and working effectively for data analyses 	January - June 2023	400		\$82,500	\$82,500
	Public Works	ADA Compliance	<ul style="list-style-type: none"> Determine whether improvements have been made to make facilities, programs, and services accessible in accordance with the Transition Plan and Self-Evaluation Final Study to ensure compliance with the Americans with Disabilities Act (ADA) OF 1990 	January - June 2023	350		\$61,550	\$61,550
	TBD	TBD / Ad Hoc Requests TBD		TBD	TBD			
Phase III Sub Total					2,300	\$0	\$468,100	\$468,100
Phase I + II + III TOTAL					5,760	\$523,792	\$521,983	\$1,045,775
FY22 - FY23 Budget						\$600,000	\$560,000	\$1,160,000
FY23 Ad Hoc / Contingency						\$76,208	\$38,017	\$114,225

* For the purpose of audit plan preparation, OCA used the FY22 budget amount for FY23

APPENDIX A: WRITING SAMPLES

FY2021/2022 Audit Plan

Appendix: Task Orders

APPENDIX A: WRITING SAMPLES

Audit Activity 4.13 – Remote and Flexible Work Study

PROFESSIONAL SERVICES TASK ORDER

TASK ORDER FY22-004.13

Consultant shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referenced in Item 8 below are incorporated into this Task Order by this reference. The Consultant shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

OR PURCHASE ORDER REQUISITION NO. (AS APPLICABLE)

- 1A. MASTER AGREEMENT NO. (MAY BE SAME AS CONTRACT / P.O. NO. ABOVE):
1B. TASK ORDER NO.: FY22-004.13
2. CONSULTANT NAME: Baker Tilly US, LLP
3. PERIOD OF PERFORMANCE: START: March 1, 2022 COMPLETION: December 31, 2022
4. TOTAL TASK ORDER PRICE: \$60,000
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT \$TBD
5. BUDGET CODE
COST CENTER
COST ELEMENT
WBS/CIP
PHASE
6. CITY PROJECT MANAGER'S NAME & DEPARTMENT:
7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)
MUST INCLUDE:
- SERVICES AND DELIVERABLES TO BE PROVIDED
- SCHEDULE OF PERFORMANCE
- MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (as applicable)
- REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)
8. ATTACHMENTS: A: Task Order Scope of Services B (if any): N/A

I hereby authorize the performance of the work described in this Task Order.

I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.

APPROVED: [Redacted]

APPROVED: COMPANY NAME: _____

BY: Name Title Date

BY: Name Title Date

APPENDIX A: WRITING SAMPLES

Attachment A

DESCRIPTION OF SCOPE OF SERVICES

Introduction

Attachment A, the Description of Scope of Services, contains the following four (4) elements:

- Services and Deliverables To Be Provided
- Schedule of Performance
- Maximum Compensation Amount and Rate Schedule (*As Applicable*)
- Reimbursable Expenses, if any (With “Not To Exceed” Amount)

Services & Deliverables

Baker Tilly’s approach to conducting the Construction Controls Assessment involves four (3) primary steps:

- Step 1: Audit Planning
- Step 2: Control review and analysis
- Step 3: Reporting

Step 1 – Audit Planning

This step consists of the tasks performed to adequately plan the work necessary to address the overall audit objective and to solidify mutual understanding of the audit scope, objectives, audit process, and timing between stakeholders and auditors. Tasks include:

- Gather information to understand the environment under review
 - Understand the organization structure and objectives
 - Review the codes, regulations, policies, and other standards and expectations
 - Review the prior audit results, if any
 - Review previously conducted employee engagement and satisfaction surveys
 - Issue an employee survey centered on remote work capabilities
 - Issue a management survey centered on remote work capabilities
 - Review additional documentation and conduct interviews as necessary
- Assess the audit risk
- Write an audit plan and audit program
 - Define audit objectives and scope
 - Identify the audit procedures to be performed and the evidence to be obtained
- Announce the initiation of the audit and conduct a kick-off meeting with key stakeholders
 - Discuss audit objectives, scope, audit process, timing, resources, and expectations
 - Discuss documentation and interview requests for the audit

APPENDIX A: WRITING SAMPLES

Step 2 – Control Review and Testing

This step involves executing the procedures in the audit program to gather information, interview individuals, and analyze the data and information to obtain sufficient evidence to address the audit objectives. The preliminary audit objective is to: (1) Assess employee and management perspectives for long-term remote and flexible work viability and associated challenges; (2) Evaluate positive outcomes and challenges for managing a mixed location workforce; (3) Identify policies, processes, management practices and work culture improvements that may improve the City's ability to manage a remote workforce. Tasks include but are not limited to:

- Analyze employee and management surveys to identify management and policy change opportunities and barriers for managing a mixed location workforce
- Interview (focus group and/or individual) the Human Resources, employee representatives and management representatives to understand the current state, benefits and barriers to
- Review relevant policies and procedures as well as the position eligibility standards for remote work to identify the criteria to be used for evaluation of control design and effectiveness
- Research best practices and practices of surrounding communities
- Analyze available data to assess current practices impact on recruitment and retention
- Validate analysis with Human Resources

Step 3 – Reporting

In Step 3, the project team will perform tasks necessary to finalize audit working papers and submit a final audit report. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals
- Complete the supervisory review of working papers and a draft audit report
- Distribute a draft audit report and conduct a closing meeting with key stakeholders
 - Discuss the audit results, findings, conclusions, and recommendations
 - Discuss management responses
- Obtain written management responses and finalize a report

Deliverables:

The following deliverable will be prepared as part of this engagement:

- Audit Report with remote and flexible work data analysis and best practice recommendation

Schedule of Performance

Anticipated Start Date: March 1, 2022

APPENDIX A: WRITING SAMPLES

Anticipated End Date: December 31, 2022

Maximum Compensation Amount and Rate Schedule

The not-to-exceed maximum, inclusive of reimbursable expenses (as summarized below) for this Task is \$60,000. The not-to-exceed budget is based on an estimate of 285 total project hours, of which 16 are estimated to be completed by the City Auditor.

Reimbursable Expenses

If circumstances allow, Baker Tilly anticipates planning one on-site fieldwork. Given this possibility, Baker Tilly could incur reimbursable expenses for this Task.

The not-to-exceed maximum for reimbursable expenses for this Task is \$5,000.

The following summarizes anticipated reimbursable expenses:

- Round-trip Airfare – \$1,200
- Rental Car - \$600
- Hotel accommodation - \$2,500 (8 nights)
- Food and incidentals – \$700

Note that, if current restrictions associated with COVID-19 continue, an on-site visit may not be possible. The project team will work with the City to consider circumstances at the time.

APPENDIX A: WRITING SAMPLES

Audit Activity 4.14 – Cybersecurity Assessment

PROFESSIONAL SERVICES TASK ORDER

TASK ORDER FY22-004.14

Consultant shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referenced in Item 8 below are incorporated into this Task Order by this reference. The Consultant shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

OR PURCHASE ORDER REQUISITION NO. (AS APPLICABLE)

- 1A. MASTER AGREEMENT NO. (MAY BE SAME AS CONTRACT / P.O. NO. ABOVE):
- 1B. TASK ORDER NO.: FY22-004.14
- 2. CONSULTANT NAME: Baker Tilly US, LLP
- 3. PERIOD OF PERFORMANCE: START: March 1, 2022 COMPLETION: December 31, 2022
- 4. TOTAL TASK ORDER PRICE: \$110,000
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT \$TBD
- 5. BUDGET CODE _____
COST CENTER _____
COST ELEMENT _____
WBS/CIP _____
PHASE _____
- 6. CITY PROJECT MANAGER'S NAME & DEPARTMENT:

- 7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)
MUST INCLUDE:
 - SERVICES AND DELIVERABLES TO BE PROVIDED
 - SCHEDULE OF PERFORMANCE
 - MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (as applicable)
 - REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)
- 8. ATTACHMENTS: A: Task Order Scope of Services B (if any): N/A

I hereby authorize the performance of the work described in this Task Order.

I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.

APPROVED:

APPROVED:
COMPANY NAME: _____

BY: _____
Name _____
Title _____
Date _____

BY: _____
Name _____
Title _____
Date _____

APPENDIX A: WRITING SAMPLES

Attachment A DESCRIPTION OF SCOPE OF SERVICES

Introduction

Attachment A, the Description of Scope of Services, contains the following four (4) elements:

- Services and Deliverables To Be Provided
- Schedule of Performance
- Maximum Compensation Amount and Rate Schedule (*As Applicable*)
- Reimbursable Expenses, if any (With “Not To Exceed” Amount)

Services & Deliverables

Cybersecurity Maturity Assessment

Baker Tilly’s approach to conducting a cybersecurity assessment and developing a cybersecurity program strategy involves four (4) primary steps:

- Step 1: Assessment Planning and Kick-off
- Step 2: Information Gathering
- Step 3: Cybersecurity Capability Analysis and Recommendations
- Step 4: Reporting

Step 1 – Assessment Planning and Kick-off

This step consists of the tasks performed to adequately plan the work necessary to address the overall assessment objective and to solidify mutual understanding of the assessment scope, objectives, assessment process, and timing between stakeholders and assessors. Tasks include:

- Baker Tilly will work with the City to finalize the assessment scope and project timeline. Baker Tilly will also provide the City with an initial interview and documentation request list.
- Finally, Baker Tilly will perform a project kick-off discussion with the City to ensure alignment with the project timeline, interview schedule, and deliverables.

Step 2 – Information Gathering

This step involves conducting interviews with identified IT security personnel and key stakeholders to identify security capabilities, processes, and currently implemented technologies.

Baker Tilly will also review current IT security policy and procedure documentation, as well as network and infrastructure architecture documents.

APPENDIX A: WRITING SAMPLES

Step 3 – Cybersecurity Capability Analysis and Recommendations

This step involves mapping current state security capabilities to the NIST Cybersecurity Framework and evaluate the maturity of current security processes. Baker Tilly will also identify current risks related to weaknesses in the City's cybersecurity program.

Baker Tilly will then review current state capabilities and risks with the City to ensure alignment on Baker Tilly's initial analysis and identify target state objectives utilizing the Capability Maturity Model (CMMI)

Finally, Baker Tilly will take the identified improvement areas and target state maturity objectives to develop our recommendations for the City's cybersecurity program to meet its target state objectives.

Step 4 – Reporting

The project team will perform tasks necessary to finalize the initial draft cybersecurity assessment report and review a draft report with the stakeholders. Additionally, the team will submit a final assessment report to the City. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals
- Distribute a draft assessment report and conduct a closing meeting with key stakeholders
 - Discuss the assessment results, findings, conclusions, and recommendations
- Obtain written management responses and finalize a report

Deliverables:

The following deliverable will be prepared as part of this engagement:

- Cybersecurity Assessment Report and Program Strategy

External Penetration Testing

Baker Tilly will perform external penetration testing on behalf of the City. Baker Tilly's approach to conducting these security testing activities involves four (4) primary steps:

- Step 1: Assessment Planning and Kick-off
- Step 2: Open-Source Information Gathering and Reconnaissance
- Step 3: External Penetration Testing
- Step 4: Reporting

Step 1 – Assessment Planning and Kick-off

This step consists of the tasks performed to adequately plan the work necessary to address the overall testing objective and to solidify mutual understanding of the testing scope, objectives, testing process, and timing between stakeholders and assessors. Tasks include:

APPENDIX A: WRITING SAMPLES

- Baker Tilly will work with the City to finalize the testing scope and project timeline.
- Baker Tilly will perform a project kick-off discussion with the City to ensure alignment with the project timeline, testing approach, and deliverables.
- Baker Tilly will provide the City with an ISP authorization form and Rules of Engagement documents for signature to confirm testing scope and activities.

Step 2 – Open-Source Information Gathering and Reconnaissance

This step involves conducting interviews with identified IT security personnel and key stakeholders to identify security capabilities, processes, and currently implemented technologies.

Baker Tilly will also review current IT security policy and procedure documentation, as well as network and infrastructure architecture documents.

Step 3 – External Penetration Testing

Baker Tilly will conduct external penetration testing on up to 300 active and 208 dormant external IP addresses provided by the City. External penetration testing services include:

- Confirmation of active versus dormant IP addresses
- Identification of services and service versions running on each active system;
- Automated vulnerability discovery scanning for each active system;
- Penetration attempts on systems identified that have known exploitable vulnerabilities; and
- Deep dive exploitation of any identified exploitable vulnerabilities to gain unauthorized access to internal systems and/or data.

Step 4 – Reporting

The project team will perform tasks necessary to finalize our security testing report and review a draft report with City stakeholders. Additionally, the team will submit a final testing report to the City. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals
- Distribute a draft testing report and conduct a closing meeting with key stakeholders
 - Discuss the testing results, findings, conclusions, and recommendations
- Obtain written management responses and finalize a report

Deliverables:

The following deliverable will be prepared as part of this engagement:

- External Penetration Testing Report

APPENDIX A: WRITING SAMPLES

Schedule of Performance

Anticipated Start Date: March 1, 2022
Anticipated End Date: December 31, 2022

Maximum Compensation Amount and Rate Schedule

The not-to-exceed maximum, inclusive of reimbursable expenses (as summarized below) for this Task is \$110,000. The not-to-exceed budget is based on an estimate of 525 total project hours, of which 30 are estimated to be completed by the City Auditor.

Reimbursable Expenses

We plan to complete the audit work remotely, including all interviews and documentation review. However, if the City requests the assessment team to travel on-site for meetings, interviews, or assessment report readouts, these travel related expenses will be billed in addition to the fees above.

APPENDIX A: WRITING SAMPLES

Audit Activity 4.15 – Wastewater Treatment Plant Agreement

PROFESSIONAL SERVICES TASK ORDER

TASK ORDER FY22-004.15

Consultant shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referenced in Item 8 below are incorporated into this Task Order by this reference. The Consultant shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

OR PURCHASE ORDER REQUISITION NO. (AS APPLICABLE)

- 1A. MASTER AGREEMENT NO. (MAY BE SAME AS CONTRACT / P.O. NO. ABOVE):
- 1B. TASK ORDER NO.: FY22-004.14
- 2. CONSULTANT NAME: Baker Tilly US, LLP
- 3. PERIOD OF PERFORMANCE: START: March 1, 2022 COMPLETION: December 31, 2022
- 4. TOTAL TASK ORDER PRICE: \$110,000
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT \$TBD
- 5. BUDGET CODE _____
COST CENTER _____
COST ELEMENT _____
WBS/CIP _____
PHASE _____
- 6. CITY PROJECT MANAGER'S NAME & DEPARTMENT:
- 7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)
MUST INCLUDE:
 - SERVICES AND DELIVERABLES TO BE PROVIDED
 - SCHEDULE OF PERFORMANCE
 - MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (as applicable)
 - REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)
- 8. ATTACHMENTS: A: Task Order Scope of Services B (if any): N/A

I hereby authorize the performance of the work described in this Task Order.

I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.

APPROVED:

BY: _____
Name _____
Title _____
Date _____

APPROVED:

COMPANY NAME: _____
BY: _____
Name _____
Title _____
Date _____

APPENDIX A: WRITING SAMPLES

Attachment A DESCRIPTION OF SCOPE OF SERVICES

Introduction

Attachment A, the Description of Scope of Services, contains the following four (4) elements:

- Services and Deliverables To Be Provided
- Schedule of Performance
- Maximum Compensation Amount and Rate Schedule (*As Applicable*)
- Reimbursable Expenses, if any (With “Not To Exceed” Amount)

Services & Deliverables

Baker Tilly’s approach to conducting a Wasterwater Treatment Plant Agreement Review involves three (3) primary steps:

- Step 1: Audit Planning
- Step 2: Process and Control Review
- Step 3: Reporting

Step 1 – Audit Planning

This step consists of the tasks performed to adequately plan the work necessary to address the overall audit objective and to solidify mutual understanding of the audit scope, objectives, audit process, and timing between stakeholders and auditors. Tasks include:

- Gather information to understand the environment under review
 - Understand the organizational structure and objectives
 - Review the City code, regulations, and other standards and expectations
 - Review prior audit results, as applicable
 - Review additional documentation and conduct interviews as necessary
- Assess the audit risk
- Write an audit planning memo and audit program
 - Refine audit objectives and scope
 - Identify the audit procedures to be performed and the evidence to be obtained and examined
- Announce the initiation of the audit and conduct kick-off meeting with key stakeholders
 - Discuss audit objectives, scope, audit process, timing, resources, and expectations
 - Discuss documentation and interview requests for the audit

APPENDIX A: WRITING SAMPLES

Step 2 – Process and Control Review

This step involves executing the procedures in the audit program to gather information, interview individuals, and analyze the data and information to obtain sufficient evidence to address the audit objectives. The preliminary audit objective is to: (1) Determine whether adequate controls are in place and working effectively to ensure that costs for treatment plan operations are properly accounted for and allocated; (2) Assess the compliance with contracts and regulations. Procedures include:

- Interview the appropriate individuals to understand the process, the information system used, and internal controls related to accounting and allocation of costs for treatment plan operations.
- Review the contracts, policies and procedures as well as the regulations and standards to identify the criteria to be used for evaluation of compliance and control design and effectiveness
- Review the documents (such as contracts and supporting documents for allocation) for the selected allocation transactions
- Compare the cost accounting and allocation methodology against the requirements

Step 3 – Reporting

In Step 3, the project team will perform tasks necessary to finalize audit working papers, prepare and review a draft report with the stakeholders, and submit a final audit report. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals and discuss the root cause of the identified findings
- Complete supervisory review of working papers and a draft audit report
- Distribute a draft audit report and conduct a closing meeting with key stakeholders
 - Discuss the audit results, findings, conclusions, and recommendations
 - Discuss management responses
- Obtain written management responses and finalize a report
- Review report with members of City Council and/or the appropriate Council Committee
- Present the final report to the City Council and/or appropriate Council Committee

Deliverables:

The following deliverable will be prepared as part of this engagement:

- Audit Report

Schedule of Performance

APPENDIX A: WRITING SAMPLES

Anticipated Start Date: March 1, 2022
Anticipated End Date: December 31, 2022

Maximum Compensation Amount and Rate Schedule

The not-to-exceed maximum, inclusive of reimbursable expenses (as summarized below) for this Task is \$82,500. The not-to-exceed budget is based on an estimate of 400 total project hours, of which 20 are estimated to be completed by the City Auditor.

Reimbursable Expenses

If circumstances allow, Baker Tilly anticipates planning one on-site fieldwork week. Given this possibility, Baker Tilly could incur reimbursable expenses for this Task.

The not-to-exceed maximum for reimbursable expenses for this Task is \$4,750.

The following summarizes anticipated reimbursable expenses (for three team members):

- Round-trip Airfare – \$1500
- Rental Car - \$400
- Hotel accommodation - \$2500 (4 nights)
- Food and incidentals – \$750

Note that, if current restrictions associated with COVID-19 continue, an on-site visit may not be possible. The project team will work with the City to consider circumstances at the time.

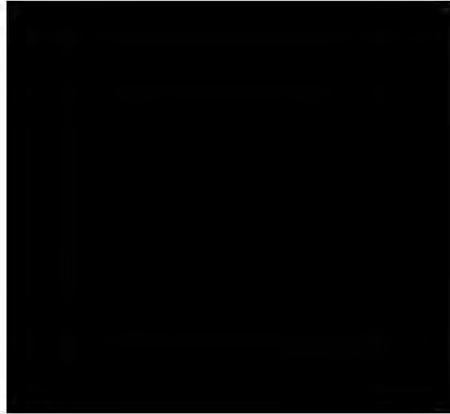
APPENDIX A: WRITING SAMPLES



al Audit Plan

August 28, 2020

FINAL REPORT



APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan

TABLE OF CONTENTS

Table of Contents

Background 2
 Department Organization and IT Environment..... 2
 [REDACTED] 3
Approach and Methodology..... 4
 Risk Assessment Approach 4
 Risk Analysis and Scoring Methodology..... 4
Risk Assessment Results 6
 Risk Heat Map..... 6
 IT Risk Areas by Rating 7
Proposed Internal Audit Activities 8
Appendix A: IT Risk Assessment Interviews..... 9
Appendix B: Detailed Risk Matrix..... 10
Contact Information..... 29

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
REPORT

Background

Baker Tilly Virchow Krause, LLP (Baker Tilly), in its co-sourced capacity with the [REDACTED] internal audit function, conducted a comprehensive IT risk assessment of [REDACTED]. This report outlines our assessment of information technology risks. The results of this risk assessment are the basis for determining high impact areas for inclusion in the [REDACTED] annual internal audit plan.

Department Organization and IT Environment

[REDACTED]

Client & Peripherals

The Help Desk provides a centralized means of contact for technology problems, system issues and service requests for the Southern Ute Indian Tribe and related business units.

- Help Desk
- Desktop Support
- Telephony & Collaboration
- Inventory Management

Network & Infrastructure

IT Operations provides the inter-entity networking and core access functions which includes data backup and retrieval, systems architecture and site security support for the [REDACTED].

- Email
- Network Access
- SAN (Storage Area Network)
- Server Side (File & Print Services)
- Wireless

Enterprise and Business Applications

[REDACTED] provides [REDACTED] Entities with Enterprise and business specific software and support.

- PeopleSoft Finance & Supply Chain Management
- PeopleSoft Human Capital Management
- Kronos
- Enertia
- Business Intelligence (BI)
- Geographical Information Systems (GIS)
- Web Services

Program Management

Program Management provides management and back-office services to support [REDACTED] internal requirements and commitments.

- Project & Portfolio Management
- Accounting & Budget Planning
- Purchasing & Procurement
- Client Relationship
- Workforce Planning

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan

REPORT

- Governance, Audit, Certifications & Compliance
- Security Awareness Training & Testing

Technology Repair Services

[REDACTED] offers free computer repair services for [REDACTED] members' personal computers and related devices that meet certain conditions. [REDACTED] staff will provide basic repairs, diagnostics and troubleshooting support. In FY 2019 [REDACTED] closed approximately 75 tickets that were opened to support technology needs for [REDACTED].

Strengths

During the IT Risk Assessment we noted in general that [REDACTED] has established an effective and strong information technology department. Some of the notable strengths include:

- [REDACTED] centralized IT functions which resulted in significant cost reduction and streamlining/consolidation of systems and services for greater service delivery and efficiencies.
- During the COVID-19 pandemic [REDACTED] was able to sustain tribal operations quickly by deploying and providing the support necessary for 400 employees to be able to work remotely.
- End users are generally quite satisfied with [REDACTED] support and noted reliable, responsive and helpful customer service from [REDACTED].

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
 REPORT

Approach and Methodology

Risk Assessment Approach

Baker Tilly’s risk assessment approach consisted of the following phases:

Risk Assessment Approach	
Planning	- The Planning phase entailed working with [REDACTED] Internal Audit to confirm the scope and determine the appropriate methodology to plan and perform the risk assessment.
Information Gathering	- The Information Gathering phase included interviews and review of key documentation to gain a high level understanding of the current state processes and controls as well as gathering [REDACTED] thoughts on IT risk levels.
Analysis	- The Analysis phase included analysis of risk ratings across all IT areas and prioritization by risk severity. Further, potential internal audit activities were identified based on higher risk areas identified through this analysis.
Reporting	- The Reporting phase included documentation of the risk assessment report summarizing the background, approach, and results of the risk assessment, as well as proposed internal audits.

Our interviews and assessment covered the following IT risk areas:

1. Application Management
2. Architectural and Deployment
3. Asset Management
4. Change Management
5. Compliance Management
6. Disaster Recovery Preparedness and Testing
7. Database and Data Management
8. End-User Support and Perceptions
9. Host Intrusion and Malware Defense
10. Information Security
11. Mobile Device Management
12. Organizational Architecture
13. Operations and Monitoring
14. Physical and Environmental Controls
15. Problem Management and Incident Response
16. Procurement and Service Provider Management
17. Portfolio & Project Management
18. Risk Management
19. Strategy and Governance

Risk Analysis and Scoring Methodology

For IT risk assessments Baker Tilly utilizes the Open Web Application Security Project’s (OWASP) Risk Rating methodology generally across all IT areas, which assesses risk based upon the likelihood that a risk event will occur and its potential impact. The matrix shown in Table 1 considers technical likelihood and business impact to help determine the overall risk severity.

Technical likelihood addresses the ease of identifying and exploiting the risk. This can be further understood by looking at “threat agents” and “vulnerability factors.” Threat agents are the items that address the motive and skill required to exploit a risk. Vulnerability factors address the ease of identifying the risk and exploiting it.

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

REPORT

Business impact addresses the exploitive effect of the vulnerability upon the business, consisting of "technical impacts" and "organizational impacts". The technical impacts are those that address the confidentiality, integrity and availability of the data. The organizational impacts are financial damage, reputational damage, regulatory non-compliance, loss of intellectual property and violation of privacy.

Table 1. Risk Rating			
Technical Likelihood	Business Impact		
	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Note	Low	Medium

Table 2 below provides further description of the categorizations for each level of risk severity.

Table 2. Risk Rating Category Descriptions	
Risk Rating	Description
Critical	These risks have both a high technical likelihood of occurrence and a high business impact upon the organization. Their exploitation could cause great damage to the organization, its systems and/or sensitive information assets. The underlying vulnerabilities should be treated as soon as possible.
High	These risks have mixed technical likelihood of occurrence and a business impact that ranges between medium and high. Their exploitation could cause much damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the critical risks. The underlying vulnerabilities should be treated with or after the "critical risk" vulnerabilities.
Medium	These risks have mixed technical likelihood of occurrence and a business impact that ranges between low and high. Their exploitation could cause moderate damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the high risks. The underlying vulnerabilities should be treated with or after the "high risk" vulnerabilities.
Low	These risks have mixed technical likelihood of occurrence and a business impact that ranges between low and medium. Their exploitation could cause nominal damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the medium risks. The underlying vulnerabilities should be treated with or after the "medium risk" vulnerabilities.
Note	These risks have both a low technical likelihood of occurrence and a low business impact upon the organization. Their exploitation would cause negligible damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the low risks. The underlying vulnerabilities may optionally be treated with or after the "low risk" vulnerabilities.

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
 REPORT

Risk Assessment Results

The results of the risk assessment are summarized in the following subsections in the form of a risk heat map and list of IT risk areas ranked by risk severity.

Risk Heat Map

Each IT risk area is mapped below under the relevant risk severity, according to the applicable likelihood and impact ratings. None of the IT risk areas were identified as critical risk severity, although two areas, database and data management as well as operations and monitoring fell under high risk severity. Of the remaining IT risk areas, ten were identified as medium risk severity, five low risk severity, and two negligible risk severity.

RISK MAP			
	Low Impact	Medium Impact	High Impact
High Likelihood	<u>Risk Severity: Medium</u>	<u>Risk Severity: High</u>	<u>Risk Severity: Critical</u>
Medium Likelihood	<u>Risk Severity: Low</u>	<u>Risk Severity: Medium</u>	<u>Risk Severity: High</u>
		1. Application Management 2. Asset Management 3. Disaster Recovery Preparedness and Testing 4. Problem Management and Incident Response 5. Risk Management 6. Strategy and Governance	1. Database and Data Management 2. Operations and Monitoring
Low Likelihood	<u>Risk Severity: Negligible</u>	<u>Risk Severity: Low</u>	<u>Risk Severity: Medium</u>
	1. Procurement and Service Provider Management 2. Project Management	1. Change Management 2. Compliance Management 3. End-User Support and Perceptions 4. Organizational Architecture 5. Mobile Device Management	1. Architecture and Deployment 2. Host Intrusion and Malware Defense 3. Information Security 4. Physical and Environmental Controls

APPENDIX A: WRITING SAMPLES

██████████ Risk Assessment Results & Proposed Internal Audit Plan

REPORT

IT Risk Areas by Rating

The following table summarizes the ranked risks by IT Risk Area. Refer to [Appendix B](#) for additional risk details.

IT Risk Area	Likelihood	Impact	Risk Severity
Database and Data Management	MED	HIGH	HIGH
Operations and Monitoring	MED	HIGH	HIGH
Architecture and Deployment	LOW	HIGH	MED
Host Intrusion and Malware Defense	LOW	HIGH	MED
Information Security	LOW	HIGH	MED
Physical and Environmental Controls	LOW	HIGH	MED
Application Management	MED	MED	MED
Asset Management	MED	MED	MED
Problem Management and Incident Response	MED	MED	MED
Risk Management	MED	MED	MED
Strategy and Governance	MED	MED	MED
Disaster Recovery Preparedness and Testing	MED	MED	MED
Change Management	LOW	MED	LOW
Compliance Management	LOW	MED	LOW
End-User Support and Perceptions	LOW	MED	LOW
Organizational Architecture	LOW	MED	LOW
Mobile Device Management	LOW	MED	LOW
Procurement and Service Provider Management	LOW	LOW	LOW
Project Management	LOW	LOW	LOW

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
 DETAILED REPORT

Proposed Internal Audit Activities

Baker Tilly identified specific IT risk areas to incorporate into the Annual Internal Audit Plan based on the risk assessment results and areas of high priority to [REDACTED]. Internal audit seeks to identify projects that provide opportunities to add value and maintain proper audit coverage. The table below summarizes our proposed projects around information technology.

Proposed Projects to Include in the Internal Audit Plan

Risk Category	Audit Area	Preliminary Scope
Database and Data Management	Data Privacy	<p>Advisory scope (recommended): Develop a unified compliance management program to align current data privacy compliance obligations with future plans to ensure the most efficient path to meeting future state objectives/requirements. Deliverables would include documentation of current compliance obligations (e.g. CCPA, CJIS, gaming, PCI), controls listing, and program governance framework, gap analysis, and recommendations including a roadmap for meeting compliance obligations.</p> <p>Audit Scope: Assessment of [REDACTED] practices around data governance for privacy, confidentiality, and compliance as well as alignment with external expectations. Scope may include privacy management, data management and collection, data security, third party compliance/contracts, and incident management and escalation.</p>
Operations and Monitoring	Capacity Management and System Maintenance	<p>Audit Scope: Audit of [REDACTED] computer operations and monitoring/maintenance practices related to capacity management, hardware and software. Scope may include system security and availability, expenditure planning/forecasting, and legacy system transition management.</p>
Business Continuity Planning (BCP)	Disaster Recovery (DR) Preparedness	<p>Advisory scope (recommended): Assist [REDACTED] in conducting a business impact analysis to identify and measure organizational impacts in order to determine key requirements from each business area such as critical activities, maximum tolerable period of disruption (MTPD), recovery time objectives (RTO), and recovery point objective (RPO).</p> <p>Audit Scope: N/A (Auditing this area would require documented business continuity plans and requirements from the various business areas/departments which are not currently developed. As such, our recommendation is to focus on the development and documentation of those requirements, per the advisory scope above.)</p>

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
 APPENDIX A: IT RISK ASSESSMENT INTERVIEWS

Appendix A: IT Risk Assessment Interviews

IT Personnel		Non-IT Personnel	
Area	Staff	Organizational Area	End Users
Application Management	[REDACTED]	Perm Fund	[REDACTED]
Architecture and Deployment	[REDACTED]	Perm Fund	[REDACTED]
Asset Management	[REDACTED]	[REDACTED] Fund	[REDACTED]
Change Management	Bill Doherty	Growth Fund	[REDACTED]
Compliance Management	[REDACTED]	Growth Fund	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Disaster Recovery Preparedness and Testing	[REDACTED]	Casino	[REDACTED]
End-User Support and Perceptions	[REDACTED]	Casino	[REDACTED]
Host Intrusion and Malware Defense	[REDACTED]		
Information Security	[REDACTED]		
Mobile Device Management	[REDACTED]		
Operations and Monitoring	[REDACTED]		
Organizational Architecture	[REDACTED]		
Problem Management and Incident Response	[REDACTED]		
Physical and Environmental Controls	[REDACTED]		
Procurement and Service Provider Management	[REDACTED]		
Project Management	[REDACTED]		
Risk Management	[REDACTED]		
Strategy and Governance	[REDACTED]		

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

Appendix B: Detailed Risk Matrix

Risk notes and ratings are detailed for each IT risk area in the matrix below.

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
Application Management This area focuses on the management of the organization's business applications – how they are developed, procured, modified and managed as well as how application security is performed and the role of the IT department in managing an application.	Application Development Process <ul style="list-style-type: none"> Software requests must have concurrence and approval from management. Works with each department to understand its requirements and provide recommendations related to procurement and custom developments. For each custom development IT provides a rough high level estimate to the customer. If they agree an in-depth planning occurs including an estimation of the effort required for the project. Testing and approvals are required for each round of development. All project work requires VP or CIO level approvals. Work completed and the related approvals are tracked in a task management system. <i>Risk consideration: Some instances in which development may initially be classified as a support ticket versus small project and does not receive same level of documentation and scrutiny.</i> Authentication to Applications <ul style="list-style-type: none"> The majority of applications are web and mobile based. 80-90% if the integrated authentication is based on Active Directory. SSL is used across the board (encrypted). Tokens expire at different intervals of time. VPN is required for internal applications such as PS and Kronos. The Password Policy is defined within the Information Security Policy. Support <ul style="list-style-type: none"> is supporting the primary and backup (at a minimum) for all in house applications and third-party applications. The helpdesk handles Tier 1 customer issues Enhancement requests go through the helpdesk and ticketing process. 	Poor application management practices causing application downtime or lack of functionality resulting in disruption of business operations.	MED	MED	MED

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Architecture and Deployment This area focuses on the architecture and deployment of organization's information technology. In-scope elements include:</p> <ul style="list-style-type: none"> The network architecture and deployed technology that is used to provide intra-site, inter-site connectivity and Internet connectivity The organization's server and storage infrastructure The computer hardware that is deployed for end-users 	<p>COVID</p> <ul style="list-style-type: none"> Remote work was not previously allowed by [redacted] unless traveling or working in a remote location. Now over 400 people are working remotely. Infrastructure set up for remote work went smoothly [redacted] was able to patch the critical infrastructure quickly. CARES ACT funding will be used to increase safeguards such as advance security features from Microsoft to help harden the system. IT is very proactive in responding to Microsoft alerts and issues. Previously phishing was a concern for the user community. Currently, the numbers have improved due to remediation efforts among the users with the most issues. SUSS has tailored the training its delivers related to the high risk areas (e.g. accounting and finance). <p>Security</p> <ul style="list-style-type: none"> Have instituted best practices around securing access to network (admin vs. user), privileged accts used in limited way, AD authentication (network and storage infrastructure); user accounts have limited access. Getting better at doing root cause analysis and getting to answers quickly Microsoft Identity Management reports on risky users which helpdesk investigates, and would block their account and require password reset Have had some instances requiring more in depth investigation and never found any incidents of compromised data, etc. Has network diagrams, gold images for server configurations, and GPOs for end user workstations. <p><i>Risk Considerations: Since IT centralization they have not fully standardized some settings/configurations on systems, password for implementation on systems, and password requirements for end users.</i></p> <p>Service Delivery</p> <ul style="list-style-type: none"> In the process of standardizing all infrastructure which has resulted in economies of scale to bring uptime and consistency in service delivery, better change control (less unexpected impacts) Now measuring/recording outages and reporting out to shared service committee and Tribal council. Outages continue to decrease (currently average 4 outages per month, 20 mins to an hour, some caused by vendors) 	<p>Poor IT architecture and deployment causing unreliable IT service delivery and security weaknesses resulting in end-user dissatisfaction or loss of data availability, integrity, or confidentiality and reputational damage.</p>	<p>LOW</p>	<p>HIGH</p>	<p>MED</p>

APPENDIX A: WRITING SAMPLES

[REDACTED]

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Asset Management This area focuses on the IT department's asset management practices. In-scope activities include the following:</p> <ul style="list-style-type: none"> Tracking information technology assets from procurement through disposal. Reusing and decommissioning information technology assets Ensuring information technology assets have an assigned owner, who is a stakeholder in the asset's protection Ensuring information technology assets are properly maintained to maximize their useful life Tracking software usage and ensuring that vendors' software license agreements are followed 	<p>Tracking</p> <ul style="list-style-type: none"> [REDACTED] does not have an Asset Management Policy. [REDACTED] is the asset management system which is used for tracking PCs/laptops; use asset tagging and [almost] every asset/inventory in the system has an assigned owner. In 2019, [REDACTED] physically walked across all the organizations and verified assets/owners. They were able to uncover a lot as a result of COVID (temp assignments) Servers are tracked separately and mobile devices are not tracked. MS monitors if [REDACTED] is going to exceed its software licenses. Other purchases are made with enterprise agreements and are not tracked per license. Justin, Shelley are notified of exceptions. In the past, [REDACTED] bought significantly more licenses than needed. Recently, there have been efforts to optimize costs. To do this they monitor and assess usage to obtain the true number of necessary licenses to ensure they are not overpaying. The also track the reusing and decommissioning information technology assets. Asset recycling is recorded. The process is to hold the asset for two weeks, remove the hard drive memory, record as recycled in asset management form, degaussing machine wipes harddrive, then destroyed. eWaste quarterly recycling, recorded in asset management form. These forms are maintained in SharePoint. [REDACTED] has the ability to lookup a device as long as it is on a form they can export to excel for inquiries. There is not a lot of unsupported software. There only a handful of users considered to be shadow IT that can be access. Any software that falls under this category is monitored (SUSS purchased end of life support at a higher cost). SUSS also scans computers for software that should not be there. <p>Maximize Useful Life</p> <ul style="list-style-type: none"> [REDACTED] tracks maintenance contracts throughout the budgeting process. This information is not stored or tracked in WASP. For example, if a workstation has problems and the related tickets are stored in [REDACTED] [REDACTED] reviews issues with multiple tickets to see if a system or computer needs to be moved up for servicing [REDACTED] reviews the help desk tickets as a method of monitoring 	<p>Poor asset management practices resulting in loss of data and IT assets, decreased asset longevity and usefulness, increased costs due to unneeded asset acquisition, and increased security vulnerabilities for untracked IT assets.</p>	MED	MED	MED

APPENDIX A: WRITING SAMPLES

[REDACTED]

[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Change Management This area focuses on the IT department's practices for controlling changes to the IT environment. In-scope activities include the following:</p> <ul style="list-style-type: none"> • Management of infrastructure hardware, software and configuration changes • Management of host system software and configuration changes • Management of normal and emergency changes • Application release management • Delineation of the activities that are controlled by change management versus help desk request ticketing 	<p>Policy</p> <ul style="list-style-type: none"> • [REDACTED] has a Change Control and Release Change Management Overview Policy • [REDACTED] has an application development, and operations change process (i.e. network, information, and DR) • [REDACTED] participates in weekly or bi-weekly CAB meetings (Change Acceptance Board) to review changes that meet a predetermined criteria (e.g. operational and high risk changes). • In the [REDACTED], a change ticket has a tab for CAB information. Once a change is CAB approved, Bill approves and moves it to a scheduled status, then the change owner performs the work. <p>Risk Consideration</p> <ul style="list-style-type: none"> • [REDACTED] need develop a mechanism to identify what should go through the CAB and how it should be identified, but trust their people to identify and raise those changes <p>Management of host system software and configuration changes</p> <ul style="list-style-type: none"> • The process starts with opening a ticket. The manager receives and approves the ticket and the change is made by owner. The business owner or change requestor gets a notification when the change is completed. • Software changes get approved by someone with a higher level of authority than the person that owns the change. <p>Management of normal and emergency changes</p> <ul style="list-style-type: none"> • These changes are managed in the [REDACTED] system. • Operations has an ECAB (i.e. needs two members of operations team plus a member making the change to meet and complete the work). <p>Application release management</p> <ul style="list-style-type: none"> • Goes through the application process with a ticket in [REDACTED] • The process is the same as normal and emergency changes (e.g. ECAB with the appropriate people involved). <p>Delineation of change management versus help desk request ticketing</p> <ul style="list-style-type: none"> • These two types are separated in [REDACTED]. Helpdesk tickets are typically a service request or a production incident that has happened to one person (50-80 tickets a day). These can sometimes transition from a helpdesk ticket into a change ticket if needed. This might require technical or financial approvers (e.g. to purchase something). • Helpdesk management participate in the weekly CAB calls so they are aware of information and big application changes. <p>Improvement areas</p> <ul style="list-style-type: none"> • Bill would ideally like the Change Management Policy to identify every scenario and procedure for each. 	<p>Poor change management practices causing inappropriate, unauthorized, under-planned and/or under-tested system changes resulting in disruption to business operations.</p>	<p>LOW</p>	<p>MED</p>	<p>LOW</p>

APPENDIX A: WRITING SAMPLES

[REDACTED]

[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Compliance Management This area focuses on the IT department's practices for complying with IT-related contract requirements, governmental regulations (e.g., HIPAA Security Rule) and industry standards (e.g., PCI Data Security Standard). In-scope are the following activities:</p> <ul style="list-style-type: none"> • Compliance program development and maintenance • Compliance program monitoring and reporting 	<p>Compliance</p> <ul style="list-style-type: none"> • Management and tracking of certifications required to work on data is maintained in PeopleSoft's HR module. PeopleSoft sends 30 and 60 days reminders depending on the type of certification. <p>Access</p> <ul style="list-style-type: none"> • [REDACTED] has the 30 and 60 day reminders. [REDACTED] has a contract with a company [REDACTED] for media disposal. • Gaming has certification licenses and is in-charge of revoking badges as needed. • HIPAA data is maintained in a database. Access to the database is managed by tribal health in collaboration with the BIA and HIS. Certification is conducted for the entire [REDACTED] team annually in October. • PCI - the casino is responsible for PCI and two IT related personnel may conduct PCI trainings. [REDACTED] does not manage PCI compliance. <p>Risk Consideration [REDACTED]</p> <p>Policies</p> <ul style="list-style-type: none"> • CJIS has an Electronic Media Disposal Policy • There is also a Cloud Computing Compliance Checklist. The checklist is required to send to vendors to ensure good practices for cloud data security. <p>IT Contracts</p> <ul style="list-style-type: none"> • There is a dedicated SME/owner that manages each contract and renewals and is responsible for compliance along with relevant manager. • Local legal firm ensures contract comply with sovereign tribal laws and TERO rules. 	<p>Insufficient compliance management practices causing non-compliance with requirements, laws or regulations resulting in penalties, fines, legal costs, and reputational damage.</p>	<p>LOW</p>	<p>MED</p>	<p>LOW</p>

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
Database and Data Management This area focuses on the IT department's practices for managing digital information. In-scope activities include the following: <ul style="list-style-type: none"> Classifying the information that is received, processed, transmitted and stored by the work staff Protecting digital information from the following security losses: confidentiality, integrity and availability Controlling access to digital information via file share and database management controls Performing procedures to backup stored information Ensuring backed up information is recoverable 	Data Classification <ul style="list-style-type: none"> There is no data classification policy. There are 3 classifications of data in the organization. How data is secured and stored for [REDACTED] is only specified for HIPAA and credit card data. Data Protection <ul style="list-style-type: none"> Data loss prevention scanning and analysis is conducted to identify improperly stored data. Confidentiality is controlled through application access control (i.e. least privilege access). Write access to the database is only given to an end user if it is required to perform their job duties. Access to digital information is controlled via file share and database management controls through active directory users and groups. CJIS and HIPAA training is required. Data Integrity <ul style="list-style-type: none"> A few databases run auditing and can see if someone is updating data. Data Availability <ul style="list-style-type: none"> There is replication between two of the data centers. High availability clusters are utilized. Database clustering is used by MS availability groups The SQL server for file and network shares and Veeam to backup to SAN (ops team monitoring for backup failures). Data Recovery <ul style="list-style-type: none"> Minimum hourly log backups and daily full backups are taken. Restoration tests not being performed on a set schedule. Backups run checks for completion. 	Poor database and data management practices causing data loss and accidental or unauthorized data modification or disclosure resulting in unplanned staff time and expense to recover (reenter) lost data, disruption of business operations, and reputational damage.	MED	HIGH	HIGH

APPENDIX A: WRITING SAMPLES

[REDACTED]

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Disaster Recovery Preparedness and Testing</p> <p>This area focuses on the IT department's preparations and testing for disaster recovery (DR). In-scope activities include the following:</p> <ul style="list-style-type: none"> Disaster recovery strategy and alignment with the organization's business continuity plans Disaster recovery plan preparation Disaster recovery testing 	<p>Plan</p> <ul style="list-style-type: none"> There is no business continuity plan for the business side of [REDACTED]. [REDACTED] could do a better job at disaster recovery planning. <p>Development process</p> <ul style="list-style-type: none"> [REDACTED] went through the process of identifying critical work streams which include critical business systems such as the ERP systems (e.g. AP, payroll, etc.), systems critical to run day to day ops (e.g. 911, police) Applications for productivity include outlook and active directory. <p>Authority to declare a disaster</p> <ul style="list-style-type: none"> There is an emergency response individual designated in [REDACTED] focuses more on an IT perspective and what triggers a disaster from their standpoint (e.g. massive hardware failure, cyber incident, power outages, etc.) Key plan execution team The team depends on the disaster. This is not formally defined in writing. Key people on the execution team would include the data center manager, [REDACTED] <p>Testing</p> <p>The current plan was developed and last tested in 2015. The plan does not address restoration back to normal operations after a disaster.</p>	<p>Insufficient disaster recovery preparedness causing less effective and timely recovery from disaster events, resulting in increased disruption of business operations and service delivery, expenditures for system recovery, and reputational damage.</p>	MED	MED	MED

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>End-User Support and Perceptions This area focuses on the IT department's scope and approach for providing end-user support as well as the perceptions that end-users have regarding IT service delivery. In-scope activities include the following:</p> <ul style="list-style-type: none"> • End-user request intake • Help Desk triaging of end-user requests and problems • Help Desk request tracking and reporting • End-user notification of request handling progress and completion • Requesting and receiving end-user feedback on completed or abandoned service requests 	<p>Helpdesk process</p> <ul style="list-style-type: none"> • Request are submitted through a call, email, or ticket in [REDACTED] (i.e. self service). • The process includes helpdesk triage of an issue to address or assign problem to the appropriate support team. • Customers receive email alerts once ticket is assigned, and reminder emails if ticket is not resolved within a certain period of time. • Ticket prioritization may not be formally defined. It will depend on the issue/situation and number of users affected. • Tier 1 and 2 helpdesk analysts are responsible for resolving issues such as password resets, system problems (e.g. adobe, word formatting), and setting up printers. Generally, they address any single-machine related issues. • End user receives automated notification after tickets are created, an email when technician claims the request and then an email when ticket is closed. <p>Customer satisfaction survey</p> <ul style="list-style-type: none"> • After connecting to end users machine during a remote session a popup to rate their service from 1-5 will appear and they can enter comments into a text box. These ratings are reported monthly to the department heads and the tribal council. Generally [REDACTED] receives a 4.9/5 average rating • There is no separate customer satisfaction survey being conducted. They are working on something to send out annually. • The department does well at prioritization and communication related to upgrades. • Room for improvement in technical expertise of some helpdesk staff. Wait times can be long if the expertise is not there and in some cases customers can be waiting for a couple of weeks to get a resolution • There are some issues that come up with applications but IT is on top of it when they ask for help. <ul style="list-style-type: none"> • They know who to contact directly depending on the system to get help with their issues • Support ticket provide a notification of receipt and if clarification is needed by IT support. • There have been some issues with the Reporting Tree and Visual One • They systems they utilized have limited functionality but IT does it best to work around the limitations to resolve users issues. <p>Improvements</p> <ul style="list-style-type: none"> • [REDACTED] is limited by PeopleSoft's ability to integrate with bowling systems/software • Communication can be improved on the possible interruptions that may result from upgrades. There used to be regular monthly meeting with [REDACTED] however, when COVID hit these meetings stopped. <p>Growth Fund</p> <ul style="list-style-type: none"> • The support and helpdesk services provided by [REDACTED] are expensive. • In previous years, [REDACTED] had project managers for large projects. • The monthly close cycle can be a challenge each month. • Working from home has been great although sometimes there is a need to physically access paper files in the office. <p>Service</p> <ul style="list-style-type: none"> • Different tickets types determine if the helpdesk can fulfill the request in a satisfactory manner. 	<p>Poor end-user support causing customer dissatisfaction resulting in loss of end-user sponsorship and partnership in IT initiatives, and loss of IT funding.</p>	<p>LOW</p>	<p>MED</p>	<p>LOW</p>

APPENDIX A: WRITING SAMPLES

████████████████████
 ██████████ Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Host Intrusion and Malware Defense This area focuses on the IT department's practices for protecting network connected computers, telephones, printers and infrastructure hardware devices from intrusive activity and malicious software exploitation. In-scope activities include the following:</p> <ul style="list-style-type: none"> • Intrusion detection and prevention deployment, operation, and monitoring • Malware defense deployment, operation (e.g., signature updating), and monitoring for hosts and applications (e.g., spam email) 	<p>Cyber ██████████ has cyber insurance.</p> <p>IDS/IPS ██████████ uses internet edge IDS/IPS (i.e. NextGen firewall - feature for IDS/IPS) ██████████ is utilized for logging of the servers. It is checked daily but does not have automatic alerts</p> <p>Antivirus and malware software ██████████ is deployed on all servers and workstations and knows when the host does not have malware defense</p> <ul style="list-style-type: none"> • Cisco FTD (firepower threat defense) is utilized. <p>Spam filtering</p> <ul style="list-style-type: none"> • Ironport is utilized for cloud email security • PhishER from KnowB4 provides additional visibility and gives end users ability to report spam to ██████████ <p>Web Filtering</p> <ul style="list-style-type: none"> • Currently, ██████████ has a Cisco web security appliance that does web filtering, reputation scores and whitelisting as needed. They will be switching to Umbrella in a few months. • Cisco web reputation scores are utilized. • Sites are whitelisted as needed. 	<p>Poor host intrusion and malware defense practices resulting in system vulnerabilities/weaknesses that lead to a loss of data availability, integrity, or confidentiality, reputational damage, and/or monetary loss and penalties.</p>	<p>LOW</p>	<p>HIGH</p>	<p>MED</p>

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Information Security This area focuses on the IT department's practice of information security. Information security programs are developed to protect an organization's information systems and information from plausible threats and vulnerability exploitation that could result in one or more losses of security: confidentiality, integrity, availability, authenticity and/or non-repudiation. Programs should address the following:</p> <ul style="list-style-type: none"> • Policy development and enforcement • Identity and access management • Threat identification and management • Vulnerability identification and management • Security roles and responsibilities • Security training and awareness for IT and non-IT personnel 	<p>Policy</p> <ul style="list-style-type: none"> • The Information Security Policy 2017 version in process of being updated. <p>Identity and Access Management</p> <ul style="list-style-type: none"> • There is no formalized process. The process varies between entities (gov/perm fund-templates/forms, growth fund-email, [REDACTED]). • Granting access to finance systems requires CFO approval. • For terminations, HR notifies [REDACTED] and a ticket is created. • Active Directory and critical application access is revoked same day (application access housed in data warehouse). • [REDACTED] checks weekly to audit the active directory audit queries to check for terminated users. • Granting privileged access follows a similar provisioning and deprovisioning process. • There are some shared admin accounts. The password is changed occasionally and generally when someone leaves. • The windows dashboard indicates how often the global admin account is used. Admin accounts are not included in VPN group. • There are also separate personal (non-admin) accounts used. • [REDACTED] reviews privileged access quarterly. <p>Risk Considerations: HR not always timely to communicate terms prior to term date. Employee transfers not always communicated and/or old access not always revoked (focus on new access).</p> <p>Security Training/Awareness</p> <ul style="list-style-type: none"> • KnowB4 used for end user and IT security training. There are required trainings for each group plus additional targeted training for users of critical data and onboarding training. • Training completion is tracked. • [REDACTED] conducts phishing tests. Currently, there is a 5.8% failure rate (improved from 10% last year). <p>Monitoring, Threat Logs and Risky User Reports</p> <ul style="list-style-type: none"> • Power BI is utilized. • MS sends alerts for risky users. This reviewed daily and followed up is conducted with users and they are required to reset their passwords. • [REDACTED] is working on implementing more advanced MS monitoring/threat detection tools (E3+). • Pen testing will be scheduled for August. 	<p>Under-developed information security program resulting in system vulnerabilities/weaknesses that lead to a loss of data availability, integrity, or confidentiality, reputational damage, and/or monetary loss and penalties.</p>	<p>LOW</p>	<p>HIGH</p>	<p>MED</p>

APPENDIX A: WRITING SAMPLES

████████████████████
 Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
Mobile Device Management This area focuses on the IT department's management of mobile devices. In-scope activities include the following: • Authorization to use mobile devices • Mobile device provisioning, monitoring, support and deprovisioning • Mobile device incident response	Overview • Airwatch used for all except "bring your own devices" (BYOD) which use Intune (BYOD only allowed for ██████████). • Mobile phones (iPhone and android) and iPad. • Access to email, SharePoint, OneDrive and MS teams. • Provisioning - Supervisor request to finance group to initiate purchase with AT&T. When phone received Finance creates ticket for ██████████ and provides procurement approval information, device enrolled in Airwatch then delivered to end user. • Deprovisioning - Offboarding process with HR, HR creates helpdesk ticket or reaches out directly to ██████████ for termination. Ticket created. Active directory linked to Airwatch so upon termination notification sent to Airwatch (puts device in hold status until ██████████ confirms unenrollment of device from Airwatch). Manager submits request that Finance terminate AT&T line and retrieves device from employee (or HR). • Transfers are coordinated internally with department managers to collect the device then ask ██████████ to deprovision device to another user in their department. Support • Desktop team handles and escalates to Landri as needed • Helpdesk can pull up limited device information • Desktop team (tier 2) has more access into the mobile device • Aaron/Landri (tier 3) can pull up full info (e.g. mobile tracking) Monitoring • iOS and android devices are encrypted. Check for devices that have not checked in within 7, 14 and at 30 days halts communication. Alerts go to the helpdesk then desktop team then Landri as needed, check for active passcode and version is checked and the unenrollment process begins. If the user calls the helpdesk they check for device enrollment and escalate to tier 2 support. Incident Response • Lost phone - Airwatch logs location, if not contact apple for location support. Send command to wipe (also would wipe automatically after 10 pin failures). If cannot locate request Finance to turn off and contact apple enterprises services to add to protected list to prevent reactivation (notify if attempted). • Android more open architecture - Launch a block with AT&T and when device reported stolen, will send command to the device to do an erase. Do not have the ability for BYOD/personal devices - can only manage the applications and must go into Intune and remove that device's access which will uninstall the Microsoft apps.	Poor mobile device management practices causing a data breach resulting in loss of data confidentiality.	LOW	MED	LOW

APPENDIX A: WRITING SAMPLES

[REDACTED]
 Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
	<p>Security</p> <ul style="list-style-type: none"> - Currently, in an open state but beginning to migrate over to full apple ecosystem and deploying apple device enrollment to program to have supervised access to corporate devices they own. There is a whitelist for applications on corporate devices. - Cryptographic mechanisms to protect enterprise data. - Pin is utilized and native email is encrypted. Wipe after 10 incorrect login attempts. Android employ Boxer (email client) so that everything is encrypted and copy/paste and screenshots not allowed. - ActiveSync protective controls (e.g., PIN#, mandatory storage encryption, remote wipe), Protect email content, contact and calendar entries that are sourced from [REDACTED] Exchange Server, Control camera and microphone usage, Provide "jail break" protection. - Create a user area and a SUIIT-controlled area. Disallow non-authorized programs from accessing the [REDACTED]-controlled storage area. - Airwatch agent scans. <p><i>Risk Considerations:</i></p> <ul style="list-style-type: none"> - Android more open architecture and ability to side load software onto their devices. There are policies to prevent this, but cannot prevent 100% so are working to change policy to only use apple devices. - Apple email client is pin-related risk because does not require additional pin/password like the other apps. 				

APPENDIX A: WRITING SAMPLES

[REDACTED]

[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Operations and Monitoring This area focuses on the IT department's practices for operating, monitoring and maintaining the computer systems and supporting infrastructure that are used by the work staff. In-scope activities include the following:</p> <ul style="list-style-type: none"> Capacity management Hardware and software maintenance 	<p>Capacity management</p> <ul style="list-style-type: none"> There is no formal capacity planning. However, the centralization of IT (with related strategic plan) provided a better understanding of system, storage, memory Primarily managed within [REDACTED] on an ongoing basis, but meetings are also held with stakeholders during budget season to determine potential needs for additional capacity. Daily standup meetings and team meetings, monitoring capacity System monitoring in Microsoft system center as well as VMware environments, and some other tools for network that are used to monitor capacities. Network tools - Pixier and more recently installed StealthWatch (CISCO) Targets - Targets related to delivery and uptime of service in SLAs. Outages recorded in ticketing system including information on the cause and downtime, reported monthly to tribal council. <p>System maintenance (Hardware/software)</p> <ul style="list-style-type: none"> Hardware maintenance - done mostly internally (use vendors for new install or products less familiar with) Software maintenance/patching - staggered each month starting with windows update; roll out to dev, prod, etc. servers. Clients pushed out in same manner. Third party updates completed through Avant. <p><i>Risk consideration: A few business areas have legacy software not supported on newer versions or have conflict with patches. Work with business units to get as patched as possible without impacting services and provide recommendations to replace legacy software</i></p> <p>COVID</p> <ul style="list-style-type: none"> A bit of a challenge, but pleasantly surprised on how well the transition went on the IT side. Looking forward there are some capacity and architectural concerns such as VPNs configured a particular way to previously only manage a small number of people, now adjusting to manage larger numbers of people for this access and ensuring better supportability of a larger remote workforce that will be incorporated into the environment. 	<p>Poor computer operations and monitoring/maintenance practices causing loss of system security and availability, increased costs from insufficient planning/forecasting, and disruption of business operations.</p>	MED	HIGH	HIGH

APPENDIX A: WRITING SAMPLES



Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
Organizational Architecture This area focuses on the organization of the IT department, its placement within the organization and its approach to staffing.	Centralizing the IT function <ul style="list-style-type: none"> As a result reduced IT spend from \$45 million to \$22M per year. Before there were 6-7 IT Directors, now less staff is needed. Outages and time to resolution has been reduced. Org structure allow for effective service delivery <ul style="list-style-type: none"> The help desk was moved from the PMO/Back Office team to the operations department last year which has allowed for better interfacing with higher tier groups. Greater communication is needed both internally and with the business units. Management could do a better job by working together. Staffing <ul style="list-style-type: none"> Outside of the key management positions they are well-staffed. Overall reduced head count by 20% as part of centralization. No formal succession planning being performed. Nearly zero turnover which is good for institutional knowledge but has resulted in staff being at the higher end of the salary scale. Entry level positions are hard to fill. Recruiters are utilized and searches must extend beyond the local area. Previously noted (from 2019 cyber risk assessment) qualified staff are hard to find due to locale, as well as retention of staff once trained. Staff/Resource Deployment <ul style="list-style-type: none"> Resource leveling exercises are completed as needed. On-going production support needs and availability is considered during project planning. Staff is cross trained informally, new skills are learned and broaden to avoid silos when people get sick and go on vacation. Have been trying to address single points of failure, but still a couple areas where an individual is heavily relied upon. Staff are assigned to support specific applications/systems and at a minimum have an owner and backup for each. No contractual employees currently to ensure control, maintain in-house knowledge and manage costs. Network security and managed service providers in a few areas may be utilized in the future, or part time CISO. 	Poor organizational structure and staffing causing communication gaps, lacking knowledge/skillssets, excessive workload, or decreased productivity resulting in poor service delivery.	LOW	MED	LOW

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Physical and Environmental Controls This area focuses on IT physical and environmental safeguards that are deployed to protect the organization's application systems and information. In scope activities include the following:</p> <ul style="list-style-type: none"> • Deployment and monitoring of physical access controls that protect IT assets • Deployment and monitoring of environmental controls that protect IT assets 	<p>Data Centers</p> <ul style="list-style-type: none"> • All employees must have licenses and certifications related to HIPAA, CJIS, etc. • Infrastructure is being migrated so it will be enveloped into • There are two ISPs (Century Link and Fast Track). <p>Access</p> <ul style="list-style-type: none"> • Networking team has access all three data centers, some helpdesk personnel have access to and facilities manager has access. • Facilities manager manages access to Growth Fund building and manages access to <p>• Multiple tools are utilized for badging Solutions. There is an initiative to consolidate solutions.</p> <ul style="list-style-type: none"> • Access provisioning/deprovisioning is documented and tracked in the ticketing system. Access is granted in the system. Email request is sent to facilities manager for the Growth Fund. Separation checklist includes revoking badge access. <p>Environmental controls at all three data centers</p> <ul style="list-style-type: none"> • Temperature sensors - alerts if thresholds exceeded for temperature and humidity. • Fire detection/suppression - water-based solution but considering moving to halon. • UPS/PDU power - monitoring is in place. Power outages are frequent but they have backup generators across the campus. • Security cameras are in all data centers. They are visible by police, dispatch, and employees. • Data replication between the three data centers for the entire tribe. 	<p>Lack of proper physical and environmental safeguards over data centers causing unauthorized access or physical damage resulting in loss of data or hardware.</p>	<p>LOW</p>	<p>HIGH</p>	<p>MED</p>

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Problem Management and Incident Response This area focuses on the IT department's practices for managing problems and incidents. In scope are the following activities:</p> <ul style="list-style-type: none"> The method(s) by which IT problems are reported and resolved Problem tracking, reporting and communication Incident response preparation and response testing Incident identification, triaging, containment, eradication and recovery 	<p>Monitoring</p> <ul style="list-style-type: none"> 24/7 issue monitoring and notification via phone and email. PhishER (KnowB4) - to flag suspicious emails which generates a helpdesk ticket. Issues are triaged to SAN/LAN team for investigation. If exposure, change password and then ESET scan. OpenDNS and Umbrella is being implemented. <p>Problem Tracking</p> <ul style="list-style-type: none"> Tracked via HEAT ticketing system and in PhishER. Working to implement a risk register tool. MS Office 365 software that monitors risky sign ins (e.g. accessing from unknown source). <p>Reporting</p> <ul style="list-style-type: none"> Added cyber inquiry to helpdesk ticket categories. Ticket type reporting monthly to the head of each business unit and Tribal council. Average of 75-100 tickets per month. Planning to pull this data into a BI system (currently excel/pivot chart reporting) <p>Incident Response</p> <ul style="list-style-type: none"> High level incident response procedure is documented currently (does not define roles and responsibilities). There is a process for high impact incidents. Root cause analysis performed if it is a serious incident. The incident response plan has not been tested. Planning to get Gartner's assistance for an annual exercise going forward. 	<p>Ineffective management of IT problems and incidents causing loss of IT asset confidentiality, integrity and availability resulting in impacts to business operations, reputational damage, and/or monetary loss and penalties.</p>	MED	MED	MED

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Procurement and Service Provider Management This area focuses on the IT department's practices for procuring hardware, soft-ware, facilities and services as well as managing the contracted service providers. In scope are the following activities: • Procurement strategy • Vendor and service provider due diligence and performance monitoring</p>	<p>Process • Quotes received and sent to purchasing, PO created then signed based on the required authority levels. PO sent to vendor and when invoice received it is submitted to A/P for processing in PeopleSoft. • CIO [redacted] authorizes items that are out of budget. The Perm Fund issues a memo of unbudgeted items or email approval from appropriate authority level, [redacted] keeps a folder and attachments in PeopleSoft. Approvals • The procurement approval process is more manual (obtained via signatures). Authority matrix with thresholds for approval. • A/P process is automated through PeopleSoft. Large System/Application Requests • During budget process, business areas would get preliminary budget approval and work with IT to determine what would be a good fit for them and [redacted] can identify if there is an existing tool already being used within the tribe. • Formal process for submitting memo of needs/requirements and obtaining approvals. Vendor Selection/Evaluation • Formal procurement process for RFP/quotes and evaluation. Strategic Procurement • They have a Gardner subscription; Gardner representative will review and consult on alternatives and options for negotiation and cost effectiveness for services/equipment being procured. • Have improved within [redacted] operations team in terms of evaluating purchases to determine what they really need and opportunities to consolidate (would previously over purchase). • Focus on establishing contracts for higher spend items in order to incur savings. • Note: PeopleSoft contract ending so they will be moving to year-to-year contracts Supplier/vendor performance monitoring • There is no formal process for supplier/vendor performance monitoring • No tracking or SCORE cards. • Generally obtain preferred best in class vendors so do not have issues with vendors. Any concerns identified by [redacted] or communicated from end users, [redacted] would assess and take appropriate action. Vendor oversight/security controls • Security audits are performed for some vendors. • Cloud use policy - obtain SOC report from the vendor. If they don't have a SOC (currently one vendor) they require this cloud use questionnaire. • Consultants cannot promote to production. • Any vendor changes are monitored (remote in with vendors). • Sign in/out of data centers. • During contracting, legal requires SUSS to know if vendor would have access to tribal data and would include language into the contract.</p>	<p>Insufficient procurement practices and oversight of vendors/service providers resulting in higher spending, product/service delivery problems, or security issues.</p>	<p>LOW</p>	<p>LOW</p>	<p>LOW</p>

APPENDIX A: WRITING SAMPLES

Risk Assessment Results & Proposed Internal Audit Plan

APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
<p>Project Management This area focuses on the IT department's project management practices. In-scope activities include:</p> <ul style="list-style-type: none"> Initiating, planning, executing, controlling, and closing projects Managing projects' scope, milestones, quality and budget Ensuring projects are adequately staffed Reporting project progress and issues on a recurring basis to management and stakeholders 	<p>Project Requests</p> <ul style="list-style-type: none"> There are two project managers but the processes not formal. Requests are addressed during the budget process. Each organization submits request to senior management and they are vetted for collaboration. There are PMO tools and templates. There is a strict capitalization method to determine if capital project. Standard naming conventions are used and time is tracked for projects. <p>Project Determination</p> <ul style="list-style-type: none"> Determination of an official project is based on established level of effort by hours (160 hours or more). <p>PM Methodology/approach</p> <ul style="list-style-type: none"> PM methodology/approach is not strictly defined or documented but currently moving towards Agile. Management have weekly standup meetings with project leads and others involved to discuss project scope, status, issues and next steps, outcomes/quality. Time is tracked and charged to projects. oversees the budget to actual with a monthly report and provides overrun statuses. Project status is reported to tribal council and committee along with status of other initiatives. <p><i>Risk consideration: During growth fund and user meeting it was noted that in the past year has no longer been using PM consultants on their larger projects. Experience was split with one functional area (Finance) noting a lack of PM support, and another area (Energy) indicating internal project management is organized and effective (improvement from prior year).</i></p> <p>Project staffing</p> <ul style="list-style-type: none"> There are two project managers Typically do not need to hire contractors but will as needed. Using MS to track time, periodically monitored by . They are looking into a BI tool to have this information available in a dashboard. <p><i>Risk consideration: VP of project management existed previously but role is vacant and will not be replaced.</i></p>	<p>Poor project management resulting in cost/schedule overruns or unmet customer needs, impacting business operations.</p>	LOW	LOW	LOW
<p>Risk Management This area focuses on the IT department's risk management practices. In-scope activities include IT risk identification, triaging, treatment, tracking and management reporting.</p>	<p>Risk Management Practices</p> <ul style="list-style-type: none"> There is no formal risk framework being followed. Maintain an excel spreadsheet with risk prioritization that they review/update monthly for only technical cyber-related risks (e.g. from vulnerability scans, from vendors); No scoring or formal discussion of likelihood and severity or internal controls. They track completion on a backlog board in MS Planner but not tracking how they are resolved. Currently looking into a risk register tool to procure and assign someone to monitor. Vacant leadership positions is delaying this from being completed. 	<p>Lack of awareness and management of internal and external technology risks caused by inadequate risk management practices resulting in severe impacts to the tribe and its operations.</p>	MED	MED	MED

APPENDIX A: WRITING SAMPLES

████████████████████
 ██████ Risk Assessment Results & Proposed Internal Audit Plan
 APPENDIX B: DETAILED RISK MATRIX

IT Risk Area	Current State Notes	Risk Statement	Likelihood	Impact	Risk Severity
Strategy and Governance This area focuses on IT strategy and governance practices. In-scope activities include the following: • Development, maintenance and approval of an IT strategic plan that is aligned with the organization's business strategy • Development and execution of tactical IT plans that are aligned to the IT strategy • Development, maintenance and approval of an IT operating budget • Recurring performance and risk reporting to Executive Management and the Board of Directors • Oversight of IT operation and resource consumption by Executive Management and the Board of Directors	Strategy • Overall tribe has a mission but there is no strategic plan. A formal IT strategic plan does not exist, but prior CIO would roll out annual strategic priorities during the budgeting process. • IT strategy driven by annual budgeting process. Gather input from end users, informally prioritize based on ██████ resources and urgency of end user needs. On operations side, review what needs to be replaced. Governance/Oversight • Meet with Shared Services Committee monthly on status items and approvals needed • Twice monthly meetings with ██████ presenting operational report (projects, heat ticket and outage numbers, SLAs). Second meeting of the month covers financial statement and budget to actuals; HR update - info on TERO compliance, changes in staffing/terms/hires. Monthly work sessions for anything to discuss in more detail and to discuss initiatives from a high level. Discuss security risks with tribal council often (e.g. recently shared threat map) • Monthly or every other month meet with Executive Officers to discuss items at a tactical level, go through monthly report/status/SLA performance, and any areas where help is needed. These meetings have been halted during COVID. Policy and procedures • No formal policy and procedure process development and approval process. Most IT policies shared with ██████ committee for approval, but some in the past implemented by the CIO. • HR generally dictates policies as a result of them being the only ones able to enforce them. Issues with this due to there being 3 different HR groups (perm, growth fund, casino) with different policies. Tone at the top • Issues with turnover in Executive Officer roles as they run operations on day-to-day basis and term only lasts 3 years. Disruptive to ██████ depending on their priorities and motivation to increase/decrease spend on technology	Poor IT strategy and governance practices resulting in the inability to properly oversee and manage IT functions and align with the tribe's needs and priorities.	MED	MED	MED

APPENDIX A: WRITING SAMPLES

[REDACTED]
[REDACTED] Risk Assessment Results & Proposed Internal Audit Plan
CONTACT INFORMATION

Contact Information

If you have any questions about this report, please contact:

Joel Laubenstein
Principal, Baker Tilly
joel.laubenstein@bakertilly.com

Atit Shah
Cybersecurity Principal, Baker Tilly
Atit.Shah@bakertilly.com

Brian Nichols
Cybersecurity Director, Baker Tilly
Brian.Nichols@bakertilly.com

Kyle O'Rourke, MPA, CIA, CRMA, CGAP
Engagement Manager, Baker Tilly
kyle.orourke@bakertilly.com

Stacey Gill, CISA
Project Manager, Baker Tilly
stacey.gill@bakertilly.com

Tiffany McCoy, MSAA, CFSA, CSOE
Consultant, Baker Tilly
tiffany.mccoy@bakertilly.com

02-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

Client Cybersecurity Audit Program - Full Scope

Area	Control #	Control Description	Testing procedures	Results	Pass/Fail	Ref. Workpaper	RFI
1. Asset Management (AM)							
AM	1.1	Physical devices, information systems and applications within the organization and hosted by third parties are inventoried.	1. Obtain a list of physical devices, systems and software inventory. Review the inventory considering the following: a. Scope of physical devices and systems is documented based on the organization's risk appetite (e.g., systems/software that access, store and/or process sensitive information, allow access to the network, hosted by third parties, or are critical to business operations (ERPs)) b. Completeness of inventory (e.g., location, asset number, version, system, vendor, owner, etc.) c. Inventory collection process ensures new devices and software are collected accurately and in a timely manner (e.g., automated software to detect and/or store the inventory) d. Frequency of inventory reviews				a. List of physical devices, systems and software inventory within the organization or hosted by third parties
AM	1.2	Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality and business value.	1. Obtain a copy of the organization's data classification program (classification may also be identified in the risk assessment or business impact analysis). 2. Review the list of physical devices, systems and software within the organization or hosted by third parties and determine if they are classified and prioritized based on criticality and business value.				X a. Organization's data classification program/framework b. Documented classification of physical devices, systems and software within the organization or hosted by third parties
AM	1.3	Organizational communication and data flows are mapped.	1. Obtain current copies of data flow diagram(s) (DFD), logical network diagram(s) (LND), and/or other diagrams to show organizational communication and data flow. a. Ensure the flow diagrams are accurate and up to date b. Frequency of review and update				a. Current copies of data flow diagram(s) (DFD), logical network diagram(s) (LND), and/or other diagrams to show organizational communication and data flow
AM	1.4	Installation and execution of unauthorized software is restricted.	1. Obtain a copy of the asset management policy and verify software installation is restricted. 2. Determine if a mechanism is in place to restrict the installation and execution of unauthorized software.				a. Asset management policy b. Evidence the installation and execution of unauthorized software is disabled.
2. IT Strategy and Business Continuity (ISBC)							
ISBC	2.1	The organization IT strategic plan, cybersecurity strategy and business continuity plan are clearly defined	1. Obtain documentation or evidence that an overall IT strategic plan exists and review if it includes: a cybersecurity strategy, business continuity plan, information system acquisition procedures, business impact analysis, acquisition/procurement process, security hardening guidelines, key supplier reviews, supplier relationship management, supplier due diligence reports, etc..				a. Overall IT strategic plan b. Cyber security strategy c. BCP/DR strategy
ISBC	2.2	Critical functions for the delivery of critical services are established.	1. Obtain the organization's business continuity plan, disaster recovery plan, business impact analysis and risk assessments and review for the following: a. Information systems and software supporting critical business functions are identified and prioritized based on maximum allowable downtime. b. Third parties who support critical business functions and information systems/software are identified and prioritized. 2. Determine if the organization's business continuity and disaster recovery plans (including business impact analysis) support resilience of critical services. 2. Determine if appropriate due diligence (e.g., business continuity plans (BCP), service level agreements (SLA), Service Organization Control (SOC) reports) is in place and reviewed to ensure resilience requirements of the organization can be met by critical third-party services.				a. Business Continuity/Disaster Recovery (BCP/DR) and related artifacts (BIA, business impact analysis (BIA), risk assessments (RA), etc.) b. Service level agreements (SLA) (if any) c. Service Organization Control (SOC) reports (if any)
ISBC	2.3	The organization has obtained cyber liability insurance to manage the financial impact of a cyber incident.	1. Obtain and review the cyber liability insurance policy to verify coverage is appropriate.				a. Cyber liability insurance policy
ISBC	2.4	The organization's mission is documented and communicated to employees.	1. Obtain the organization's mission statement. 2. Determine if the organization's mission statement is communicated to employees.				a. Organization mission statement.

3. IT Governance (ITG)				
ITG	3.1	Organizational information security policy is established.	<p>1. Obtain a copy of the information security policy.</p> <p>2. Determine if the policy is complete and has been approved (by a governance structure within the organization). The policy should cover the following areas:</p> <p><i>Acceptable Use of Information Resources</i></p> <p><i>Access and Authentication Policy</i></p> <p><i>Anti-Virus and Anti-Spyware Management Policy</i></p> <p><i>Asset Management Policy</i></p> <p><i>Audit Logging and Monitoring Policy</i></p> <p><i>Backup and Recovery Policy</i></p> <p><i>Bring Your Own Device (BYOD) Policy</i></p> <p><i>Business Continuity Policy</i></p> <p><i>Clear Desk Policy</i></p> <p><i>Corporate Email security Policy</i></p> <p><i>Data Classification, Handling, and Protection Policy</i></p> <p><i>Data Retention and Disposal Policy</i></p> <p><i>Exception Management Policy</i></p> <p><i>Incident Response Policy</i></p> <p><i>Network Device Configuration Policy</i></p> <p><i>Physical Security and Access Policy</i></p> <p><i>Remote Access Policy</i></p> <p><i>Risk Management Policy</i></p> <p><i>Security Testing Policy</i></p> <p><i>Security Training Policy</i></p> <p><i>Server and Computer Configuration Policy</i></p> <p><i>Software Development Life Cycle (SDLC) and Change Management Policy</i></p> <p><i>Third Party Management Policy</i></p> <p>3. Determine if the policy is communicated to employees.</p>	a. Documented security policy
ITG	3.2	Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	<p>1. Determine if information security roles and responsibilities are defined. (i.e. Roles and responsibilities may be defined in policies, job descriptions, agreements, RACI charts, hierarchy charts and/or contracts).</p> <p>2. Determine if there is sufficient independence within the information security roles in order to provide adequate separation of duties for critical functions.</p> <p>3. Review contracts, nondisclosure agreements (NDAs) and service level agreements (SLAs) with critical vendors to determine if cybersecurity controls and incident notification are addressed appropriately.</p>	<p>a. Documented evidence where security roles and responsibilities are defined (i.e. policies, job descriptions, RACI charts, contracts)</p> <p>b. Contractual agreements with critical vendors</p>
ITG	3.3	Exceptions to information security policies are documented and tracked for remediation.	<p>1. Review the organization's policy exception management process to identify if known policy exceptions are properly documented and monitored.</p>	<p>a. List of policy exceptions</p> <p>b. Exception remediation plans and timelines</p>
ITG	3.5	Legal, regulatory, and contractual obligations regarding cybersecurity are catalogued.	<p>1. Review a register of legal, regulatory, and contractual obligations.</p> <p>2. Determine if compliance to obligations is tracked and updated when needed.</p>	a. List of compliance obligations
4. Risk Assessment (RA)				
RA	4.1	Threats and vulnerabilities, both internal and external, are identified and reported.	<p>1. Review IT risk assessment to determine if internal and external threats are identified and documented. Identify if likelihood and potential business impacts and sufficient controls are documented to mitigate the risk associated with those threats.</p> <p>2. Determine if the organization is a member of or subscribes to a threat and vulnerability information sharing organization (e.g., United States Computer Emergency Readiness Team [US-CERT]).</p> <p>3. Determine if processes are in place to provide threat and vulnerability information to appropriate functions with the right knowledge and expertise to develop risk mitigation plans.</p> <p>4. Determine if formal processes are in place to actively monitor and report potential threats (i.e. to the board, senior/executive management).</p>	<p>a. IT Risk Assessment (including documentation of internal and external threats)</p> <p>b. Documented threats and vulnerabilities likelihood and potential business impacts</p>
RA	4.2	Risk management processes are established, managed and agreed to by organizational stakeholders.	<p>1. Evaluate the framework or process used for risk management. Consider the following:</p> <p>a. Is the process formally documented?</p> <p>b. Is the process regularly updated?</p> <p>c. Is the process repeatable and measurable?</p> <p>d. Does the process have an owner?</p> <p>e. Are stakeholders involved or informed of the process?</p>	a. Documented Risk Management process/plan
RA	4.3	Risk responses are identified and prioritized.	<p>1. Obtain the risk management plan in response to recently identified risks in the risk assessment. Determine if sufficient controls are identified to mitigate the risks or if rationale is documented for risk acceptance in accordance with the organization's risk appetite.</p> <p>2. Determine if risk responses to recent threats and vulnerabilities are prioritized according to risk levels.</p>	a. Risk management plan in response to recently identified risks

20-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

RA	4.4	Third-party service provider risks are assessed, documented, and managed.	<ol style="list-style-type: none"> 1. Review the third-party vendor risk assessment procedure 2. Validate that third-party vendor risk assessments have been performed and are documented 3. Review documented findings and identify how the identified risks are being managed 	<ol style="list-style-type: none"> a. Inventory of third-party service providers b. Contracts with third-party service providers c. Third-party risk assessment documentation, including findings and next steps
RA	4.5	Third-party vendors are prioritized based on criticality to the organization.	<ol style="list-style-type: none"> 1. Review the third-party management policy and determine if criticality levels are outlined. 2. Determine if the criticality of a third-party vendors is defined during the risk assessment. 3. Validate that third-party vendors are labeled and prioritized based on the criticality to the organization. 	<ol style="list-style-type: none"> a. Inventory of third-party service providers b. Third-party risk assessment c. Third-party risk management policy, including criticality definitions and assessment procedures
RA	4.6	Contracts with critical vendors include provisions for activities that occur following the conclusion of a service agreement.	<ol style="list-style-type: none"> 1. Obtain the third-party management policy and determine if a policy is in place for cybersecurity related activities that must occur following the termination of a third-party service agreement. 2. Obtain the contracts of critical vendors and verify provisions are in place for activities that occur following contract termination. 	<ol style="list-style-type: none"> a. Third-party management policy b. Contractual agreements with critical vendors
5. Access Controls (AC)				
AC	5.1	Remote access is managed.	<ol style="list-style-type: none"> 1. Determine whether policies and procedures related to remote users' access capabilities are formalized. Consider the following: <ol style="list-style-type: none"> a. Remote users (e.g., employees, contractors, third parties) with access to critical systems are approved and documented. b. Remote connections are only opened as required. c. Remote connections are logged and monitored. d. Remote connections are encrypted. e. Strong authentication is in place (e.g., multifactor, strong password parameters). f. Institution of security controls (e.g., antivirus, patch management) on remote devices connecting to the network. 	<ol style="list-style-type: none"> a. Remote user access policies and procedures
AC	5.2	Privileged access is restricted and managed	<ol style="list-style-type: none"> 1. Determine whether access to network devices (e.g., servers, workstations, mobile devices, firewalls) is restricted to appropriate users (access profiles are consistent with job functions). Compare a sample of users' access authority with their assigned duties and responsibilities. 2. Determine if users with local administrative privilege on workstations require this level of access. 3. Review how access to sensitive data by users with elevated network privileges is restricted and/or monitored. 4. Determine if role-based access controls are implemented (e.g., roles vs. users are assigned access rights). 	<ol style="list-style-type: none"> X a. Admin access list to the network, network devices b. List of user with local admin access c. IT Org. chart
AC	5.3	Network integrity is protected, incorporating network segregation where appropriate.	<ol style="list-style-type: none"> 1. Review network diagrams and data flow diagrams and consider the following: <ol style="list-style-type: none"> a. High-value/critical systems (e.g. ERPs) are separated from high-risk systems (e.g., VLAN, DMZ, etc.) where possible. b. Main Wi-Fi network is separated from Guest networks 2. Formal processes are in place to approve/change data flows and/or connections between networks and/or systems. 	<ol style="list-style-type: none"> a. Network topology and data flow diagrams
AC	5.4	End user access to company data and systems is managed.	<ol style="list-style-type: none"> 1. Review the organization's user access provisioning and deprovisioning procedures 2. Review the technology utilized to manage user access requests and inventory individual user access rights 	<ol style="list-style-type: none"> a. User access policies and procedures
AC	5.5	Multifactor Authentication is in place for higher risk access procedures	<ol style="list-style-type: none"> 1. Review the organization's use of multifactor authentication (MFA) 2. Review the technology utilized to enable MFA controls 	<ol style="list-style-type: none"> a. Multifactor authentication procedures
AC	5.6	Physical access to data center facilities, computer rooms, and networking closets is properly managed.	<ol style="list-style-type: none"> 1. Review physical access provisioning and deprovisioning processes 2. Review the technology in place to manage and monitor physical access 	<ol style="list-style-type: none"> a. Physical access policies and procedures b. Physical access user list
6. Information Protection Processes and Procedures (IP)				
IP	6.1	Security policies, processes, and procedures are maintained to manage protection of information systems and assets.	<ol style="list-style-type: none"> 1. Determine if baseline configurations are adopted to harden the security of information systems (e.g., Center for Internet Security [CIS] benchmarks, Security Technical Implementation Guides [STIG]) for systems (e.g., servers, desktops, routers). 2. Determine if tools (e.g., security event and information management systems [SIEMs]) are used to establish typical (baseline) traffic so abnormal traffic can be detected. 3. Sample systems against the baseline configurations to ensure standards are followed and enforced. 	<ol style="list-style-type: none"> a. Documented system baseline configurations and hardening guidelines (e.g. SIEM) b. List of mission-critical systems (i.e. servers) for which baseline configurations were applied

02-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

IP	6.2	Configuration change control processes are in place.	<ol style="list-style-type: none"> Determine if configuration change control processes for information systems are in place. Consider the following: <ol style="list-style-type: none"> Proposed changes are documented Changes are prohibited until designated approvals are received. Changes are tested and validated before implementation. Changes are documented and reported upon completion. 	<ol style="list-style-type: none"> Configuration change control process
IP	6.3	Data is destroyed according to policy.	<ol style="list-style-type: none"> Review media sanitization (data destruction) policies. Ensure sanitization techniques and procedures are commensurate with the security category or classification of the information or asset and in accordance with applicable federal and organizational standards and policies. Spot-check trash cans, dumpsters, shred bin and/or shredders to ensure compliance with policy. Obtain proof (e.g., destruction certificates) that media sanitization is occurring according to policy. 	<ol style="list-style-type: none"> Documented media sanitization (data destruction) policy Examples of media sanitization (e.g., destruction certificates)
IP	6.4	Response plans (incident response and business continuity) are in place and managed.	<ol style="list-style-type: none"> Obtain and review the incident response and business continuity plans to determine how the entity responds to a cyber incident. Evaluate the plans against standards and best practices and determine how frequently they are updated and approved (e.g., roles and responsibilities are defined, reporting and notification requirements, incident priority/impact classification, containment, mitigation, etc.) Response processes and procedures are executed timely (after detection of a cybersecurity event) Determine whether the plans are tested, or rehearsed, according to policy and any applicable guidance. And whether the plan is updated based on action items and lessons learned. 	<ol style="list-style-type: none"> Incident response plan Business continuity plan Copies of reports from recent incidents
IP	6.5	Recovery processes and procedures (incident recovery and disaster recovery plans) are maintained and executed to ensure timely restoration of systems or assets affected by cybersecurity events.	<ol style="list-style-type: none"> Determine whether recovery plans and procedures are documented, maintained and updated based on results of recent cybersecurity events or event tests. Determine if the plans and procedures include the following: <ol style="list-style-type: none"> Designation of points of contact within the organization to communicate with customers, partners, media, regulators and law enforcement Training for employees regarding where to refer questions about cybersecurity incidents Key positions responsible for managing the organization's reputation risk during cybersecurity incidents Timely and responsible notification of customers, partners, regulators and law enforcement of a cybersecurity incident Assess whether lessons learned and analysis of failed or missing controls are documented Validate that the recovery plans and procedures are updated and approved when changes are made to systems and controls or as a result of lessons learned from recent cybersecurity events or event tests. 	<ol style="list-style-type: none"> Documented recovery plans and procedures Recent cybersecurity events or event tests
IP	6.6	A vulnerability management plan is developed and implemented.	<ol style="list-style-type: none"> Obtain the documented vulnerability management plan and ensure it includes the following: <ol style="list-style-type: none"> Frequency of vulnerability scanning Method for measuring the impact of vulnerabilities identified (e.g., Common Vulnerability Scoring System [CVSS]) Incorporation of vulnerabilities identified in other security control assessments (e.g., external audits, penetration tests) Procedures for developing remediation of identified vulnerabilities 	<ol style="list-style-type: none"> Documented vulnerability management plan Sample vulnerability scanning report
IP	6.7	Data is protected when accessed on mobile devices	<ol style="list-style-type: none"> Obtain and review the mobile device management policy (or Bring Your Own Device Policy) Review the technical controls in place to manage company data stored on mobile devices, including: <ol style="list-style-type: none"> the organization's ability to ensure mobile devices are secured with the use of a passcode the ability to wipe data remotely company data from mobile devices when the device is reported lost/stolen or if the user leaves the company 	<ol style="list-style-type: none"> Mobile device management policy (or BYOD policy) Mobile device provisioning and deprovisioning process Mobile device wipe procedures
IP	6.8	Data backups are performed, protected, and tested for restorability.	<ol style="list-style-type: none"> Review the scope of data backups currently being performed Review the technology for performing backups is properly secured, including encryption of backup data and protection from ransomware encryption Review the restorability testing procedures 	<ol style="list-style-type: none"> Data backup policy and procedures Data backup restoration procedures Results from restoration testing

02-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

IP	6.9	Sensitive production data is sanitized prior to use in development or testing environments.	1. Review the procedures for using production data in development or testing environments to ensure any sensitive data is sanitized.	a. Data classification policy b. Data sanitization procedures
IP	6.10	Incidents are initiated, documented, and closed in accordance with the incident response plan.	1. Obtain and review the documented incident response plans and procedures and ensure they include the following: a. Criteria for when an adverse event should be defined as an incident. b. Criteria for when an incident should be closed. c. Requirements for incidents to be documented with supporting evidence. d. Procedures for containment and eradication of incidents. e. Criteria for when incident recovery should be performed. 2. Review sample incident reports and ensure they include the following in accordance with policy: a. Actions performed during the investigation. b. Any relevant data and metadata. c. Lessons learned during the incident. d. The categorization and prioritization of the incident. e. Activities performed to contain the incident. f. Activities performed to eradicate the incident.	a. Incident response policy and procedures b. Copies of reports from recent incidents
7. Maintenance Processes (MP)				
MP	7.1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.	1. Review controlled maintenance processes. Consider the following: a. Maintenance activities are approved, scheduled and documented (e.g., date and time, name of individual(s) performing maintenance, description of maintenance performed, systems removed/replaced) b. Maintenance staff or vendors are approved, authorized and supervised (if required). c. Maintenance tools and media are approved and inspected for improper or unauthorized modifications prior to use. 2. Determine whether remote maintenance on servers, workstations and other systems is performed. Consider the following: a. Whether a list of authorized third-party vendors is maintained and approved b. What software/version or service is used to connect c. What authentication requirements are in place (e.g., multifactor authentication) d. Whether the remote access is logged and monitored	X a. Documented maintenance process b. Sample maintenance log c. Documented remote service requirements
MP	7.2	The integrity and authenticity of hardware and software is verified prior to implementation.	1. Obtain the asset deployment policy and process. 2. Determine if integrity checking (i.e. visual inspection for anomalies, verifying serial numbers, checking model numbers) is performed prior to hardware being deployed. 3. Obtain the patch management policy and process. 4. Determine if integrity checking mechanisms (i.e. hash verification, restricting software downloads) are in place and performed prior to the deployment of software patches.	a. Asset deployment policy and process b. Patch management policy and process
8. Technical Security Solutions (TSS)				
TSS	8.1	Removable media is protected and its use is restricted according to policy.	1. Obtain a copy of the removable media policy. Review controls defined in the policy. Consider the following: a. Access to removable media is restricted (e.g., USB drives) b. Encryption of removable media is performed when used c. User training on the access and use of removable media d. Sanitization procedures for decommissioned media 2. Perform spot-checks on systems with removable media restrictions to ensure restrictions are working as expected and comply with the organization's policy.	a. Removable media policy b. Sanitization procedures for removable media

02-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

TSS	8.2	Audit/log records are determined, documented, and reviewed	<ol style="list-style-type: none"> Determine if audit logs (e.g., security, activity) are maintained and reviewed in a timely manner. Verify the adequacy of the logs to monitor and evaluate IT activities and security events. Consider the following: <ol style="list-style-type: none"> Audit records contain appropriate content (e.g., type of event, when the event occurred, where the event occurred, source of the event, outcome of the event, identity of any individuals or subjects associated with the event). Audit logs are protected from unauthorized access, modification and deletion. Audit log files are being backed up. Audit logs are monitored and reviewed. Identify responses to detected event and assess for reasonableness. 	<p>X a. Audit logs pertaining to the following:</p> <ul style="list-style-type: none"> - Network perimeter (e.g., intrusion detection systems [IDS], firewalls) - Microsoft systems (e.g., Windows event logs) - Non-Microsoft systems (e.g., syslog files for Unix/Linux servers, routers, switches) <p>b. Evidence of audit logs monitoring and review</p>
TSS	8.3	Forensic capabilities have been implemented either internally or through a formal relationship with a third-party incident response service provider.	<ol style="list-style-type: none"> Review computer forensic capabilities, or the contract with a third-party computer forensic service provider 	<p>a. Forensic service provider contract/retainer</p>
9. Security Continuous Monitoring (SCM)				
SCM	9.1	The network, physical environment and user activities are monitored to detect potential cybersecurity events.	<ol style="list-style-type: none"> Determine if monitoring controls at the network (e.g., firewall, router, switch), Operating System (e.g., server platforms, workstation platforms, appliances), and application (e.g., account, and database access) levels include detection of cybersecurity events. Consider: <ol style="list-style-type: none"> Network level: Denial-of-service [DoS] attacks, unauthorized account access, unauthorized file/system access, privilege escalation attacks, SQL injection attacks). Physical level: Sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports User level: Unauthorized account access, unauthorized file/system access, access out of hours, access to sensitive data, unusual access, unauthorized physical access, privilege escalation attacks 	<p>a. Evidence of cyber security event monitoring at the network, physical environment and user levels (e.g., Network: Denial-of-service [DoS] attacks, privilege escalation attacks, etc.); Physical: Physical access controls, Sign in/out logs, etc.; User: Unauthorized account/file/ system access, access out of hours, access to sensitive data, etc.)</p>
SCM	9.2	Malicious, Mobile codes and phishing attempts are detected.	<ol style="list-style-type: none"> Obtain a copy of the processes and procedures used to detect malicious code (e.g., malware, phishing email, intrusions, etc.), and mobile code (e.g., Java, JavaScript, ActiveX, Flash, VBScript) on the network, servers/workstations and devices. <ol style="list-style-type: none"> Installed on all applicable systems and network control points (e.g., anti-malware software on servers and workstations, phishing filters on email systems, intrusion prevention/detection systems on the network [IDS/IPS], endpoint security products on workstations and/or servers, etc.) Updated on a regular basis Configured to perform real-time scanning or periodic scans at regular intervals Are tested on a regular basis using test code (e.g., EICAR test virus) Determine if detective mobile code controls block unauthorized mobile code when detected. Consider the following: <ol style="list-style-type: none"> Detecting and blocking mobile code attachments in emails (e.g., .exe and .js files) Detecting and blocking mobile code portions of websites Removing the ability to run mobile code on systems that do not require this functionality (e.g., uninstalling Java from workstations without a need for it) Configuring systems to generate alerts and block execution when mobile code that is not signed with an approved code-signing certificate attempts to execute Spot-check workstations and other user endpoint devices to verify the following: <ol style="list-style-type: none"> Malicious code controls are installed and updated Mobile code controls are installed (e.g., Java is uninstalled, .exe and .js email file attachments are blocked) 	<p>X a. Documented processes and procedures to detect malicious code that is run on the servers, workstations and devices (e.g., anti-malware software, phishing filters, intrusion prevention/detection systems [IDS/IPS], endpoint security products, etc.)</p> <p>b. Documented processes and procedures to detect mobile code that is run on the servers, workstations and devices (e.g., quarantine, execution blocking, download blocking).</p> <p>c. Documented policy on the installation, use and security of mobile code (e.g., Java, JavaScript, ActiveX, VBScript, Flash, etc.)</p>
SCM	9.3	Vulnerability scans are performed.	<ol style="list-style-type: none"> Obtain a copy of the organization's schedule for performing internal and external vulnerability scans and the results of the most recent internal and external vulnerability scans. Review the schedule and results for the following: <ol style="list-style-type: none"> Frequency Successful completion Documented resolution or mitigation of identified vulnerabilities Scope of testing includes all critical systems (i.e., Static Site IPs, Website IPs, etc.) Determine whether vulnerability scan results were reported to individuals or teams with appropriate authority to ensure resolution. 	<p>a. Internal and external vulnerability scan results (most recent).</p> <p>b. Internal and external vulnerability scans schedule</p>
SCM	9.4	Third-party penetration testing is performed at least annually	<ol style="list-style-type: none"> Obtain and review the latest third-party penetration testing report to validate it was performed within the last 12 months Review the findings from the latest report to validate they have been remediated, or a plan is in place to remediate. 	<p>a. Penetration testing policy and procedures</p> <p>b. Results from latest penetration test</p>

02-11-2025 AUDIT COMMITTEE MEETING - A-2 IT AUDIT CONSULTANT FINALIST INTERVIEWS

SCM	9.5	Scanning is performed on internally developed applications to identify vulnerabilities in the source code. (e.g. Veracode static and dynamic code scanning)	<ol style="list-style-type: none"> 1. Obtain and review secure coding procedures for application developers 2. Review the technology used to scan internal source code for vulnerabilities 3. Review identified vulnerabilities to validate that they have been remediated, or a plan is in place to remediate. 	<ol style="list-style-type: none"> a. Secure code scanning/review policies and procedures b. Results from latest code scans
SCM	9.6	Resource capacity is monitored throughout the environment.	<ol style="list-style-type: none"> 1. Determine if monitoring controls at the network and servers include resource capacity monitoring (e.g., bandwidth, average response time, disk usage). 	<ol style="list-style-type: none"> a. Evidence of resource capacity monitoring of the network. b. Evidence of resource capacity monitoring of servers.
SCM	9.7	External service providers are monitored to detect potential cybersecurity events.	<ol style="list-style-type: none"> 1. Determine if external service providers are monitored to find potential incidents. Consider: <ol style="list-style-type: none"> a. Monitoring of physical and remote maintenance activities. b. Monitoring deviations from normal behavior. c. Notifications are received for incidents involving third-party service providers. 	<ol style="list-style-type: none"> a. Logs of third-party service provider activities
SCM	9.9	Logs are correlated from multiple sources.	<ol style="list-style-type: none"> 1. Determine if a SIEM solution or similar tool is in place. 2. Determine if logs from a variety of sources (i.e., IDS/IPS, User access, physical access, threat intelligence, etc.) are being ingested and correlated. 	<ol style="list-style-type: none"> a. Evidence of logs from a variety of sources being ingested into a security information and event management solution or similar tool for correlation across logs.
10. Awareness Training (AT)				
AT	10.1	All users are informed and properly trained on the use of information systems.	<ol style="list-style-type: none"> 1. Obtain and review the IT Policy and/or acceptable use policy (AUP) and ensure the content is adequate. 2. Review the security training and continuing education programs and/or materials and validate the following: <ol style="list-style-type: none"> a. Specific role-based training is assigned based on roles and responsibilities (i.e., end-users, privileged users, senior/executives, security/cybersecurity roles, etc.) (e.g., users with elevated privileges are taught security roles and responsibilities associated with elevated privileges, etc.) b. A method is in place to measure cybersecurity knowledge and understanding against organization requirements (e.g., tests, quizzes, etc.) c. Training and education materials are updated to reflect changes in the threat environment d. Frequency of training (e.g., cybersecurity training of all employees is conducted annually at a minimum) 	<ol style="list-style-type: none"> a. IT Policy and/or acceptable use policy (AUP) (e.g., use of IT systems and equipment, information, email, internet, IT devices, etc.) b. Security training and continuing education programs and/or materials
AT	10.2	Third-party stakeholders (e.g., suppliers, customers, partners) understand security roles and responsibilities.	<ol style="list-style-type: none"> 1. Review applicable third-party contracts, customer agreements, and partner agreements to ensure security roles and responsibilities are clearly defined. 2. Review the organization's vendor management program to ensure third parties are complying with cybersecurity responsibilities defined in contracts and agreements. 	<ol style="list-style-type: none"> a. Sample third-party contracts and/or agreements
AT	10.3	Phishing awareness campaigns are utilized to educate users about email social engineering risks.	<ol style="list-style-type: none"> 1. Review phishing campaign scope and frequency 2. Review phishing campaign reporting metrics and training requirements of users that fell for the phishing test 	<ol style="list-style-type: none"> a. Phishing campaign procedures b. Results from latest phishing campaign



Appendix B: Curriculum Vitae

MANAGING DIRECTOR



Chris Kalafatis, CPA, CIA, CFE

Chris is managing director of the firm's public sector industry within the Risk Advisory practice and offers extensive experience with internal audit, IT audit and fraud risk management.



Baker Tilly US, LLP

T: +1 (703) 923 8007

christoper.kalafatis@bakertilly.com

bakertilly.com

Education

Bachelor of Science in Accounting,
Virginia Commonwealth University

Chris is a self-motivated leader with 25+ years of audit and consulting experience and leads Baker Tilly's risk advisory public sector practice. He consistently delivers on commitments and achieves individual and team goals and offers strong management abilities, setting high expectations for himself and the teams he leads.

Specific experience

- Led projects with 50+ public sector entities and 10+ Fortune 1000 companies
- Directed financial, operational, IT, SOX and compliance audits
- Supervised or performed 200+ fraud investigations
- Presented audit reports and investigations to Audit Committees and Executive Management
- Served as Chief Audit Executive for multiple Internal Audit outsource relationships
- Identified internal control issues and operational deficiencies that impacted service delivery to citizens, caused financial losses to state and local governments, and non-compliance with laws and regulations
- Uncovered collusion between City employees and a vendor that led to the arrest of nine individuals. This investigation revealed a culture of overtime abuse that was prevalent for approximately 20 years.
- Partnered with a vendor to develop an app to allow citizens to report fraud on their smartphone. This City became the 2nd local government in the U.S. to develop a fraud reporting app for citizens.
- Previously served as Director of Internal Audit at a Fortune 500 international company and reported to the CFO and Audit Committee

Industry involvement

- Institute of Internal Auditors (IIA)
- Association of Local Government Auditors (ALGA)
- Association of Government Accountants (AGA)
- Association of Certified Fraud Examiners (ACFE)

Licenses and certifications

- Certified Public Accountant (CPA)
- Certified Internal Auditor (CIA)
- Certified Fraud Examiner (CFE)

MANAGING DIRECTOR

Chris Kalafatis, CPA, CIA, CFE

Page 2

Thought Leadership

- Delivered more than 25 CPE presentations or webinars to audit and accounting organizations such as the IIA, ISACA, ACFE, AGA, and ALGA. Example topics included fraud, internal controls and supply chain management
- Authored multiple thought leadership articles on topics such as fraud and inventory management

Awards and Recognition

- Recipient of the AGA's 2024 Private Sector Financial Excellence Award given to an individual across the nation that exemplifies and promotes excellence in state or local government financial management, outstanding leadership, high ethical standards and innovative management techniques



PRINCIPAL

Madhu Maganti, CPA, CISA, M.S.

Madhu is a principal with Baker Tilly's risk advisory practice.



Baker Tilly Advisory Group, LP

T: +1 (713) 677 3701

madhu.maganti@bakertilly.com

bakertilly.com

Education

Masters in accountancy
Baruch College
(New York, NY)

Bachelor of Commerce
Bangalore University
(Bangaluru, India)

Madhu joined the firm in 2022 and is a goal-oriented cybersecurity/IT advisory leader with more than 20 years of comprehensive experience leading high-performance teams with a proven track record of continuous improvement toward objectives. He is highly knowledgeable in both technical and business principles and processes. Known for hands-on leadership style, Madhu is able to instill a sense of teamwork and commitment while maintaining a reputation of integrity, dependability and a strong work ethic. In addition, he is a thought leader, having spoken at several conferences and authored articles for leading publications. Madhu specializes in cybersecurity risk assessments, enterprise risk management, regulatory compliance, Sarbanes-Oxley (SOX) compliance and system and organization controls (SOC) reporting.

Specific experience

- Principal-in-charge on risk-based engagements, including cybersecurity risk assessments, HIPAA compliance, GDPR/CCPA compliance, SOX compliance, business process improvement, international restructuring, SOC-2 attestation and other information security related services
- As a fractional CISO, streamlined operations and developed a robust information security environment for several SMBs
- Developed practice offerings, employees, training and other initiatives focusing on healthcare, finance, technology, energy and higher education clients
- Managed HIPAA security assessment for \$6 billion healthcare company resulting in remediation and compliance
- Fractional CISO for several SMBs, designing their overall cybersecurity system
- Managed end-to-end NIST/ISO assessments for clients in healthcare, finance, energy, higher education and technology
- Initiated the SOX IT program for a Fortune 50 organization while developing strong audit tools which increased productivity and audit efficiency
- Designed patent-pending tools that have saved a Fortune 50 organization more than \$100 million year over year

Industry involvement

- Information Systems Audit and Control Association (ISACA)
- InfraGard

PRINCIPAL

Madhu Maganti, CPA, CISA, M.S.

Page 2

Community involvement

- Works with several dog rescue groups – fostering and transporting shelter dogs
- Coaches cricket players in the greater Houston area

Thought Leadership

- Speaker in multiple conferences including Houston Cyber Summit, TXCPA Houston, TEI Houston, etc.
- Authored several articles on cybersecurity and data protection, including [*What cybersecurity trends should we look for in 2024?*](#) March 2024, Houston Business Journal

SENIOR MANAGER**Peter Tsengas, CISA, CISM**

Peter is an IT senior manager with Baker Tilly's risk advisory public sector practice.



Baker Tilly Advisory Group, LP

T: +1 (703) 827 9350

peter.tsengas@bakertilly.com

bakertilly.com

Education

Bachelor of Science in Accounting Information Systems, Virginia Polytechnic Institute & State University

Peter has 25+ years of IT audit and IT risk compliance consulting experience with three top 10 firms, and industry experience in the public sector and Fortune 500 companies. Stays current on new industry technologies, risks, and regulatory compliance requirements. Experienced in leading managers and other team members and serving as a client relationship manager.

Specific experience

- Led and supervised IT risk and compliance projects with 40+ public sector entities, including IT security audits for sensitive systems and independent assessments for third-party cloud hosted sensitive systems, to assess compliance with industry best practice standards such as NIST (Publication 800-53 and NIST Cybersecurity Framework)
- Led and supervised multiple annual IT audits for Internal Audit outsourced public sector clients
- Led and supervised statewide internal control framework annual risk assessments and IT control testing for 10+ public sector clients
- Led and supervised a business resiliency project for a public sector client that included 50+ project stakeholders, and focused on delivering a revised business impact assessment (BIA), business continuity plan (BCP), and disaster recovery (DR) plan for the client
- Led and supervised multiple Independent Verification & Validation (IV&V) engagements for public sector clients to assess compliance with project management standard (CPM 112) requirements
- Led and supervised a general controls IT risk and compliance engagement, that resulted in improvements to the organization's IT security governance framework
- Previously served as an IT Auditor for three state government agencies, where he led and supervised multiple IT security audits, IT general controls audits, and IT systems development audits

SENIOR MANAGER

Peter Tsengas, CISA, CISM

Page 2

Industry involvement

- Information System Audit and Control Association (ISACA)
- Institute of Internal Auditors (IIA)
- Association of Government Accountants (AGA)

Licenses and certifications

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)

Thought leadership

- Delivered numerous IT risk and compliance focused presentations at CPE events across multiple states for organizations such as ISACA, IIA, and the AGA
- Authored an IT whitepaper focused on the best practices for IT systems development



SENIOR MANAGER

Stacey N. Gill, CIA, CISA

Stacey Gill is a senior manager with Baker Tilly's risk advisory public sector practice.



Baker Tilly Advisory Group, LP

T: +1 (512) 975 7284
stacey.gill@bakertilly.com

bakertilly.com

Education

Bachelor of Science in business management
 Louisiana State University

Stacey has 15 years of experience providing risk advisory, business process improvement and compliance-based consulting services to public sector clients. She has wide-ranging project experience across functional areas generally, focused on ensuring clients are aware of and managing key risks and that operations are efficient and aligned with organizational strategy. She has significant experience in internal auditing, supporting clients collaboratively to execute audit activities and serving as an outsourced provider conducting all facets of the internal audit function including enterprise risk assessment, annual audit plan development, audit execution, remediation follow up and reporting to audit committees.

She has a deep understanding of assessing operational and governance-related risks, reporting on compliance and providing organization-specific improvement recommendations.

Specific experience

- Outsourced and co sourced internal audit services including financial audits, compliance audits, operational audits, information technology audits, performance audits and advisory projects
- Business process and internal controls reviews
- Information technology (IT) department assessments of governance, organizational structure and operations
- IT general controls audits
- Cybersecurity assessments
- IT risk assessments in connection with financial audits
- Sarbanes-Oxley (SOX) 404 internal audit support services
- System and Organization Controls (SOC) reporting

Industry involvement

- Institute of Internal Auditors (IIA)
- Information Systems Audit and Control Association (ISACA)
- Association of Local Government Auditors (ALGA)
- American Public Power Association (APPA)

Continuing professional education

- Certified Internal Auditor (CIA)
- Certified Information Systems Auditor (CISA)

SENIOR MANAGER

Stacey N. Gill, CIA, CISA

Page 2

Thought leadership

- "Risk assessment and audit planning," IIA Long Island Chapter Conference, 2023
- "Finding operational efficiencies with internal audit," Utility University webinar, 2022
- "Resource optimization and cost reduction," IIA Austin Chapter Luncheon, 2020
- "Risky business: Assessing risks in your organization," Baker Tilly webinar, 2019
- "Emerging risks in public utilities," Baker Tilly webinar, 2019
- "Elevating IT in the decision-making process," APPA Business and Financial Conference, 2017
- "Risks and considerations for ERP systems implementations," IIA Southern Regional Conference, 2017
- "Using information technology benchmarks to evaluate your IT resources," APPA webinar, 2017
- "Success in succession planning," APPA webinar, 2016
- "Developing and implementing utility succession planning," APPA National Conference, 2016



MANAGER

Andrew Kennedy, CISA

Andrew is a manager with Baker Tilly's risk advisory practice.



Baker Tilly Advisory Group, LP

T: +1 (346) 318 0209

andrew.kennedy@bakertilly.com

[bakertilly.com](https://www.bakertilly.com)

Education

Bachelor of Business
Administration in finance
Texas A&M University

A fast-paced, innovative consultant with a focus on communication, project management and exceeding goals. Andrew has a strong history of adaptability and a proven work ethic has led to a steady increase in responsibilities while maintaining a high-quality output. Experienced across both information security and GRC fields. Adept in strategy development, dealing with complex issues and challenges, and developing a quick understanding of new subject matter.

Specific experience

- NIST CSF risk assessments
- SOC1 and SOC2 readiness and attestation
- IT and non-IT SOX readiness
- Privacy assessments (HIPAA, GDPR, CCPA, etc.)
- policy creation and incident response, business continuity and disaster recovery planning
- Financial and IS internal control environments.
- Process improvement and control implementation
- Compliance and risk mitigation

Continuing professional education

- Certified Information Systems Auditor (CISA)



SENIOR CONSULTANT

Valentine Acquah

Valentine is a senior consultant with Baker Tilly's risk advisory practice.



Baker Tilly Advisory Group, LP

T: +1 (972) 748 0345
valentine.acquah@bakertilly.com

[bakertilly.com](https://www.bakertilly.com)

Education

Master of Science in cybersecurity
University of Dallas

Bachelor of Arts in political science
and sociology
University of Ghana

Valentine has experience in compliance and risk advisory engagements related to information systems and internal controls over financial reporting.

Specific experience

- NIST cybersecurity assessment and providing recommendations for improvement
- System and Organizational Controls (SOC) 1 and 2 testing
- Assist with IT SOX testing and audit planning
- Evaluate existing internal controls for IT risk impacting financial reporting surrounding change management, system security and IT operations



Smart decisions. Lasting value.™

Proposal to Provide Information Technology Audit & Consulting Services

November 22, 2024

Submitted to:

Jim Doezie, Contracts, Risk & Performance Administrator
Orange County Employees Retirement System (OCERS)
2223 E Wellington Ave., Suite 100
Santa Ana, California 92701
Email: jdoezie@ocers.org

Submitted by:

Michael Del Giudice, Principal
Crowe LLP
650 Town Center Drive, Suite 740
Costa Mesa, California 92626-7192
Direct 630.575.4359 | mike.delgiudice@crowe.com
Tel 714.668.1234
Central 312.899.5300





Crowe LLP
Independent Member Crowe Global

650 Town Center Drive, Suite 740
Costa Mesa, California 92626-7192
Tel 714.668.1234
Fax 714.668.1235
www.crowe.com

Cover Letter

November 22, 2024

Jim Doezie, Contracts, Risk & Performance Administrator
Orange County Employees Retirement System (OCERS)
2223 E Wellington Ave., Suite 100
Santa Ana, California 92701
Email: jdoezie@ocers.org

Dear Mr. Doezie:

Crowe LLP (Crowe) is pleased to present our proposal in response to the Orange County Employees Retirement System's (OCERS) Request for Proposal to provide Information Technology Audit & Consulting Services.

Crowe is a public accounting, consulting, and technology firm with offices around the world, including Orange County. Our vision is built on deep specialization and a focus on our clients, our people, and the hallmarks of our profession: integrity, objectivity, and independence.

We forge each relationship with the intention of delivering exceptional client service while upholding our firm's core values – **care, trust, courage, and stewardship**– and strong professional standards. Crowe has delivered value to our clients for decades by listening to their needs and developing a comprehensive understanding of their businesses and would appreciate the opportunity to do the same for you.

Based upon the requirements and desired outcome of this project, we feel that Crowe has the capability to make this project an unqualified success. Crowe is an experienced, stable, and well-respected firm with a strong state and local government commitment. We have delivered high value results to our clients for decades, and we feel that we are well-suited to help the OCERS with this project. Our team is strong and skilled in several attributes that we feel are important to the success of this project, including:

- **We have proven expertise** in performing the specific work requested
- We perform over **200 cybersecurity assessments and penetration tests a year**
- **We provide security and compliance experts** with certifications that include Certified Information System Security Professional (CISSP), Offensive Security Certified Professional (OSCP), and Certified Ethical Hacker (CEH)
- **Speaks at industry leading cybersecurity conferences**, such as Blackhat and Defcon;
- Contributes to the industry through **development and release of cybersecurity tools**;
- **Experience with public retirement systems**, including cybersecurity assessments, penetration testing, and application of key business systems such as employer and member portals; and
- **Strong public sector consulting practice.** Professionals throughout our firm who devote their efforts to serving more than 1000 public sector clients including governmental entities at the local, state and federal levels. This commitment to specialization allows us to develop and retain personnel who are very familiar with the transportation environment, work with diverse organizational and governance structures, and participate in understanding, developing, and implementing best practices with our clients.

Jim Doezie, Contracts, Risk & Performance Administrator
Orange County Employees Retirement System (OCERS)
Page ii

Fresh Perspective and Smooth Transition

You have been audited by the same firm and team members for several years and may have grown accustomed to certain ways of doing things. This is a chance to re-think how you perceive your internal financial management, audit and business partner relationships and start fresh. The selected firm should bring local and national experience to the team in order to be able to share industry trends, best practices, and other insights to the financial reporting process. We will leverage our deep specialization in government agencies of similar size and complexity to mitigate risk on your issues.

Exhibit C – Affirmation

By submitting this response, Crowe hereby affirms and represents that we have reviewed the proposal requirements, meet or exceed all minimum qualifications outlined in **Exhibit B – Minimum Qualifications Certification**, and have submitted a complete and accurate response to the best of our knowledge.

By signing below, I hereby affirm that Crowe has reviewed the entire RFP, intends to comply with all requirements, and has submitted a complete and accurate response to the best of my knowledge. I also affirm that this proposal constitutes an irrevocable offer for the 120 days following the deadline for submission of proposals, and as a Principal of Crowe LLP, I am authorized to bind the firm contractually.

A signed copy of **Exhibit C – Proposal Cover Page and Check List** has been provided on the following pages.

Closing Comments

Crowe has reviewed the Orange County Employees Retirement Systems RFP for Financial Auditor Services and the accompanying **Exhibit D – Orange County Employees Retirement Systems Agreement for Services**.

Crowe understands that both parties reserve their respective rights to negotiate an appropriate and mutually acceptable agreement for Crowe to provide Information Technology Audit & Consulting Service to OCERS. Crowe's response to the Request for Proposals for Financial Auditor Services does not constitute an agreement, nor does it provide terms of an agreement. Should Crowe be selected to engage in negotiations for a final agreement, Crowe will request the modifications and additions outlined in **Appendix D** of this proposal.

Should there be questions regarding our proposal, please contact me at 630.575.4359 or via email at mike.delgiudice@crowe.com.

Thank you for taking the time to consider our proposal. We are looking forward to demonstrating why Crowe is the best firm to engage for your provide Information Technology Audit & Consulting Service's needs.


Sincerely,

Mike Del Giudice
Principal

Exhibit C

PROPOSAL COVER PAGE AND CHECK LIST (TO BE SUBMITTED IN FIRM'S LETTERHEAD)

Respondent Name:

Respondent Signature: 

Respondent Address:

By submitting this response, the undersigned hereby affirms and represents that they have reviewed the proposal requirements and have submitted a complete and accurate response to the best of their knowledge. By signing below, I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements.

Respondent specifically acknowledges the following:

1. Respondent possesses the required technical expertise and has sufficient capacity to provide the services outlined in the RFP.
2. Respondent has no unresolved questions regarding the RFP and believes that there are no ambiguities in the scope of services.
3. The fee schedule submitted in response to the RFP is for the entire scope of services and no extra charges or expenses will be paid by OCERS.
4. Respondent has completely disclosed to OCERS all facts bearing upon any possible interests, direct or indirect, that Respondent believes any member of OCERS, or other officer, agent, or employee of OCERS presently has, or will have, in this contract, or in the performance thereof, or in any portion of the profits thereunder.
5. Materials contained in the proposal and all correspondence and written questions submitted during the RFP process are subject to disclosure pursuant to the California Public Records Act.
6. Respondent is not currently under investigation by any state or federal regulatory agency for any reason.
7. Except as specifically noted in the proposal, respondent agrees to all of the terms and conditions included in OCERS Services Agreement.
8. The signatory above is authorized to bind the respondent contractually.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Table of Contents

Cover Letter i

Proposal Requirements 2

- Firm Profile – Number of Employees 3
- Organizational Structure 3
- Organizational Chart 4
- Annual Revenues 4
- Scope of Services Offered 5
- Respondent’s Specialties, Strengths, and Limitations 5

Internal Audit Services 7

- IT General Controls, Cybersecurity Audit and IT Risk Project Experience 10
- IT Audit Capabilities 11
- Annual Risk Assessment and Audit Plan Development 12

Scope of Services 13

- 1. IT / Cybersecurity Audit 13
- 2. Internal Audit IT Risk Assessment / Audit Program 18
- Project Deliverables 24

Fees 30

- Pricing Proposal 30
- Project Dependencies 30

Appendix A: Exhibit B – Minimum Qualifications Certification 36

Appendix B: Resumes 37

Appendix C: Writing Samples 47

Appendix D: Exceptions to Agreement for Services 48

Proposal Requirements

1. The “Minimum Qualifications Certification,” attached as Exhibit “B.”

We have provided completed copy of the **Exhibit B – Minimum Qualifications Certification** form in **Appendix A** of this proposal.

2. The “Proposal Cover Page and Check List,” attached as Exhibit “C.”

We have provided completed copy of the **Exhibit C – Proposal Cover Page and Check List** in the cover letter of this proposal.

3. An executive summary that provides the respondent’s background, experience, and other qualifications to provide the services included in the Scope of Services.

We are committed to those things most important to you. Coupled with our deep investment knowledge and governmental expertise in conjunction with our proprietary innovative solutions, we are confident that Crowe is the best choice for the Orange County Employees Retirement System (OCERS).

We understand that you require an experienced and proficient provider that has the knowledge necessary to assist OCERS with (IT) Internal Audit Services under the supervision of OCERS Director of Internal Audit. The IT audit/consulting services will include:

1. The development and execution of an **IT General Controls (ITGC) and Cybersecurity Audit**. In collaboration with OCERS Internal Audit, OCERS management and OCERS external auditor, Crowe will assist in the documentation of an audit policy, procedure(s), audit programs to tests the design and operating effectiveness of those controls, and the risk controls matrix for the identification of controls that mitigate the corresponding ITGC and Cybersecurity risks. At the conclusion of the review, we will provide observations and recommendations within a report. Inquiring with management, Crowe will assist with the documentation of action plans to assistance with future remediation.
2. Execution of an **IT Risk Assessment** leveraging the methodology and formats used by OCERS’ Internal Audit Department.
 - Develop a project level risk assessment.
 - Develop internal audit procedures to be executed by OCERS internal audit staff.
 - Provide training and guidance to OCERS staff who will execute the audit program.
 - Provide advice and guidance for issue development and when assessing management developed and agreed upon remediation plans.

This will allow us to assist Internal Audit in the development of a 1-to-3-year IT Audit Plan.

In addition, we understand the OCERS is looking for a firm to provide advice / information on specific IT audit/technical matters as needed to support the OCERS Internal Audit Department over the course of the contract period.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

California Commitment

Crowe has significantly invested in California with six offices that employ approximately 500 staff throughout the state. Specifically, Crowe has three offices within the Orange and Los Angeles counties to serve OCERS audit engagements, fully supported and complemented by our Public Sector Services specialists throughout California and nationally.

Orange County – Costa Mesa California Office

The Orange County location serves a broad range of Southern California government clients, particularly entities in Orange, Los Angeles, Riverside, San Bernardino and San Diego Counties. Contributing employers of your system, Orange County Transportation Authority and Transpiration Corridor Agencies are current clients of Crowe.

Organizational Chart

Crowe is limited liability partnership with more than 500 partner/principals This proposal is being submitted by Mike Del Giudice, Principal who be your primary contact. Mike will lead the team and will manage the coordination of all services. For day-to-day operations, Trevor Krause will be the single point of contact coordinating delivery of engagement activities, qualified specialists, and overseeing all services for consistency and cohesiveness. Addition information regarding the proposed engagement team has been provided in response to item #5 in this section.

Crowe Leadership Organization

You can find more information about our firm leadership at <https://www.crowe.com/about-us/leadership>

Annual Revenues

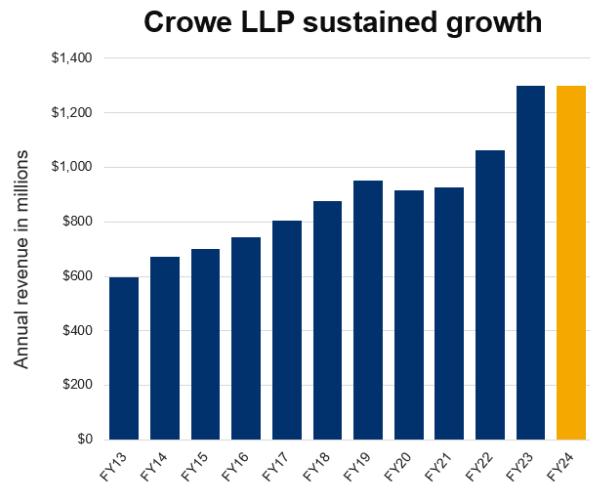
Founded in 1942, Crowe is celebrating more than 80 years of stability, growth, and innovation.

Crowe LLP (Limited Liability Partnership) is an independent member of Crowe Global, which ranks as the **ninth-largest international accounting network**.¹

If requested, we will make the balance sheet and income statement summary (financial statements) of Crowe LLP, which we assert are confidential, available to OCERS, for inspection and examination by the appropriate staff under separate cover. We will be pleased to provide you any additional information you may need to determine our financial stability.

Please note, Crowe LLP is privately held and asserts that its financial statements are confidential trade secret information. The financial statements provided are not audited as we do not issue audited financial statements or annual reports.

¹ International Accounting Bulletin, 2024, based on market share and fee data.



Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Scope of Services Offered

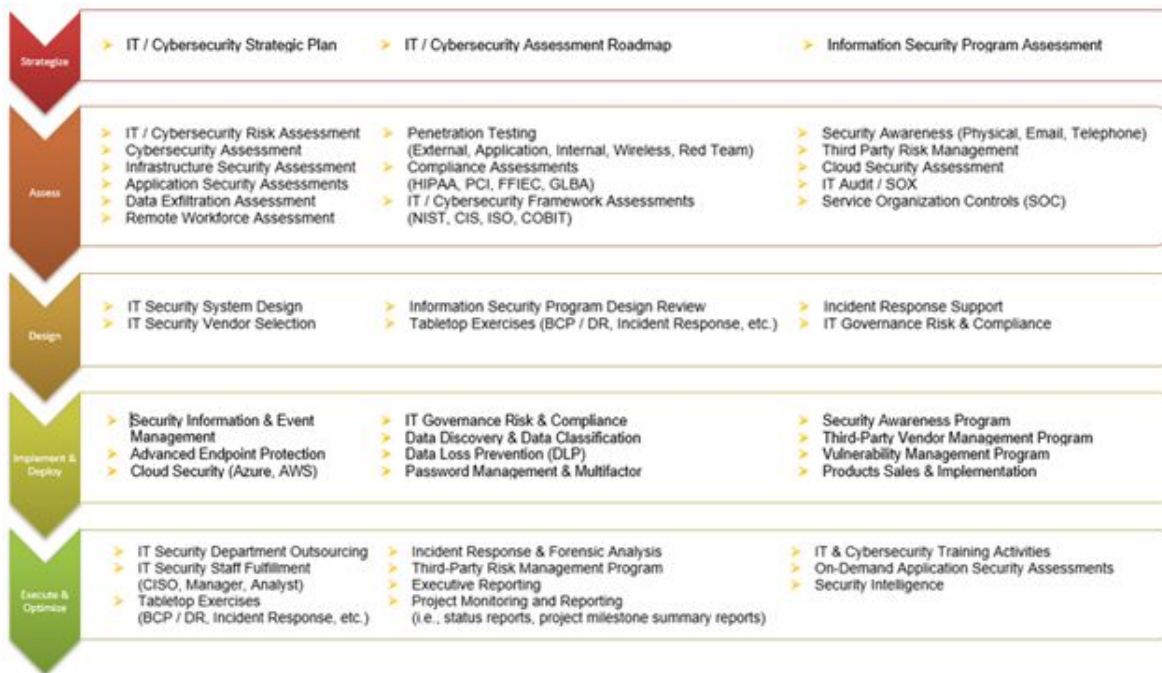
The Firm’s core services include audit, tax, advisory, and consulting services complemented by industry specialization. Industry specialization is the primary go-to-market strategy for the firm, relying on teams of individuals contained within the business units to drive service delivery and growth within key industries.

- Banking
- Financial Services
- Healthcare
- Manufacturing and Distribution
- **Public Sector**
- Technology, Media, and Telecommunications
- Cannabis
- Fintech
- Insurance
- Metals
- Real Estate and Construction
- Consumer Markets
- Food and Commodities
- Life Sciences
- Private Equity
- Retail Dealer

Respondent’s Specialties, Strengths, and Limitations

Crowe has been providing Cybersecurity services, including the review of Information Security practices and implementation of IT solutions, **for over 25 years**. Crowe has worked with hundreds of companies across the United States and internationally to improve the quality of their Cybersecurity posture through risk assessments, penetration testing, Cybersecurity assessments, and the implementation of security/technology solutions. Crowe’s Cybersecurity team consists of over 250 professionals who deliver the following services within our Cybersecurity Risk Lifecycle:

Crowe’s Cybersecurity Risk Lifecycle



The ultimate success of our relationship with the Orange County Employees Retirement System involves the commitment of an accomplished team of experienced professionals.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

6

Qualifications of Management Personnel

Our Cybersecurity team includes professionals who have functioned as CISOs, served as security administrators, and managed internal risk assessment functions. A large majority of our professionals, including all our managers and above, are certified and regularly speak on information security issues at national security conferences such. Crowe maintains multiple consultants that hold the following certifications:

- CRISC – Certified in Risk and Information Systems Control
- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager
- OSCP – Offensive Security Certified Professional
- GPEN – Certified GIAC Penetration Tester
- GWAPT – Certified GIAC Web Application Pen Tester

Cybersecurity Training

The Crowe cybersecurity practice supports a vigorous continuous learning environment for all staff and executives. Our strength is in our people, and because of this, we recognize the need for everyone to continually develop both professionally and personally throughout his or her career. While Crowe requires each professional to attend 120 hours of continuing professional education over a three-year period, with a minimum of 20 hours in each calendar year, our staff attends over 55 hours of formal continuing professional education programs per year.

Crowe has provided Cybersecurity solutions to over 300 organizations. Our industry coverage is broad and includes state and local government, higher education, not-for-profit, energy, manufacturing, construction, financial services, healthcare, insurance, real estate, services, and technology.

Scope of Services

Helping clients succeed is our intent for every relationship. Our goal is to work with you to deliver a unique solution that exactly meets your needs and value expectations. Crowe can meet and exceed the scope requirements as stated within the Executive Summary with the proposed Crowe service offerings detailed on the following pages. We understand your organization's needs are to assist Internal Audit with the execution of an IT General Controls review, a Cybersecurity Audit, and an IT Risk Assessment. Crowe will execute each engagement following industry standard Internal Audit methodology, described below.

Internal Audit Services

Internal Audit Methodology

Our internal audit services help organizations improve risk management and strengthen internal controls. We provide objective, credible, and timely information to help management and audit committees make critical decisions.

Our internal audit methodology is described more fully below. But the fundamentals are simple. We will:

- Fully grasp your organization, industry, the regulatory environment, and our discussions with you
- Communicate frequently so that managers are aware of our progress and status.
- Report risks and recommendations that address the underlying root causes of the issues.
- Provide pertinent data on internal controls to management and the audit committee.
- Maintain active awareness of the ongoing operations and strategy in order to understand current issues and offer input regarding future plans.

Approach and Scope

Our internal audit specialists use a five-step, risk-based methodology that is based on standards and guidelines of the Institute of Internal Auditors.



Component 1: Risk Assessment



We want to emphasize the importance of first understanding your organization at the highest level. To accomplish this, we work closely with management to develop a risk assessment based on your strategic priorities.

We will conduct interviews with senior management to discuss risks, controls, and strategic plans within your organization. This insight, along with prior audit results and the regulatory landscape, will generate the risk assessment summary that drives the audit plan and audit. Assessing risk continues throughout each component of the audit process.



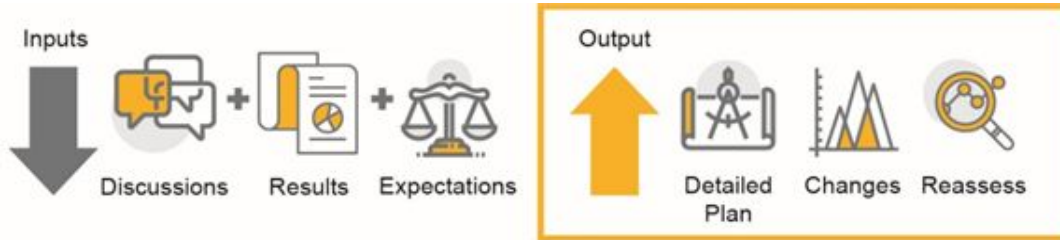
Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Component 2: Audit Plan



The risk assessment process provides the information needed to develop the audit plan and audit procedures tailored based on the needs of the organization. A detailed audit plan documenting the audit procedures is provided to the internal audit manager for review and approval prior to each audit. This audit plan outlines the segments and processes that will be audited.

We also recognize that risks in organizations change. To offset this, prior to the fieldwork we will conduct a secondary risk assessment. This secondary risk assessment reviews significant activities or processes and addresses the risk control objectives and major control points for each activity or process.

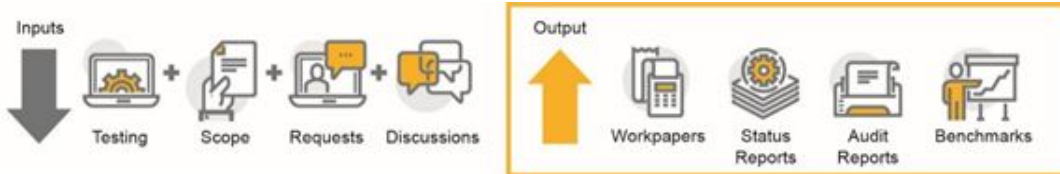


Component 3: Results



We conduct audits throughout the year at mutually agreed-upon times and request information in advance to make our time in the field efficient. During the audit, we will communicate audit findings to confirm assumptions and discuss potential issues. Once audit findings are confirmed, we will finalize best practice recommendations and issue a draft report for management’s response and action plans.

Your results will be benchmarked to those of other similar organizations so you can compare your business to peers and identify areas of needed improvement.



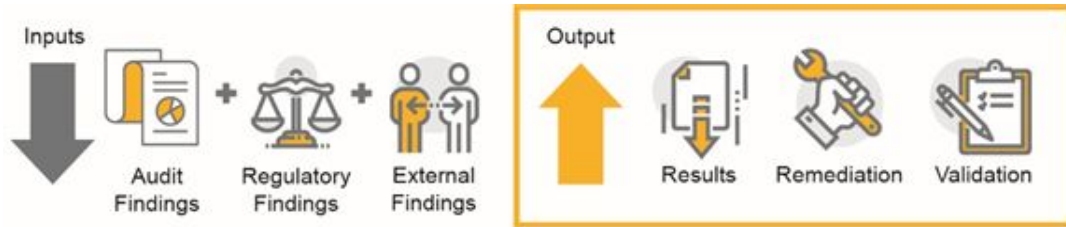
Component 4: Follow-up



The internal audit process does not end with the communication of audit results. The internal audit results, along with regulator and external audit findings, should be regularly monitored and substantiated. Once management completes remediation efforts to address the audits and examinations, if you choose, we will follow up to validate that the control has been fixed.

We will also maintain ongoing communication with the audit committee, board of directors, executive management, and primary business personnel throughout the organization so that we can react quickly and effectively to changes in risks.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System



Component 5: Risk Analysis



We analyze the audit results for thematic issues within the organization and benchmark them against peer data. This intelligence helps you understand how effectively your risk is being managed in the various areas of the organization. It will also help you appropriately allocate resources to strengthen your internal controls.



Communication with the OCERS

Crowe has developed a proven approach to managing internal audit service arrangements. At the core of the methodology is communication and a focus delivering projects on time and within budget. This methodology has survived the test of time, and we consistently meet or exceed our clients' expectations for a quality outcome.

Whether the project is categorized as Staff Augmentation or as Project Solution (i.e., vendor-directed) we will maintain regular communications with all stakeholders to confirm that the OCERS is aware of issues, risks, and other matters as they arise. We will also submit formal status reports on a monthly basis, or as directed, so that each party is aware of key matters that may impact project outcomes.

Our communications will serve to make sure that the projects are managed in a manner that is consistent with our oversight responsibilities, team structure, and management approach.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

10

IT General Controls, Cybersecurity Audit and IT Risk Project Experience

Crowe's IT Audit team consists of over 150 professionals nationally locations who deliver a full range of IT audit services, including those requested as part of the scope of work for this engagement. We have provided a brief description of the services requested, as well as some of our most common IT audit solutions.

A qualified Internal Audit services provider has the capacity and expertise to meet your needs. Throughout the remainder of this document, we have detailed our qualifications. Listed below are the main points of emphasis.

- Crowe has been auditing employee benefit plans for more than 35 years and is currently a trusted advisor for more than 1,200 ERISA plans (approximately 340 defined benefit pension and health and welfare benefit plans and 950 defined contribution plans).
- Our dedicated government group is comprised of over 200 individuals, and serves more than 700 governmental organizations nationwide, including several multi-billion-dollar entities (among them the Ohio Bureau of Workers Compensation and Industrial Commission of Ohio with an investment portfolio of \$25.3 billion). In addition, Crowe has delivered more than 400 California public sector projects and provides audit services to over 100 local governments annually.

We have provided audit and consulting services to public pension funds, including but not limited to:

- California State Teachers' Retirement System
- Chicago Transit Authority Supplemental Retirement Plans
- Dallas Area Rapid Transit Retirement Plans
- City of Tampa General Employee Pension Plan
- City of Lakeland Retirement Plans
- Illinois Municipal Retirement Fund
- Pension Benefit Guaranty Corporation
- Chicago Teachers' Pension Fund
- Tennessee Valley Authority Retirement System
- State Board of Administration – (Florida Retirement Trust)
- Minnesota State Retirement System
- City of Fort Lauderdale Retirement Plans
- Minnesota State Retirement Fund
- Employees' Retirement System of Rhode Island

We maintain membership in the AICPA Governmental Audit Quality Center, AICPA Employee Benefit Plan Audit Quality Center, Government Finance Officers Association, and the Public Pension Financial Forum.

We will direct, review, and supervise the day-to-day performance of the IT Risk Assessment and Audit services. However, the audit consulting manager and the Audit Committee are responsible for the results of the review work. We cannot perform management functions, make management decisions, or appear to act in a capacity equivalent to a member of OCERS management or an employee. Additionally, we cannot be involved in activities such as authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of OCERS. Accordingly, we cannot perform ongoing monitoring activities or control activities, prepare source documents on transactions, or have custody of the OCERS's assets. We will comply with applicable AICPA, U.S. Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), and other regulatory independence guidance.

We will perform periodic consulting services, as authorized by the audit consulting manager, based upon the approved risk-based compliance review plan. Our services will include testing a selection of transactions. Higher risk areas will be covered in more detail and with greater frequency, while lower risk areas will be covered in less detail and on a rotational basis. Specifics concerning the risks, frequency, and scope of the areas to be reviewed will be outlined within the compliance consulting services plan. We will periodically discuss with the compliance consulting manager the status of the review engagement and reviews in progress. We will provide the Audit Committee with a periodic update of the status of the consulting plan.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

IT Audit Capabilities

At Crowe, we offer a full suite of information technology risk, and cybersecurity services designed to help organizations identify, assess, and mitigate IT risks. Facing increasing dependence on technology and an ever-growing array of internal and external risk factors, organizations of all types turn to Crowe to help them pursue a consistent, coordinated, and integrated approach to IT Audit.

Crowe’s IT Audit and Cybersecurity teams consists of over 150 professionals across the country, including professionals who have functioned as CISOs, served as security administrators, and managed internal risk assessment functions. Crowe maintains multiple consultants, including all our managers and above, that hold the certifications such as the Certified Information System Security Professional (CISSP), Certified Information Security Auditor (CISA), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), and Certified in Risk and Information Systems Control (CRISC).



IT Audit Procedures

Based on the results of the IT Risk Assessment (discussed below), Crowe will develop an IT audit plan focusing on the most critical risks from the assessment. This plan will typically be a 3-year plan, which is re-evaluated each year for appropriateness, and will include a combination of enterprise controls and technology audits. Some of the typical procedures include:



Information Technology Audit & Consulting Services
Orange County Employees Retirement System

12

Annual Risk Assessment and Audit Plan Development

We believe that a comprehensive risk assessment should drive the annual audit planning process, so that the internal audit function is able to identify areas in which it may be most impactful. Our approach is to identify key risks to the organization, measure their significance and probability of occurrence, and map them to auditable functions or entities.

Our approach involves consulting with leadership and senior management through surveys, interviews, and other methods to obtain their perspective and insight on the OCERS objectives and associated risks, as well as how those risks are managed through implemented of controls and other management activities.

We will also conduct our own research and compile a refined list of risks to complete a comprehensive risk assessment, which will be the basis for the annual audit plan. We will discuss the plan with the OCERS Manager before submitting it to the Board for their input and approval. We have also provided an in-depth discussion of our approach to satisfy the requested scope of services within the next section.

Scope of Services

Cybersecurity and IT General Controls are one of the top risks' organizations are facing today. As part of any IT Risk Assessment, it is imperative to fully understand how these cybersecurity and IT General Control risks are being managed. As part of this engagement, Crowe will leverage the Crowe Integrated Cybersecurity Framework (CICF) and the IT General Controls Framework to evaluate these risks.

Our procedures will be specific to your Information Technology environment. Our involvement with multiple organizations that have either outsourced or co-sourced the IT audit function will enable us to effectively and efficiently meet your needs for a comprehensive information systems examination which considers both IT general controls, security, and operational efficiencies.

We will provide management and the audit committee with recommendations for improvements in overall controls and the efficiency of the information systems. We will not stop at merely recommending improvements; we also have the capability to assist management at identifying and implementing solutions. This may be done by providing reference materials, industry contacts, or through additional engagements including rolling up our sleeves and working with management to resolve the issue.

1. IT / Cybersecurity Audit

Overview

Crowe views IT / cybersecurity risk as the assurance of the **confidentiality, integrity, and availability** of critical organizational assets. Crowe's will provide a comprehensive analysis of your organization by evaluating the people, processes, and technologies supporting your organizations information security efforts.

- **People:** Information Security requires collaboration and support from across the organization. In addition, the consumerization of IT has increased the reliance organizations have on their personnel properly protecting sensitive information. Crowe will evaluate the controls in place to mitigate risks associated with the accidental or malicious disclosure of sensitive information by personnel.
- **Process:** Organizational standards and formal procedures set expectations and help define organizational tolerance for risk. Crowe will review these standards and procedures to evaluate the effectiveness of these programs.
- **Technology:** Technology supports information security initiatives by enforcing policy, automating processes, and providing opportunities for real time management of risk that manual processes are unable to achieve. Crowe will evaluate the technology infrastructure and validate systems are properly managing information security risk.



Project Methodology and Approach

Our methodology for the execution of the Cybersecurity & IT General Controls Audit, includes coordinating with control owners to gather evidence and assesses security controls, which encompass the following steps:

Project Planning and Kickoff

During planning, an information request list is submitted to gather existing policies, procedures, and technical configurations. A kickoff meeting is held to discuss the Project Plan that includes the project timeline, identification of assessment stakeholders (OCERS resources), sampling approach, automated and manual scanning windows, and expectations. Additionally, interviews are scheduled for information-gathering sessions with both business stakeholders and IT management.

Control Design Review

Once planning is complete, a comprehensive assessment of all IT / security controls is performed to provide the most accurate understanding of the environment. This begins by reviewing existing documentation, the evaluation of technical configurations, and/or conducting numerous interviews with control owners, as well as with IT subject matter experts. Crowe will complete a design review of the controls to determine testing procedures.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

14

Control Effectiveness Testing

If necessary, once the design of the control is determined and a testing plan is completed Crowe will conduct testing to validate the operating effectiveness of IT / security controls to determine information system and network device weaknesses by observing vulnerability scans and assessing system configurations.

This testing will be customized based on the control design, and could include a combination of observation, walkthrough, and/or technical testing to confirm network control standards are being met.

Crowe will leverage a sampling approach when testing controls. The samples selected will be dependent on various factors, such as the design of the control, overall testing population, and frequency of control performance.

Audit Report(s)

Once all fieldwork activities are completed and the discussion of gaps identified has occurred, in collaboration with OCERS, the audit team will start the process to develop the audit report(s). The purpose of each report will detail the assessment methodology, scope approach and the results of the assessment. The reporting phase will consist of the following activities:

- Analyze and summarize assessment results.
- Document the results of the network security and controls assessment.
- Determine the level of risk (ratings) for all identified security control gaps.
- Deliver and review deliverables with personnel.
- Collaborate on the development of Management Responses from respective Subject Matter Experts (SMEs)

Project Scope of IT General Controls

Each IT general controls area will be considered with respect to standards and best practices with a focus on efficiencies and controls.

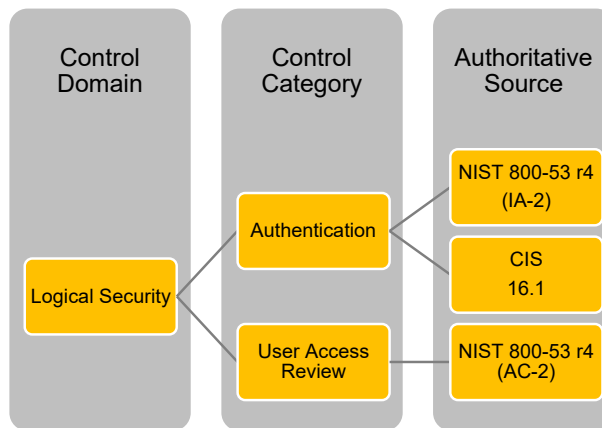
- Management
 - Annual review of IS policies
 - Segregation of IS duties
 - Strategic Planning
 - Supervision of IS employees
- IS Insurance Coverage
- Development and Acquisition
 - Escrow agreements
 - Documentation
 - Parameter changes
 - Contractual Relationship
 - Use of report writers
 - Vendor access
- Online Security
- Contingency / Resumption Planning
- Operations
 - File handling and retention
 - Data control
 - Procedures for reviewing input documents
 - Preparing daily processing parameters
 - Balancing control totals
 - Distributing reports
 - Processing files prepared from the image area
- Item / Image Capture Processing
- Voice Response
- Review of Risk Management of Outsourced Technology Services / Vendors

Project Scope of Cybersecurity Controls

Crowe has extensive expertise performing cybersecurity controls assessments for multiple organizations. Determining an appropriate control framework for cybersecurity is challenging for even mature organizations. The complexities and nuance with existing regulatory requirements (e.g., PCI-DSS, HIPAA, ISO 27001) combined with industry standards (e.g., **CIS Top 18**, NIST CSF) make managing control expectations nearly impossible.

To address this challenge, Crowe has established the Integrated Cybersecurity Framework. This framework allows Crowe to bring value to our clients by defining integrated controls that address multiple cybersecurity requirements (i.e., regulatory and industry standards) as efficiently as possible and manage their cybersecurity risk.

Crowe has mapped multiple regulatory and industry standards, or authoritative sources, to the framework in order to provide our clients with a comprehensive understanding of their ability to address various regulations and standards when evaluating the control environment.



By correlating the controls, this integrated control can be defined in a way that includes a single test procedure that allows the organization to understand compliance with all common control requirements across the different standards and regulations.

Crowe’s framework includes:

- **Regulatory requirements:** Gramm–Leach–Bliley Act (GLBA), FFIEC Information Security Booklet, NY Department of Financial Service (DFS) Part 500, NY SHIELD Act, Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA).
- **Industry frameworks:** Cybersecurity Maturity Model Certification (CMMC), NIST (800-30 r2, 800-53 r5, 800-171 r2, 800-171B, Cybersecurity Framework v2), ISO 27001/2, CIS Top 18 Critical Security Controls, CJIS, CSA Cloud Controls Matrix, and the FFIEC Cybersecurity Assessment Tool (CAT).

Crowe’s proprietary methodologies are designed to provide the greatest value to OCERS by incorporating a risk-based approach to target key areas of review. This is due to Crowe developing its methodologies over years of experience with multiple security resources including industry standards, various regulatory requirements, and vendor best practices. Based upon experience in reviewing an array of client networks and IT operations, Crowe is uniquely positioned to customize these methodologies to provide focused reviews for OCERS’s environment.

Crowe’s experiences also allow us to avoid ‘checklist auditing’ and focus review time on areas of new or significant risk. In turn, this enables Crowe to provide sensible, reliable, and proven recommendations which will help mitigate cybersecurity risks.

For the evaluation of Cybersecurity controls, Crowe will leverage an integrated cybersecurity framework, as aforementioned above, which consists of a balanced IT security coverage across all areas of risk, customizable to your needs. The review will include both information *Cybersecurity Governance* components that support the overall IT / Cybersecurity program, as well as specific areas of the *IT Environment* (hardware and software) of the infrastructure, applications, and endpoints within the organization.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

16

Cybersecurity Governance

Cybersecurity governance consists of 14 domains segmented into control categories, which are mapped at the control level with various regulations and industry frameworks. Cybersecurity governance may include one or more of the following areas depicted below:

<p>INFORMATION SECURITY GOVERNANCE</p> <ul style="list-style-type: none"> <input type="checkbox"/> Information Security Program <input type="checkbox"/> Roles & Responsibilities <input type="checkbox"/> Oversight & Strategy <input type="checkbox"/> IT Risk Management <p>DATA PROTECTION</p> <ul style="list-style-type: none"> <input type="checkbox"/> Data Management (Handling & Classification) <input type="checkbox"/> Data Inventory <input type="checkbox"/> Data Protection Controls <input type="checkbox"/> Data Privacy <input type="checkbox"/> Data Sanitization & Destruction <input type="checkbox"/> Encryption <p>LOGICAL SECURITY</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identification & Access Control <input type="checkbox"/> Access Management (Least Privilege & Segregation of Duties) <input type="checkbox"/> Access Reviews <input type="checkbox"/> Authentication <p>PHYSICAL SECURITY</p> <ul style="list-style-type: none"> <input type="checkbox"/> Physical Information Security <input type="checkbox"/> Data Center Security <input type="checkbox"/> Physical Access <input type="checkbox"/> Physical Monitoring & Detection <input type="checkbox"/> Physical Audit Log & Review <input type="checkbox"/> Clean Desk <p>LOGGING & MONITORING</p> <ul style="list-style-type: none"> <input type="checkbox"/> Audit & Logging Management <input type="checkbox"/> Audit Configuration <input type="checkbox"/> Audit & Log Aggregation <input type="checkbox"/> Audit Monitoring & Detection <input type="checkbox"/> Audit Alerting <input type="checkbox"/> Audit Log & Review <p>THREAT & VULNERABILITY MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Malicious Code Detection <input type="checkbox"/> Patch Management <input type="checkbox"/> Threat Intelligence <input type="checkbox"/> Vulnerability Management 	<p>IT OPERATIONS</p> <ul style="list-style-type: none"> <input type="checkbox"/> Asset Management <input type="checkbox"/> Asset Lifecycle (Procurement, Transfer, Destruction) <p>EMPLOYEE MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Employee Standards <input type="checkbox"/> Hiring Practices <input type="checkbox"/> Job Transition Practices <input type="checkbox"/> Termination Practices <input type="checkbox"/> Security Training <p>THIRD PARTY RISK MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Third Party Security Oversight <input type="checkbox"/> Third Party Inventory <input type="checkbox"/> Third Party Network Access <input type="checkbox"/> Third Party Contracts <input type="checkbox"/> Third Party Due Diligence <p>CONFIGURATION MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Approved Infrastructure <input type="checkbox"/> Standard Build Procedures <input type="checkbox"/> Configuration Certification <p>BUSINESS CONTINUITY MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Business Impact Assessment <input type="checkbox"/> Business Continuity & Contingency Planning <input type="checkbox"/> IT Resiliency & Backup Processes <input type="checkbox"/> Disaster Recovery Planning <input type="checkbox"/> Incident Response Procedures <p>CHANGE MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Change Control <input type="checkbox"/> Maintenance <p>SECURE DEVELOPMENT & ACQUISITION</p> <ul style="list-style-type: none"> <input type="checkbox"/> Development & Acquisition Standards <input type="checkbox"/> Project Management (System Security Plans) <input type="checkbox"/> Coding Practices <input type="checkbox"/> Testing <p>COMPLIANCE MANAGEMENT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Compliance & Regulatory Standards
--	---

IT Environment

Interviews and reviews of policies and procedures only paint a portion of an IT / Cybersecurity compliance program. As part of the audit, Crowe will conduct additional control testing of key areas to validate that people, process and technology are effective to reduce risk to an acceptable level as required by the industry and regulatory requirements.

To determine technical compliance of security control requirements, as defined within policy, Crowe will assess a sample of information systems (i.e., servers, workstations), network devices (i.e., firewalls, routers, switches, wireless), and applications, which is centered around understanding the people, processes, and technologies. The review will assess a standard set of control areas related to that system to verify that the appropriate technical controls, supporting processes, and governance structures are in place to ensure secure operation of a given system.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Our review may include one or more of the following areas depicted below:



Our technical assessments are designed to address real risks and security best practices. We have built our assessment programs using applicable regulatory guidance and industry best practices, including guidance from the National Institute of Standards and Technology (NIST), CIS Benchmarks, applicable vendor guidance, and best practices Crowe has aggregated through its work with other organizations.

2. Internal Audit IT Risk Assessment / Audit Program

Overview

Crowe's IT Risk Assessment services can assist organizations from multiple perspectives, from reviewing and evaluating existing programs to designing and implementing enterprise programs. Crowe's risk assessment services provide our clients with consulting professionals who can perform numerous assessments utilizing industry and regulatory standards that include, but not limited to, an evaluation of information security governance practices, detailed technical device / system configuration, and vulnerability reviews. Additionally, our teams design and implementation experience deliver extra value by providing solutions and best practices that not only address key industry requirements and standards, but those that are also practical and have been successfully implemented by our clients.

Crowe's risk assessment process follows the NIST SP 800-30 leveraging a framework that aligns with the IT Governance Institute's risk management framework.

Crowe has provided risk solutions to over 600 organizations. Our industry coverage is broad and includes state and local government, higher education, not-for-profit, energy, manufacturing, construction, financial services, healthcare, insurance, real estate, services and technology.

Project Methodology and Approach

Crowe's overall risk assessment methodology most closely aligns with NIST SP 800-30. Crowe's solution will follow a phased approach with defined tasks to provide clarity in project execution.

Initiate Project

The purpose of this task is to initiate the project, define project roles, and identify key stakeholders for the engagement. The fieldwork will consist of the following activities:

- Discuss and finalize approach for executing the risk assessment.
- Develop a high-level project charter including the roles, responsibilities, timeline and deliverables.
- Identify risk assessment workshop participants.
- Provide a request list.

Phase 1 – Preparation, Categorization, Security Control Selection

The purpose of phase 1 is to finalize all necessary materials and prepare personnel to complete the risk assessment. The fieldwork will consist of the following activities:

- Conduct workshops to identify and customize IT / Cybersecurity risks related to the organization's assets, systems, and data.
- Meet with key IT stakeholders to review and finalize draft IT / Cybersecurity risks.
- Determine metrics for rating IT / Cybersecurity risk (Impact, Likelihood and Control Effectiveness).
- Coordinate workshops to discuss IT / Cybersecurity risks for the following:
 - Evaluate the likelihood and impact of each risk to understand the organization's operations, reputation, and financial stability; and,
 - Risk prioritization of risk based on their likelihood and potential impact, allowing the organization to focus its resources on addressing the most critical risks first.
- Selection of a security control framework that include industry accepted security frameworks and regulatory standards (i.e., *NIST CSF*, *CIS Top 18*, *CJIS*, etc.) to identify and document risks.
- The development of a risk management plan, which provides the foundation for developing a risk management strategy including recommendations for the implementation of policies, procedures, and controls to mitigate the identified risks effectively.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

19

Phase 2 – Controls Assessment

The purpose of this phase is to qualitatively evaluate the IT / Cybersecurity risks by leveraging the results of the IT General Controls and Cybersecurity Audit to determine the design and effectiveness of the OCERS's IT / security controls. The fieldwork activities performed during the IT General Controls and Cybersecurity Audit, as previously stated, will consist of the following activities:

- Review requested materials.
- Conduct workshops with key stakeholders to:
 - Review and discuss IT / Cybersecurity risk environment; and,
 - Assess the design and control effectiveness of the control environment, utilizing the IT General Controls and Integrated Cybersecurity Framework.
 - Assess technical controls, based on a sampling approach, for network devices, information systems, and
 - Discuss the capabilities to identify and manage IT / Cybersecurity risk.
- Compare the OCERS's capabilities against peers.
- Assess the risk level based on the evaluation of information system security controls.
- Determine and provide recommendations for the OCERS's on-going monitoring strategy for the information system(s) and its security controls to ensure that they remain effective and to identify any changes in the system's risk posture.

Crowe will leverage a sampling approach when testing controls. The samples selected will be dependent on various factors, such as the design of the control, overall testing population, and frequency of control performance.

If the assessment requested requires compliance with a specific industry framework and/or regulatory standard, Crowe will leverage a standard methodology in order to rate the effectiveness of each of the controls. Each individual control is rated at Compliant, Not Compliant, or Partially Compliant. This will help determine control gaps to be reported during the engagement.

Analysis, Reporting, and IT Audit Plan

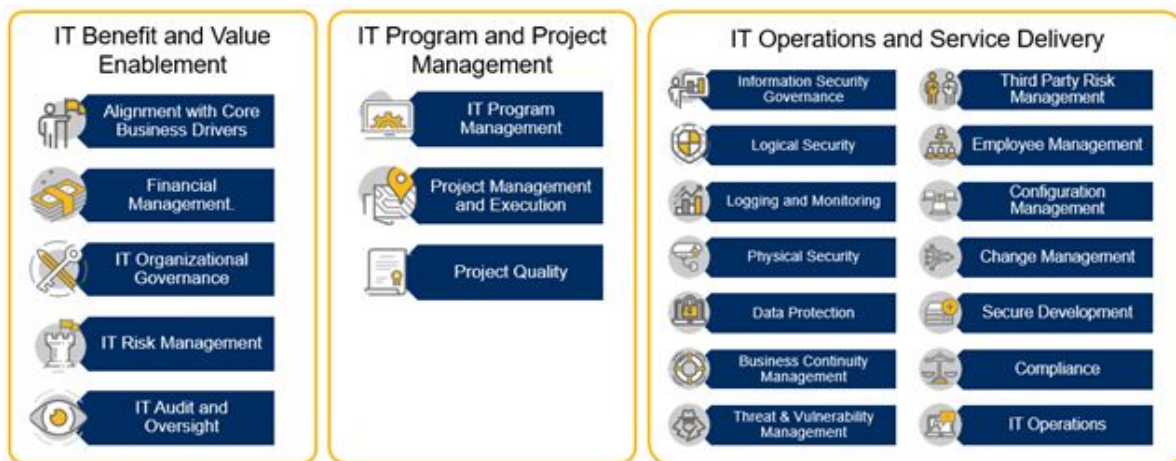
The purpose of this task is to review the results of the IT Risk Assessment, including the IT General Controls and Cybersecurity Audit, to develop a 1-to-3-year audit plan. This task will consist of the following activities:

- Analyze and summarize the IT Risk Assessment results from Phases 1 and 2.
- Document the results of the IT Risk Assessment, which includes inherent risk (likelihood and impact), control effectiveness, and residual risk.
- Document a risk register for all identified risks that include owners, risk ranking, inherent risk, mitigating controls, and residual risks.
- Document and collaborate with OCERS for the development of the 1-to-3-year IT Audit Plan. IT Audits will be selected within the plan based where the residual risk rating exceeds the organizations acceptable tolerance for risk.
- Deliver and review deliverables with personnel.

Project Scope

Crowe’s IT Risk and Control Framework most closely aligns with the IT Governance Institute’s IT risk management framework, consisting of three primary IT domains: *IT Benefit and Value Enablement, IT Program and Project Management, and IT Operations and Service Delivery*.

- The **IT Benefit and Value Enablement** domain considers risks associated with opportunities to use technology to improve the efficiency or effectiveness of business processes or as an enabler for new business initiatives.
- The **IT Program and Project Management** domain considers risks associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs. This includes the decisioning around the portfolio of projects pursued by the IT organization.
- The **IT Operations and Service Delivery** domain considers risks associated with the operational stability, availability, protection and recoverability of IT services that can bring destruction or reduction of value to the enterprise. IT Operations and Service Delivery is segmented into fourteen (14) risk categories.



Crowe’s Baseline IT Risk and Control Framework

Furthermore, the **IT Operations and Service Delivery** domain is divided into unique control categories that contain a series of controls and test procedures, which include the following:

The components included as part of the IT / Cybersecurity Governance Review include:

1. Information Security Governance

Cybersecurity Governance focuses on the core components that set organizational tone on cybersecurity/information security and support execution of the Information Security Program. Crowe will review key Cybersecurity policies, conduct interviews with key personnel, and review select documentation or supportive information to validate the effectiveness of your program. Areas of review include:

- Information Security Program
- Roles and Responsibilities
- Oversight & Strategy
- IT Risk Management

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

21

2. Data Protection

Proper data protection is an important component of a sound information security program. Crowe will evaluate a number of factors related to the protection of data from inception to destruction. Areas of review include:

- Data Management (Handling & Classification)
- Data Inventory
- Data Protection Controls
- Data Sanitization & Destruction
- Encryption

3. Logical Security

Logical Security focusing on the controls in place to limit access to resources to only those individuals with a need to know. The focus includes processes for requesting and authorizing access requests, removing access when no longer necessary, and restricted unauthorized access. Areas of review include:

- Identification & Access Control
- Authentication
- Access Management (Least Privilege & Segregation of Duties)
- Access Reviews

4. Logging & Monitoring

The Crowe team will investigate the current standards for security logging and monitoring. An understanding of the standards will be obtained through a series of interviews and by investigating various devices on the network as outlined below. Areas of review include:

- Audit & Logging Management
- Audit Configuration
- Audit Log Aggregation
- Audit Monitoring & Detection
- Audit Alerting
- Audit Log Review

5. Physical Security

Appropriate physical security controls are essential components of an effective information security program and environment. Crowe will review the processes by which the data center is properly protect (utilizing physical and environmental controls), monitored, and accessed. Crowe will interview key personnel and perform a technical review over configuration settings physical security. Areas of review include:

- Physical Information Security
- Data Center Security
- Physical Monitoring & Detection
- Physical Access
- Physical Audit Log & Review
- Clean Desk

6. Business Continuity Management

Appropriate business continuity management and backup processes are essential components of an effective information security and system management program. Crowe will review the Backup processes for the website environment to ensure that proper controls are in place. Crowe will review the contingency plans, systems redundancy and disaster planning. Crowe will also review the incident response procedures to ensure the proper steps are included in the event of various incidents. Areas of review include:

- Business Impact Analysis
- Business Continuity & Contingency Planning
- IT Resiliency & Backup Processes
- Disaster Recovery Planning
- Incident Response Procedures

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

22

7. Threat & Vulnerability Management

The Crowe team will investigate current threat protection requirements including items such as malicious code detection tools (anti-virus and anti-malware, intrusion detection & prevention systems, and integrity checking solutions), patch management, and vulnerability management. An understanding of the standards will be obtained through a series of interviews and review of documented standards. Crowe will conduct this review using a comprehensive, structured methodology. Areas of review include:

- Malicious Code Detection
- Patch Management
- Vulnerability Management
- Threat Intelligence

8. Third Party Risk Management

Crowe will review policies and procedures for third party risk management, if applicable, by inspecting current documentation and interviewing key personnel to confirm that these policies and procedures represent best practices while supporting core business objectives. Third party management is a key component of overall network security and stability. Areas of review include:

- Third Party Security Oversight
- Third Party Contracts
- Third Party Inventory
- Third Party Due Diligence
- Third Party Network Access

9. IT Operations

IT Operations are the processes and services associated with IT to deliver business operations to the organization. These processes are critical to support quality and competitive delivery of IT services to the business. Areas of review include:

- Asset Management
- Asset Lifecycle (Procurement, Transfer, Destruction)

10. Employee Management

The Crowe team will perform interviews and review policies and procedures over current practices regarding employee hiring and training processes. The review will also cover items such as IT specific training and the use of social media. Areas of review include:

- Employee Standards
- Job Transition Practices
- Hiring Practices
- Security Training
- Termination Practices

11. Configuration Management

Crowe will evaluate the security oversight of standard build procedures and certification against these procedures. Areas of review include:

- Standard Build Procedures
- Approved Infrastructure
- Configuration Certification

12. Change Management

Crowe will review the security change management procedures to verify they include an evaluation of how devices are placed back on the network after a re-image or an upgrade to the system. Areas of review include:

- Change Control
- Maintenance

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

23

13. System Development & Acquisition

The Crowe team will investigate any organizational policies and procedures around software development and the system development life cycle (SDLC). The areas include:

- Development & Acquisition Standards
- Project Management (System Security Plans)
- Coding Practices
- Testing

14. Compliance

The Crowe team will investigate any organizational policies and procedures around regulatory and compliance requirements are met for cybersecurity. Areas of review include:

- Compliance & Regulatory Standards

To be most effective, this IT risk and control universe will be customized at the beginning of the engagement to identify your most critical IT risks. Crowe will leverage industry expertise working with similar organizations and collaboration with key stakeholders to determine the final framework.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

24

Project Deliverables

Crowe anticipates the following deliverables will be created during the engagement:

Deliverables	Brief Description
Periodic Status Reports	Ongoing status report summarizing the status of the project, including key tasks, accomplishments and project risks. Frequency of the status will be determined during Phase I.
Project Plan	A project plan will summarize the following project topics for all engagements. The objective of the project plan is to define responsibilities and client expectations to meet and/or exceed project management activities. <ul style="list-style-type: none"> • Project Scope • Project Timeline • Communications Plan • Requested Items
Exit Meeting Document	Discussion document presented at the end of the fieldwork to facilitate a discussion on the results of the engagement prior to formal reporting.
IT / Cybersecurity Audit Report	The final report discussing results of the engagement, including: <ul style="list-style-type: none"> • Executive summary of findings • Overview of engagement • Scope and Assessment Methodology, including tools utilized • Overall assessment of risk posture, relative to industry standard and the experienced observation of the organization • General recommendations • Details of findings, risk analysis and remediation
IT Risk Assessment Report	The IT Risk Assessment Report will be included the following: <ul style="list-style-type: none"> • Background, Objective, Scope and Approach; • Methodology and Framework; • Risk Scoring / Ratings; • Overall assessment results by IT Risk domain, in table format by scope area and sorted by risk level; • Key / Significant Areas of Risk; and, • Detailed results per IT Risk domain including: <ul style="list-style-type: none"> ○ Domain objectives and current security practices ○ Inherent and residual risk levels ○ Identified IT risks and threats ○ Suggested recommendations
Audit Plan (IT Risk and Assessment Coverage Matrix)	The defined audit plan will include control assessments over a three-year period. The audit plan will include the following: <ul style="list-style-type: none"> • Audit Area – Separated by Process, Technology, or Specialty Audits (such as penetration testing) • Audit Objective – High level scope and objectives for each Audit • Audit Rotation – In-scope audits to be performed over a three-year period.

We thoroughly document each item examined to ensure that you understand its significance to your security. For each item, we will document the following information:

- **Risk Rating:** A rating for the issue identified based on its level of risk to the organization in the form of high, moderate, low, or best practice.
- **Description of Finding:** This section provides the details outlining the issue identified.
- **Recommendations:** This section details Crowe's recommendations to each addressed issue.
- **Management Response (Optional):** Crowe offers the opportunity for you to respond to our recommendations. Additionally, a due date and individual responsible may be provided below the Management Response area.

Examples of our Reports (IT General Controls / Cybersecurity Audit and IT Risk Assessment) are provided in **Appendix C: Writing Samples**.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

5. The names and qualifications of the staff that will be assigned to OCERS work, including a detailed profile of each person’s background and relevant individual experience.



Key Personnel

Crowe brings substantial expertise by using IT specialists from throughout Crowe’s diverse practice areas with nearly 250 Cybersecurity and IT Audit team professionals. This is an important reason for our clients to outsource, and it has been exciting to see the value of using IT specialists to bring their industry knowledge to our clients. However, we also know the need to maintain a single contact point.


We assign a single contact point to oversee consistency in the services provided and to manage information received from multiple teams in a cohesive manner. This streamlines communications and provides you with a single source of accountability when questions arise.

The proposed engagement team is well-qualified to provide the OCERS with quality, timely, and personalized service. **Mr. Mike Del Giudice**, Principal will lead the team and will manage the coordination of all services. For day-to-day operations, **Trevor Krause** will be the single point of contact coordinating delivery of engagement activities, qualified specialists, and overseeing all services for consistency and cohesiveness.


Below we have provided the profiles of key individuals that are representative of the skills across teams that could be utilized to support delivery of this contract.

Team Member	Years of Experience	Role	Certifications
 <p>Michael J. Del Giudice Engagement Principal</p>	25	Cybersecurity/IT Audit Team Leader Lead on IT components of the engagement and IT-related operations	<ul style="list-style-type: none"> Certified Information System Security Professional (CISSP)
<p>Mike is a Principal in Crowe’s Public Sector Cybersecurity division. He has over 24 years of experience helping clients assess, design, and implement cybersecurity solutions. Currently he is the national cybersecurity solution lead for the Public Sector Industry, including K-12 school districts, higher education, state and local government, not-for-profit, and federal government.</p>			
 <p>Trevor J. Krause Senior Manager</p>	15	Project Manager Subject Matter Expertise	<ul style="list-style-type: none"> Certified Information System Security Professional (CISSP)
<p>Trevor is a Senior Manager with over 15 years’ experience in Crowe’s Public Sector Cybersecurity division and is part of the global IT Governance, Risk, and Compliance solution team. He is the one of the solutions leaders and developer of Crowes Cybersecurity Framework. He has continued to perform Cybersecurity Assessments and Penetration Testing services; however, as a project manager his roles is to oversee the project team to verify the completion of work meets and exceeds the client expectations. He has served Public Sector clients in multiple service industries, including the higher education, transportation, not-for-profit, and public retirement systems.</p>			

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Team Member	Years of Experience	Role	Certifications
 <p>Ian Jacoway Senior Consultant</p>	9	Technical Lead – Option 1	-

Ian is a Senior Consultant and leverages 9 years of experience in computer science, data privacy, and penetration assessments. He joined the Public Sector Cybersecurity division as a consultant utilizing his prior network development projects and involvement on multiple subversive security assessments. As a senior consultant he acts as a technical leader for penetration testing services by improving on and developing new attack methodologies. He also is a threat researcher and communicates new and emerging threats to the penetration testing team and his clients. Ian specializes both in security awareness exercises testing the security mindfulness of employees, as well as assessing whether internal and external technical controls can withstand offensive measures. He continues to work on projects in multiple service industries that include higher education, state and local government, not-for-profit, and federal government, transportation, and financial institutions.

 <p>Nick Baily Senior Consultant</p>	3	Technical Lead – Option 2	<ul style="list-style-type: none"> Zero Point Security – Red Team Operator I
--	---	---------------------------	---

Nick is a part of the Cybersecurity team at Crowe, providing security and privacy technology services for clients in the public sector. He has performed information security assessments and penetration services for Crowe, filling the technical lead role. Nick oversees Crowe’s penetration testing training program, providing onboarding training for new hires on our tools and methodologies.

 <p>Michael Jenkins Felipe Tapia-Sasot Will Klonsky Elise Klinestiver Consultants*</p>	1-2	Project Consultant	-
---	-----	--------------------	---

*The project team will be finalized once mutually agreed delivery dates for fieldwork have been identified.

Resumes

We have provided resumes of the individuals listed above in **Appendix B**. The resumes outline education, years of experience, licenses and certifications, professional affiliations, and other relevant experience.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

27

6. At least three (3) references for which the respondent has provided services similar to those included in the Scope of Services. Please include for each reference the individual point of contact, a summary of the work performed, and the length of time the respondent provided each service.

Quality work based on strong functional competency and deep expertise is the core element of creating value for our clients. Quality service involves prompt and efficient service delivery and effective communication with clients.

Crowe has delivered value to our clients for more than 82 years by listening to their needs and developing a comprehensive understanding of their businesses and would appreciate the opportunity to do the same for you.

Listed below are four (4) of our clients that we have provided services similar to those requested by OCERS. Please feel free to contact the individuals listed below for an appraisal of our work.

Ohio Public Employees Retirement System	
Contact Name and Title	Caroline Stinziano, Director of Internal Audit
Address	277 E Town St, Columbus, OH 43215
Phone E-mail	cstinziano@opers.org
Period of Performance	April 2019 to current date
Objective / Scope	<p>Crowe has executed multiple Cybersecurity projects for OPERS through the course of the relationship. Crowe has provided multiple services for OPERS through the course of the relationship:</p> <ul style="list-style-type: none"> • IT Risk Assessment – Crowe worked with the Internal Audit organization to perform an IT Risk Assessment to develop a multi-year IT Audit plan. Crowe customized an IT Risk Universe with the organization. Crowe assessed risks through both an initial survey and interviews with key stakeholders to help determine the top risks. Crowe conducted interviews with key stakeholders to discuss and fine tune the results, as well as to understand key projects that could impact the future state of risk. Based on the results of the engagement, Crowe provided a report summarizing the results of the assessment, as well as a preliminary 3-year IT Audit Plan. • O365 Security Assessment – Crowe assisted with execution of an IT Audit to assess the security of the organization’s O365 implementation. Crowe reviewed policies and procedures, interviewed key personnel, and performed technical testing of the implementation. Crowe provided a report summarizing the results of the engagement, including a summary of the procedures performed, identified gaps, and recommendations for addressing the gaps. • Remote Workforce Security Assessment – As part of the IT Audit Plan, Crowe performed an Audit of the controls in place to secure connectivity for remote workers. Crowe interviewed personnel to evaluate the design of the controls, then conducted testing of controls to evaluate the operating effectiveness of the control environment. Crowe provide a report summarizing the results of the engagement, including a summary of the procedures performed, identified gaps, and recommendations for addressing the gaps. • IT Compensation Study – Crowe worked with the Human Resources Department to perform an IT Compensation Study for the organization. Crowe conducted a comprehensive survey of personnel and interviewed key resources to discuss current perspectives on compensation. Crowe met with Human Resources to understand the process for evaluating the current compensation approach. Crowe benchmarked the results against industry data and provided feedback to the organization on the results of the analysis. <p>Crowe has maintained an ongoing relationship with the organization to provide expertise to support their needs. This includes both IT Audit engagements as well as consulting projects to support organizational growth and maturity.</p>

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

Indiana Public Retirement System (INPRS)	
Contact Name and Title	Mr. David Finta, Information Security Officer
Address	One North Capitol, Suite 001 Indianapolis, IN 46204
Phone E-mail	317.234.6128 DFinta@inprs.in.gov
Period of Performance	May 2018 to current date
Scope of Work	<p>INPRS has engaged Crowe to perform security assessments to identify security risks and improve the posture of security controls since 2018. These assessments include a Cybersecurity Maturity Assessment following the NIST Cybersecurity Framework, Application Security / Code Reviews, Penetration Testing (Application, External, & Internal Penetration Assessments), Security Control Assessments (i.e., Servers, Databases, Network Architecture, etc.), and Cloud or Software as a Service (SaaS) Security Assessments.</p> <p>The last penetration assessment was conducted in 2022 that included an evaluation of Internal, External, and Web Application security controls. The overall objective of the assessments was to determine if INPRS was able to identify, resist, and respond to malicious attacks from internal threats as well as from the Internet and other external sources. Furthermore, the assessment objectives were to identify and verify vulnerabilities that could allow an attacker to gain access to INPRS internal / external network, gain elevated access, or to gain access to sensitive information. The application penetration assessment was performed to identify the effectiveness of security controls for the member self-service web portal and the retirement pension management application. The applications assessed are utilized for a population greater than 1,000,000 people.</p>

School Employees Retirement System of Ohio	
Contact Name and Title	Jeffrey A. Davis, CPA, CISA, CIA, CFE Chief Audit Officer
Address	300 East Broad Street, Suite 100 Columbus, OH 43215
Phone E-mail	614.222.5980 jdavis@ohsers.org
Period of Performance	June 2022 to current date
Scope of Work	<p>Over the past two years (2023 and 2024), SERS of OH has engaged Crowe's Cybersecurity consultants to perform the following engagements</p> <ol style="list-style-type: none"> 1. Internal \ External Penetration Assessments 2. Application Penetration Assessments 3. Cloud Security Assessment (Microsoft) 4. Identity and Access Management Review <p>The penetration assessments performed above concluded with the identification of IT / Cybersecurity vulnerabilities within information systems, networked devices, and application. Furthermore, the control assessments performed for IAM, and cloud services identified misconfigurations and weaknesses within policies, procedures, and IT \ security practices. Each assessment resulted in a report that provided detailed descriptions of the condition, root cause, impact, and suggested recommendation for remediation.</p>

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

29

San Diego County Employees Retirement Association (SDCERA)	
Contact Name and Title	Laura Flores, CIA, CFE, CGAP, Internal Audit Director
Address	2275 Rio Bonito Way, Suite 100 San Diego, CA 92108-1685
Phone E-mail	619.515.5015 lflores@sdcera.org
Period of Performance	September 2022 to current date
Scope of Work	Crowe has assisted SDCERA with the execution of an Active Directory Audit in 2022 and a NIST Cybersecurity Framework Assessment in 2023. The assessments performed concluded with the identification of IT / Cybersecurity control weaknesses within policies, procedures, and processes, including a listing of vulnerabilities / weakness within information systems. The report provided detailed descriptions of the condition, root cause, impact, and suggested recommendation for remediation.

7. Copies of any pertinent licenses required to deliver respondent’s product or service (e.g., business license).

Crowe LLP is a licensed public accounting firm authorized to practice public accounting in the State of California. Below is a copy of Crowe’s license.

BOARD OF ACCOUNTANCY
LICENSING DETAILS FOR: 7223
NAME: CROWE LLP
LICENSE TYPE: CPA - PARTNERSHIPS
LICENSE STATUS: CLEAR
PREVIOUS NAMES: CROWE HORWATH LLP
ADDRESS
 ONE MID AMERICA PLAZA
 SUITE 600
 OAKBROOK TERRACE IL 60181
 OUT OF STATE COUNTY

ISSUANCE DATE
 AUGUST 7, 2008
EXPIRATION DATE
 AUGUST 31, 2026
CURRENT DATE / TIME
 SEPTEMBER 6, 2024
 12:28:14 PM

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

8. An explanation of the pricing proposal for the scope of work, including pricing of fees and costs, billing practices, and payment terms that would apply. OCERS does limit the pricing approach to pricing and will consider alternative pricing methods for the scope of work, or portions of it. This section of the response should include an explanation as to how the pricing approach(es) will be managed to provide the best value to OCERS. The respondent should represent that the pricing offered to OCERS is, and will remain, equivalent to or better than that provided to other public pension fund or institutional investor clients or explain why this representation cannot be provided. All pricing proposals should be “best and final,” although OCERS reserves the right to negotiate on pricing.

Fees

Overview

Our goal in setting fees is simple: to provide long-term, cost-effective pricing for our clients. We are confident that we can work together to achieve an optimized plan for the proposed services.

We are committed to working with you to make sure the scope of our proposal is appropriate. While we experience cost increases throughout our relationships with our clients, we make every effort to structure an engagement fee arrangement which will meet your needs while providing us with sufficient resources to perform the expected work.

We ask clients to pay invoices via check, ACH, or wire transfer. Crowe invoices in equal quarterly installments. Our contract with you clarifies that, should a termination occur, you and we would determine any appropriate adjustments to actual fees paid as needed.

Pricing Proposal

Scope of Work Services	2025	2026	2027
IT General Controls (ITGC) & Cybersecurity Audit	\$45,000	\$46,350	\$47,740
Internal Audit IT Risk Assessment / Audit Program	\$35,000	\$36,050	\$37,132
Totals	\$80,000	\$82,400	\$84,872

Fees for Additional Services

Professional fees for special projects outside of the agreed-upon scope will be determined based on project factors, such as type of project, subject matter experience required, scope, and resource requirements. Prior to commencing additional services, we will obtain your approval and agreement on the scoping and pricing.

Project Dependencies

Crowe assumes the following sample sizes and dependencies as relates to the Cybersecurity Audit described above:

Scope Dependencies	
General Project Assumptions	<ul style="list-style-type: none"> • NO ADDITIONAL CHARGE: Routine telephone calls are considered part of the basic services. • NO ADDITIONAL CHARGE: for access to our thought leadership e-communications, webinars and literature. • NO ADDITIONAL CHARGE: for use of our secure information-sharing tool (Exchange) to gather and track audit requests or for additional data analytics tools that we incorporate into our audits. • We will not surprise you with additional fees that have not been agreed to by all parties in advance. If a question results in significant research or additional work or if we are requested to perform a consulting project, such effort is billed separately. We will provide you with an estimate of fees for such services and obtain management approval before proceeding. • Fees include professional time for work associated with fieldwork, on-site and off-site performance and documentation of procedures, preparation of written drafts and final reports, and presentation of results at finance and management committee meetings.

Scope Dependencies	
	<ul style="list-style-type: none"> • Our fee estimate assumes a risk-based approach to frequency and scope based on our experience with similar organizations. If we need to assess most areas of the organization without rotating scope each year, then we likely need to re-evaluate our planned scope and related pricing. • Significant changes in organizational status, operations, or processes not directly associated with asset growth could have a material impact on required engagement coverage. Balance sheet growth is expected, but material change, such as new lines of business, is not anticipated. • No significant changes in regulatory or client expectations or actions are expected. Should significant change occur, Crowe will assess the impact on our services and fees. All fee adjustments will require approval by all parties in advance. • The organization accepts all statements made within this document regarding scope. • Your resources and subject matter experts will be available to participate in interview sessions, individual meetings, and conference calls as necessary to provide input about the technology, organization, and processes that are currently in place at OCERS. • Crowe consultants will have access to all necessary systems, resources, and personnel for the duration of the engagement. OCERS will be responsible for ensuring appropriate exclusions are configured to provide Crowe access as needed to complete testing. • You agree to be responsible to make all management decisions and perform all management functions; designate an individual who possesses suitable skill, knowledge, and/or experience, preferably within senior management to oversee our services; evaluate the adequacy and results of the services performed; and accept responsibility for the results of the services. • Crowe will perform detailed testing as part of the IT General Controls / Cybersecurity Audit and IT Risk Assessment. Control design and effectiveness will be evaluated through interviews, inspection of detailed records, and technical configurations. • Information requested through a separate resource request letter will be gathered and available for our consultants upon arrival. • OCERS will not send any sensitive information to Crowe via unencrypted solutions. OCERS will notify Crowe of any information sent that is deemed to be confidential and it will be clearly marked as such. • Upon delivery and acceptance of the Report, OCERS will be responsible for handling and implementing any and all remediation/mitigation recommendations documented in the Report. • Crowe's deliverables are intended for OCERS personnel only. Crowe is not issuing an overall opinion on the effectiveness of the Cities control environment or a guarantee of their ability to prevent an IT / cybersecurity event. • All tests requiring sampling will be performed using Crowe's sampling methodology. <ul style="list-style-type: none"> ○ Sampling will be determined based on the criticality / risk of the information systems, which may include the sensitivity of the data stored (amount of records / type of data) and/or impact to business operations. • The IT General Controls / Cybersecurity Audit and IT Risk Assessment is based on a point in time assessment of the control at the time of the testing and do not represent an opinion on the ongoing effectiveness of the control. • The IT General Controls / Cybersecurity Audit and IT Risk Assessment will be performed remote leveraging technologies to support virtual conference calls (i.e., Zoom, Microsoft Teams, etc.)
<p>IT General Controls / Cybersecurity Audit</p>	<ul style="list-style-type: none"> • The audit will include up to eight (8) interviews. • Crowe will conduct the review based on the industry standards, such as the CIS Top 18. • Includes a network security configuration review for up-to one (1) router, two (2) firewalls combining a total of 300 rules, and two (2) switches. • Includes a review of one Mobile Device Management (MDM) solution. • Includes the evaluation of six (6) Microsoft Windows servers. • Includes a sample review of eight (8) workstations and two (2) laptops. • Includes a review of one cloud tenant (i.e., Azure, AWS, etc.). • The evaluation of physical security controls for up-to one data centers will be performed virtually with OCERS personnel. • Crowe will test the security controls on one Microsoft Active Directory domain.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

32

Scope Dependencies

**IT Risk
Assessment**

- OCERS will be responsible for defining / approving the criteria to be used to evaluate risk.
- Crowe will gather risk assessment information through interviews and surveys of personnel. The risk assessment will include up to six (6) interviews.
- Crowe will perform detailed testing as part of the Controls Assessment in phase 2. Control design will be evaluated through interviews and inspection of detailed records. In addition, Crowe will evaluate the effectiveness of security controls for the following information systems, devices, and applications leveraging the results of the IT General Controls / Cybersecurity audit, listed above.
- Crowe will develop one IT Audit Plan based on the results of the IT Risk Assessment and includes two (2) revisions.
- Crowe will not be providing any Continuous Monitoring or ongoing support as part of this engagement.

9. An explanation of all actual or potential conflicts of interest that the respondent may have in contracting with OCERS.

Independence

Crowe is independent of the Orange County Employee Retirement System and any of its affiliated entities, its officials, and its employees. Crowe is not aware of any actual or potential conflicts of interest relative to performing the proposed services for OCERS. In addition, if Crowe is selected to serve as a consultant, the firm will maintain independent of OCERS and will not be related in any way to OCERS' business operations.

As a firm of certified public accountants, Crowe has policies and procedures to provide reasonable assurance that professional personnel maintain independence, integrity, and objectivity required under professional standards. A dedicated unit within Crowe, the ethics and independence group within the firm's national office, is responsible for managing and communicating independence and ethics guidance and firm protocol.

Independence precludes relationships that might in fact or appearance impair objectivity in performing audit and other attest services. Integrity requires personnel to be honest and candid within the constraints of client confidentiality. Service and the public trust are not to be subordinated to personal gain or advantage. Objectivity is a state of mind and a quality that lends value to a firm's services. The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflicts of interest.

Personnel must consciously refuse to subordinate their judgment to that of others and must avoid relationships that may impair objectivity or influence judgments. The Crowe policy is that all personnel must be in fact and appearance independent in attitude, in the conduct of work performed, and in relationships with clients, as required by applicable professional standards.

All professional personnel shall follow the applicable independence rules and regulations of the American Institute of Certified Public Accountants (AICPA) Code of Professional Conduct, the state Boards of Accountancy, the Securities and Exchange Commission, the U.S. Government Accountability Office, and other regulatory agencies. We communicate independence rules to help provide assurance that our personnel will comply with applicable rules.

Gifts or Political Campaign Contributions

Crowe confirms that neither the firm nor its employees have given a gift or political campaign contribution to any officer, Board member, or employee of OCERS within the past twenty-four (24) months.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

33

10. A description of all past, pending, or threatened litigation, including malpractice claims, administrative, state ethics, disciplinary proceedings, and other claims against respondent and/or any of the individuals proposed to provide services to OCERS.

Past, Pending, or Threatening Litigation

Like all large professional service firms, Crowe LLP (Crowe) is subject to claims from time to time for a variety of reasons, and we occasionally receive notice of claims. However, in the view of management there are no (a) current claims that will result in significant losses to Crowe or (b) pending or threatened litigation that could affect its ability to perform the required services. It is Crowe's policy not to discuss any specific matters as they are treated as confidential.

On December 21, 2018, Crowe LLP ("Crowe") and two partners consented to entry of a US Securities and Exchange Commission ("SEC") Order instituting and resolving proceedings in connection with Crowe's single-year audit of a public company's financial statements for the year ended January 3, 2014. Crowe and the partners neither admitted nor denied the SEC's findings. Crowe agreed to a censure and cease and desist order, to undertake remedial efforts, and to pay a fine. The Order can be found on the SEC Division of Enforcement website. The Order acknowledges that Crowe cooperated with the SEC and voluntarily undertook remedial efforts prior to the conclusion of the matter. The Order does not restrict Crowe's ability to perform professional services. In November 2023, the Indiana Board of Accountancy levied a \$1,000 civil penalty as a follow-on action to the SEC Order; note that Indiana is Crowe's state of formation.

OCERS Litigation

Crowe affirms that we are not currently in litigation with OCERS or any of OCERS plan sponsor agencies.

11. Any other information that the respondent deems relevant to OCERS' selection process.

Our purpose Drives Us

Our purpose is: Shaping Your Better Tomorrow. Together. Today. It's the standard we live by and reflects what we hold important as both a firm and as individuals.

We are driven by passion, deep understanding, and integrity. We work together as a team to serve the needs of our people and our communities. We embrace and celebrate collaboration, growth, and learning.

We lead with insights, and we're committed to always do better and be better. We embrace the legacy of where we've been, and our duty to tomorrow.

**SHAPING
YOUR
BETTER
TOMORROW.
TOGETHER.
TODAY.**

Our Values

Our values reflect what we hold important as both a firm and as individuals. By living out our values every single day, in every single interaction, we drive the purpose of the firm forward. These values are the fabric that makes up the tapestry of our purpose, and that tapestry is the foundation for all the work we do.

Starting with our core purpose of "Shaping Your Better Tomorrow. Together. Today." our values bring together the guiding principles that all members of the firm, regardless of title or position, are expected to use in their interactions with colleagues, with clients, and in the communities and profession in which we work. It explains to our people the standards and expectations of ethical conduct that Crowe requires when doing business, wherever that might be.

Information Technology Audit & Consulting Services

Orange County Employees Retirement System

34

This core purpose and our core values – care, trust, courage, and stewardship – guide us in exercising professional skepticism, objectivity, and being free of conflicts of interest. They guide our people in acting with the utmost integrity and professionalism in each interaction and provide a solid foundation for the firm.



The Power of Crowe means our clients have access to the top expertise across the firm and experience a seamless collaboration between our offices, our business units, our subsidiaries, and our international network in the delivery of that expertise. For our people, it means career growth opportunities and potential for leadership development. Crowe invests in and engages the most effective resources available and goes deeper to find valuable insights and opportunities. At Crowe, our people work together across our functional areas to shape a better tomorrow.

Diversity and Inclusion

Integrity and exceptional client service are the cornerstones of our client relationships. Crowe promotes and fosters an inclusive work environment where respect, trust, and integrity are valued, and people are free to reach their full potentials.



We recognize this goal can only be achieved through collaboratively leveraging the diversity, perspectives and needs of our people, our clients, and our communities. Accordingly, DE&I is one of the firm's top priorities, integrated into firmwide programs, policies, people process, systems, and day-to-day initiatives. Overall, this commitment and the firm's many inclusive initiatives help us understand, appreciate, and address everyone's perspectives and needs and support our firm's values.

Environmental Sustainability Commitment and Goals

Our firm promotes an environmentally conscientious workplace through education, awareness, and partnerships, thereby creating eco-friendly practices. We continually research ways to increase and promote our green efforts, which establishes a culture of environmental stewardship. Through this effort, each of our locations is making substantial grassroots contributions toward environmental sustainability. Our firm continuously strives to incorporate environmental accountability and thoughtfulness throughout our culture and business practices.

Education and Professional Development

At Crowe, a career is a continual learning experience. Crowe University, our firm's learning portal, helps our people pursue learning experiences that create opportunities to build deep specialization and leadership skills. Full-time professionals can take advantage of its online learning courses, webinars, and other resources.

Crowe University is organized on a university model, with colleges and departments providing specialized curriculum. It houses curriculum maps designed to enhance technical knowledge and professional skills in areas such as project management, people development, leadership, and interpersonal skills. Learning is fundamental at Crowe, so our personnel have access to the training they need to grow and develop, regardless of their career stage or role.

Employee Satisfaction

Crowe has been ranked among the best places to work in many of our geographic markets. Crowe also conducts a quarterly engagement pulse survey to gather feedback for firm leadership and to continuously improve our talent programs.

During the past three years, Crowe has experienced an average voluntary turnover rate of less than 14 percent. Our staff continuity enables us to develop and maintain an in-depth understanding of your operations, management style, and operating practices, which ultimately will allow us to serve your organization more effectively over time.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

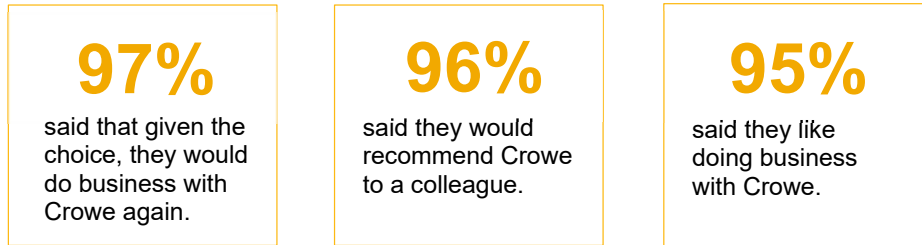
Additionally, our culture stresses the importance of partner presence throughout projects and engagements. Active, personal involvement by partners, managers, and other experienced professionals is key to a successful client relationship.

Client Experience

At Crowe, our clients are at the heart of everything we do, and we strive to demonstrate exceptional care and service through every step of the client journey.

To help us understand each client’s unique needs and value expectations, we listen closely through multiple sources, including a feedback survey that enables clients to evaluate our performance. Through the survey, clients consistently rate us highly for our industry expertise and our exceptional responsiveness, among others. Our aim is to provide an unrivaled experience for our clients, and maintaining their confidence and trust is of utmost importance.

Crowe uses a best-in-class experience management platform to monitor the experiences we deliver to our clients. In the most recent fiscal year*:



* Over 600 completed client surveys

Client Experience Resources

If, for any reason, a client is faced with a challenge or issue that is unresolvable with their Crowe partner, we encourage them to contact our Client Experience leader at ClientExperience@crowe.com. The Client Experience leader works with our clients and Crowe leaders to understand and resolve the issue while taking steps to avoid similar situations in the future.

Fortune 100 Best Companies to Work for 2024

Crowe once again is named one of the Fortune 100 Best Companies to Work For in 2024. Crowe is recognized for offering a great workplace and a positive experience for all employees – regardless of job role, race, gender, or any other demographic identifiers. Everyone at Crowe plays a role in fostering and living by a strong, values -based culture. This is Crowe’s fifth appearance on the premiere best workplaces list. The award is based on an analysis of survey responses from more than half a million U.S. employees at Great Place to Work-Certified™ organizations.

Appendix A: Exhibit B – Minimum Qualifications Certification

We have provided a completed and signed the Exhibit B: Minimum Qualifications Certification form on the following pages.

Due to varying file types, these pages will not be reflected on our Table of Contents.

Exhibit B

MINIMUM QUALIFICATIONS CERTIFICATION

All firms submitting a proposal in response to this RFP are required to sign and return this attachment, along with written evidence of how the respondent meets each qualification.

The undersigned hereby certifies that it fulfills the minimum qualifications outlined below, as well as the requirements contained in the RFP.

Minimum Qualifications include:

1. The auditor should have professional certifications such as CISA, CIA, CISSP, CRISC, or similar.
2. Minimum 7+ years of IT Audit experience: The auditor should have substantial experience in conducting both ITGC and Cybersecurity audits.
3. Experience in conducting risk-based ITGC audits: The auditor should use a risk-based approach in their audit methodology, focusing on areas with higher risks to the organization.
4. Experience conducting risk-based Cybersecurity audits: The auditor should adopt a risk-based approach, focusing on high-risk areas, critical assets, and potential vulnerabilities.
5. Familiarity with recognized security frameworks: The auditor should be proficient in assessing against the NIST Cybersecurity Framework and CIS Controls.
6. Ability to develop control matrices and test plans: Experience in designing and implementing IT control matrices and audit test plans for IT audits.
7. Proven track record in delivering audit reports: Ability to write clear, concise, and actionable audit reports suitable for presentation to senior management and audit committees.

The undersigned hereby certifies that they are an individual authorized to bind the Firm contractually, and said signature authorizes verification of this information.



Authorized Signature


Date

Name and Title (please print)

Name of Firm

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

37



Appendix B: Resumes

We have provided resumes of key personnel on the following pages.

Information Technology Audit & Consulting Services

Orange County Employees Retirement System

38



Michael J. Del Giudice
CISSP, CRISC – Principal

mike.delgiudice@crowe.com
www.crowe.com

Profile

Mr. Del Giudice is a Principal in the Consulting Practice with over 25 years of experience in the areas of cybersecurity and data privacy. Mike leads Crowe's cybersecurity practice nationally. Mike is also Crowe's cybersecurity practice lead for the public sector, including state, local, higher education, K-12, and not for profit organizations. Mike also experience includes providing security services to a broad range of Fortune 500 organizations across industries.

Professional and Industry Experience

Mr. Del Giudice evaluates and develops solutions to improve IT capability, maturity, and governance. He is experienced in critical infrastructure environments, including insurance, financial institutions, energy, transportation, healthcare, and government sectors. Mr. Del Giudice assists management in the execution of security strategies, including the solution design, requirements gathering, and vendor selection.

He also designs and implements customized cybersecurity frameworks addressing confidentiality, integrity, and availability requirements. Mr. Del Giudice has experience with data security, including data classification and inventory, control framework design and implementation, and data strategies.

He designs and implements Business Impact Assessments, Business Continuity Plans, and Disaster Recovery Programs. Mr. Del Giudice understands Intellectual Property (IP) protection procedures addressing logical, physical, and business controls; and he has experience with multiple regulatory requirements, such as GLBA, HIPAA, NERC CIP, and FTC Safeguards Rule, as well as security frameworks such as NIST 800-53, NIST Cybersecurity, and ISO.

Education and Certifications

- Bachelor of Science, Computer Engineering
 - University of Illinois | Champaign, Illinois
- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information System Control (CRISC)

Client Focus

Services:

- IT Risk Management
- Data Security and Privacy
- Security and Maturity Assessments
- Security Consulting

Publications and Speaking Engagements

- FSA Times, "Have You Conducted a Data Protection Audit Lately?"
- EUCI NERC Fundamentals course, "NERC CIP Compliance" and "NERC CIP Compliance"
- Trained the Office of the Comptroller of the Currency (OCC) on IT security
- IIA Chicago's annual seminar
- NADA national conference, "Manage your IT Risk and Improve your Bottom Line."
- IIA, "Mobile Device Risk in an Increasingly Connected World."
- NADA national conference, "Technical Security – Protecting your Dealerships Information Assets."
- WI Automobile & Truck Association, the VT Automobile Dealers Association, and the Chicago Automobile Trade Association
- Dealer Magazine and Digital Dealer, FTC's Safeguards Rule.
- IIA IT Fraud seminar
- OH Information Security Conference, "Security Strategy: Planning the Next 3 to 5 Years."
- IL Banker's Association, Community Bankers Association of IL, IN Credit Union League, MI Banker's Association, and ACBA
- BAI Institute, Auditing Technology Risks Instructor

Professional Affiliations

- Institute of Internal Auditors
- Chicago Chapter of ISACA

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

39

Representative Experience

Mr. Del Giudice has played the role of Engagement Executive across these engagements. His responsibilities include:

- Overall relationship management
- Quality control
- Providing subject matter expertise
- Account management activities

Commonwealth of Kentucky

Role: Engagement Executive | Date: April 2017 – October 2021

Crowe has a Master Agreement with the Commonwealth which allows us to perform various cybersecurity services and resell multiple cybersecurity products to public sector organizations across the Commonwealth. The entities provided services under this agreement include state agencies, local governments, municipalities, and higher education institutions. The services performed include internal and external penetration testing, cybersecurity assessments, application security assessments, code review projects, virtual information security officer solutions, and incident response services.

Indiana Public Employees' Retirement System

Role: Engagement Executive | Date: March 2019 – Current

Crowe has provided various cybersecurity services for Indiana Public Employees' Retirement system. These assessments include internal penetration testing, external penetration testing, cybersecurity maturity assessment, and creating a cybersecurity roadmap.

Mr. Del Giudice has been the Engagement Executive on this account since the beginning of the relationship in 2017. His responsibilities include overall relationship management, quality control, providing subject matter expertise, and account management activities.

Chicago Teachers' Pension Fund

Role: Engagement Executive | Date: November 2018 – October 2021

Crowe provides outsourced IT Audit services for Chicago Teachers' Pension Fund (CTPF), supporting the creation and execution of the plan for the Internal Audit Director (IAD). Crowe performs an annual IT Risk Assessment to identify risks and to develop the audit plan for the following year, with services to be performed approved by the IAD. Crowe leads the execution of these engagements, including internal and external penetration testing, cybersecurity assessments, application security assessments, and IT general controls reviews.

Ohio Public Employees' Retirement System

Role: Engagement Executive | Date: May 2020 – Current

Crowe assisted OPERS by conducting a maturity assessment of cybersecurity capabilities against the NIST PRISMA standard leveraging both strategic and technical aspects of the organization's information security program. Crowe provided the organization with a current state assessment of their maturity as well a series of recommendations to address identified gaps to improved maturity.

Mr. Del Giudice was the Engagement Executive on this project for OPERS. His responsibilities include overall relationship management, quality control, providing subject matter expertise, and account management activities.

Illinois State Board of Education


Role: Engagement Executive | Date: July 2019 – February 2020

Crowe provided a project titled a Comprehensive Risk Assessment for the Illinois State Board of Education (SBOE). The assessment included a combination of procedures in order to identify risks across SBOE, including penetration testing, application security, network architecture review, and a NIST gap assessment.

Information Technology Audit & Consulting Services

Orange County Employees Retirement System

40



Trevor J. Krause
CISSP – Senior Manager

trevor.krause@crowe.com
www.crowe.com

Profile

Mr. Krause has been with Crowe LLP for fifteen years, providing Cybersecurity & Information Security services to clients in multiple service industries, including public sector.

Professional and Industry Experience

Mr. Krause is a member of the Digital Risk Consulting practice public sector division, which includes services such as security assessments, internal and external penetration testing, and supporting clients with compliance to various regulations and security standards. Cybersecurity assessments include all elements of an organization's Information Technology infrastructure which include, but not limited to:

- IT Management and Governance,
- Application Infrastructure,
- Server Infrastructure,
- Network Infrastructure; and
- Endpoint Management.

Mr. Krause has provided Cybersecurity services assisting various industries to develop a Cybersecurity Maturity Assessment based on NIST Cybersecurity Frameworks (NIST PRISMA, NIST Cybersecurity, NIST 800-53, NIST 800-171) requirements by:

- Perform monitoring procedures of internal controls and identify compliance and control effectiveness with the NIST Frameworks;
- Proactively identifying the threats that present the greatest risks; and,
- Documenting overall risk values and recommendations.

Education and Certifications

- Bachelor of Science, Information Technology
 - Drexel University | Philadelphia, Pennsylvania
- Certified Information Systems Security Professional (CISSP)

Client Focus

Services:

- Cybersecurity / IT Risk Assessments
- Cybersecurity / Information Security Assessments (NYDFS Part 500, FFIEC CAT, NIST SP 800 Series, NERC / CIP, PCI-DSS, GLBA, SOX and HIPAA)
- Penetration Testing, Including Security Awareness

Industries:

- Federal Government
- State & Local (Municipalities / Counties)
- Education
- Not-for-Profit
- Transportation

Community Involvement

- Junior Achievement

Professional Affiliations

- (ISC)² - Certified Information Systems Security Professional
- Information Systems Security Association

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

41

Representative Experience

Mr. Krause has performed the roles of a Project Manager and/or a Cybersecurity Subject Matter Expert (SME). The responsibilities for each role are as follows:

Project Manager

- Aligning and tracking assigned resources to budgetary requirements;
- Ensuring that all resources and their respective skills are optimally utilized;
- Maintaining necessary communications with the entire project team and client expectations;
- Directing and managing Crowe resources to accomplish the engagement objectives;
- Performing detail planning, scheduling and execution of project activities;
- Coordinating and monitoring the daily tasks of all project team members; and,
- Providing quality assurance of work undertaken by staff assigned to the Project.

Subject Matter Expert

- Developed and provided project management oversight for two specialized audit reviewing Cybersecurity controls;
- Performing detail planning, scheduling and execution of project activities;
- Conducted and led interviews (10-15) across multiple departments review Cybersecurity controls to identify Cybersecurity risks;
- Assisted consultants with the development and quality assurance of project deliverables, including status meetings and project reports; and
- Provided on-going support as a Cybersecurity SME for Internal Audit departments.

Indiana Public Retirement System (INPRS) – Cybersecurity Risk Assessment Services

Role: Cybersecurity Project Manager | Date: March 2019 – August 2019

Mr. Krause worked with the INPRS to complete a comprehensive risk assessment, based on the NIST Cybersecurity Framework (CSF). The results of the assessment were used to establish a maturity rating for the organization's capability to identify threats/risks, protect assets/data, detect malicious or unauthorized activity, and respond in an appropriate manner to cybersecurity-related incidents.

Mr. Krause led a team of four staff to evaluate the control effectiveness of information systems but focusing on core NIST domains. To accomplish this the team interviewed INPRS personnel and reviewed corresponding system configurations to validate those responses. The team then documented all findings within a detailed report (including step-by-step remediation actions) and detailed the current maturity level of INPRS' capabilities. A maturity roadmap was also created to demonstrate what the projected maturity of the organization will look like once findings have been remediated. Mr. Krause presented to INPRS' executive IT management team the results of the assessment with Crowe's subject matter experts.

Ohio Public Employees' Retirement System (OPERS) – Cybersecurity Risk Assessment Services

Role: Cybersecurity Project Manager | Date: May 2020 – September 2020

Mr. Krause developed and completed a comprehensive Cybersecurity / IT risk assessment, based on the industry and regulatory standards, including the NIST frameworks. Mr. Krause led a team of three staff to document Cybersecurity / IT risks, determine inherent risk (impact / likelihood), and evaluate residual risk (the control effectiveness of information systems). To accomplish this the team interviewed OPERS personnel and reviewed corresponding system configurations to validate those responses. The team then documented all Cybersecurity / IT risks and recommendations within a detailed report (including step-by-step remediation action plans). Mr. Krause presented to OPERS' executive IT management team the results of the assessment with Crowe's subject matter experts.

Role: Subject Matter Expert | Date: June 2018 – August 2018

Mr. Krause assisted OPERS to conduct a maturity assessment of Cybersecurity capabilities against the NIST PRISMA standard leveraging both strategic and technical aspects of the organization's information security program. PRISMA incorporates standards from:

Information Technology Audit & Consulting Services

42

Orange County Employees Retirement System

- The Federal Information Processing Standards (FIPS), such as FIPS 199 and FIPS 200;
- NIST Special Publications (SPs) such as Special Publication 800-53 (Revision 3);
- Existing federal directives including FISMA; and,
- Other proven techniques and recognized best practices in the area of information security.

PRISMA focuses on nine primary review areas, each of which were derived from FISMA requirements and guidelines found in SP 800-53. Mr. Krause led a team of three staff to complete this engagement by conducting detailed interviews of key stakeholders across the organization, reviewing selected policies and procedures, and observing certain controls in order to understand the current people, processes, and technology capabilities addressing NIST PRISMA controls. Leveraging this information, Crowe was able to:

- Perform a current state assessment of OPERS cybersecurity capabilities;
- Complete a gap assessment against the NIST PRISMA standard;
- Documented all Cybersecurity / IT risks and recommendations within a detailed report (including step-by-step remediation action plans).

Grameen America, Inc. – Cybersecurity**Allice Lloyd College (ACL) – GLBA Compliance Assessment Services**

Role: Cybersecurity Project Manager | Date: December 2018 – Feb 2019

As the Project Manager providing Cybersecurity expertise, Mr. Krause lead a team of three staff to assist ACL by performing Cybersecurity Risk Consulting Services, including a Cybersecurity assessment and a web application security assessment. The objectives of the assessments were to determine compliance with Title IV regulations for federal student aid data. The audits assisted ALC in assessing current compliance with the six high level objectives defined in GLBA and the adoption of controls outlined in NIST SP 800-171 in order to identify missing controls or weaknesses within in scope security controls. The assessment included process walkthroughs (interviews) to verify the design of controls for GLBA compliance and concluded with a documented report with findings / recommendation to strengthen internal controls to meet or exceed GLBA requirements.

Los Angeles Unified School District – Information Security Audit Services

Role: Cybersecurity Project Manager | Date: January 2020 – October 2020

Trevor was the Project Manager and provided subject matter expertise related to compliance requirements for the engagement. He oversaw the Crowe team of four staff for the project ensuring a successful client delivery.

Los Angeles Unified School District (LAUSD) is the second largest in the nation, enrolling more than 600,000 students in kindergarten through 12th grade. The district covers 710 square miles, and includes Los Angeles, as well as all or parts of 31 smaller municipalities, plus several unincorporated sections of Los Angeles County. Crowe provided the Los Angeles Unified School District (LAUSD) with internal and external penetration testing, as well as a cybersecurity assessment across the district.

Berea College – GLBA Compliance Assessment Services

Role: Cybersecurity Project Manager | Date: March 2019 – July 2019

As the Project Manager providing Cybersecurity expertise, Mr. Krause lead a team of three staff to assist Berea by performing a GLBA Compliance Gap Assessment to determine if policies, procedures, and the design of controls meet and/or exceed the requirements within Gramm-Leach-Bliley Act, which states six (6) high-level objectives organizations are expected to achieve. The assessment included process walkthroughs (interviews) to verify the design of controls for GLBA compliance and concluded with a documented report with findings / recommendation to strengthen internal controls to meet or exceed GLBA requirements.

Washington Metropolitan Area Transit Authority (WMATA) – Cybersecurity Assessment Services

Role: Cybersecurity Subject Matter Expert | Date: June 2018 – March 2020

Mr. Krause assisted WMATA in performing a Cybersecurity Audit with additional (4-6) staff and as a subject matter expert for a badging (logical security) internal audit assessment, which included areas for

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

43

Cybersecurity governance and a technical information systems review. The Cybersecurity Governance review determined if WMATAs Information / Cybersecurity practices and documented requirements within policies and procedures meet and/or exceeded industry best practice security standards. The technical information system review includes a review of configurations and process walkthroughs of implemented security controls for information systems. Configurations were evaluated to verify security controls are in line with requirements stated in policy / industry standards and procedures are consistently followed. Additionally, process walkthroughs were conducted to verify that the management of security solutions are effective to identify, respond, and recover from malicious activity. Each audit concluded with a documented report with findings / recommendation to strengthen internal controls.

Battery City Park Authority (BCPA) – Cybersecurity Risk Assessment Services

Role: Cybersecurity Project Manager | Date: January 2016 – Ongoing

Mr. Krause assisted Battery City Park Authority through the development of an authority-wide risk assessment, which included the evaluation of IT / Cybersecurity risks. This risk assessment determined the audit plan for future IT / Cybersecurity audits and since the development of the plan Mr. Krause has lead teams as the Project Manager to conduct Cybersecurity, Internal Penetration, and External Penetration audits. For each audit, process walkthroughs (interviews) and technical testing (configuration reviews) were conducted to verify that the management of security solutions are operating effectively to identify, respond, and recover from malicious activity event(s). Each audit concluded with a documented report with findings / recommendation to strengthen internal controls.

Risk Assessment Services

Role: Cybersecurity Project Manager | Date: January 2019 – On-going

Mr. Krause, as a project manager, assisted Grameen with the development of the annual IT risk assessment that included the evaluation of IT / Cybersecurity risks. This IT risk assessment evaluated by performing a qualitative assessment for the likelihood and impact of each risk to determine inherent risk. Additionally, residual risk was determined based on the effectiveness of each security control. These results determined the audit plan / scope for future IT / Cybersecurity audits and since the development of the plan Crowe has conducted various audits over the past two years, which include an information systems general controls, cybersecurity audit, remote workforce audit, and follow-up with prior year issues.

YMCA of Greater New York City – Cybersecurity Assessment Services

Role: Cybersecurity Project Manager | Date: January 2017 – On-going

Mr. Krause assists the YMCA in performing Cybersecurity Audits, including a review of remote workforce controls, and as a subject matter expert (SME) for Internal Audits that require an understanding of IT / Security controls. Each audit concluded with a documented report with findings / recommendation to strengthen internal controls. On a quarterly schedule, he is responsible for assessing the evaluation of remediation activities for IT / security risks identified during past internal audits.

State University Retirement System (SURS) – NIST Cybersecurity Framework Assessment Services

Role: Cybersecurity Project Manager | Date: March 2021 – September 2021

Mr. Krause assisted SURS to complete a comprehensive assessment of Cybersecurity risk based on the NIST Cybersecurity Framework (CSF). The results of the assessment were used to establish a maturity rating for the organization's capability to identify threats/risks, protect assets/data, detect malicious or unauthorized activity, and respond in an appropriate manner to cybersecurity-related incidents. The assessment concluded with a documented report with maturity ratings, findings, and recommendation to strengthen internal controls.

Experian – Cybersecurity Gap Analysis

Role: Cybersecurity Project Manager | Date: January 2020 – April 2020

Leading the team as the Project Manager and providing subject matter expertise, Crowe performed a review of overall cybersecurity risks associated with people, process and technology. Crowe, with the assistance of Experian employees, tested in-scope controls and report against the following industry standards/frameworks:

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

44

- NIST 800-53 (Moderate Risk)
- NIST SP 800-47
- NIST SP 800-171
- ISO 27001

By conducted several interviews with Experian IT experts, Crowe determine compliance with each industry standard framework, as outlined above. The outcome of the assessment included an IT Risk Assessment report and executive level presentation detailing the scope, objectives, findings (based on a severity of risk) and recommendations. The implementation of documented recommendations assisted the client in achieving NIST and ISO certifications.

University of Texas, Austin (Applied Research Laboratories) – NIST 800-171 Assessment

Role: Cybersecurity Project Manager | Date: January 2021 – November 2021

As the Project Manager and providing subject matter expertise, a team of Crowe cybersecurity experts assessed the current state of ARL's cybersecurity capabilities and security controls to protect Controlled Unclassified Information (CUI) data following the NIST 800-171 r2 publication standards. The team performed virtual interviews with key stakeholders across the organization to understand the current people, processes, and technology capabilities related to information security to determine and report on compliance risks (gaps) with the NIST standard. The conclusion of the assessment included a Security Assessment report and executive level presentation detailing the scope, objectives, findings (based on a severity of risk) and recommendations to improve the maturity of cybersecurity controls and strengthen compliance requirements.

Connecticut Health and Educational Facilities Authority (CHEFA) – Cybersecurity & Business Continuity Assessments

Role: Cybersecurity Project Manager & Subject Matter Expert | Date: January 2021 – September 2021

CHEFA engaged Crowe to perform the following engagements to strengthen security controls, response to security incidents, and mature business continuity practices. We Performed a targeted technology risk assessment for the Authority's network infrastructure and the development of a risk assessment program, developed a written information security program that defined the policies and structure of information security for the Authority, developed of an incident response plan, and consulted on infrastructure business continuity practices specific to the Authority's network infrastructure to highlight best practices for testing, acceptable recovery times for critical systems and maintaining disaster recovery planning on an ongoing basis. Trevor led a project team to complete each task through planning, execution of fieldwork, and delivery of reports / documentation.

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

45

Ian Jacoway
Senior Consultant

ian.jacoway@crowe.com
www.crowe.com

Profile

Mr. Jacoway leverages eight years of experience in computer science, privacy, and security. He joined the Cybersecurity team as a staff member leveraging his prior network development projects, dedicated interest in the field, and involvement on multiple subversive security assessments. Ian has also evaluated a Fortune 500 organization's security assessment solution as well as numerous financial institutions.

Professional and Industry Experience

Ian has worked on teams responsible for providing various Cybersecurity services and IT Audit services, including:

- Internal and External Penetration Tests
- Network and System Security Assessments
- Cybersecurity Health Checks
- Security Maturity Assessments

Professional Affiliations

- (ISC)² - International Information System Security Certification Consortium
- Information Systems Security Association

Education and Certifications

- Bachelor of Science, Computer Science, Minor in Applied Mathematics
 - Worcester Polytechnic Institute | Worcester, MA

Client Focus

Services:

- Penetration Testing
- Cybersecurity Assessments
- Wireless Security Testing
- Social Engineering
- Health Checks

Industries:

- Financial Services
- Healthcare
- Higher Education
- Public Sector
- Retail Dealer

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

46



Nick A. Bailey
Consultant

nick.bailey@crowe.com
www.crowe.com

Profile

Mr. Bailey recently graduated from Purdue University with a B.S. in Computer and Information Technology. He is a staff consultant in Crowe LLP's Digital Risk Consulting practice public sector division, which includes services, but not limited to, External/Internal Penetration Assessments, Application Security, Cybersecurity Assessments, Network Security Assessments, NIST Gap Assessments, and IT Audit.

Client Focus

Services:

- Penetration Testing
- Cybersecurity Assessments

Industries:

- State Agencies
- Local Municipalities
- Higher Education
- K-12
- Not-for-Profit

Professional and Industry Experience

Mr. Bailey is a Consultant with Crowe's Public Sector Cybersecurity Team after completing an internship in the with the same team. He has performed multiple security assessments and IT audits for clients while with Crowe. Nick's role includes hands on testing of technology controls, reviews of policies and procedures, and providing guidance on best practices.

While at Purdue, Nick worked as a teaching assistant for a lab section covering Active Directory Administration and a lab technician for the university's various information systems. He has collaborated and worked with the teams responsible for the provision of services which include:

- Internal and External Penetration Tests
- Cybersecurity Assessments

Education & Certifications

- Bachelor of Science, Computer and Information Technology, Concentration in Cybersecurity
 - Purdue University | West Lafayette, Indiana
- Zero Point Security – Red Team Operator I

Appendix C: Writing Samples

The following writing samples demonstrate Crowe's ability to create an adequate IT General Control Audit, Cybersecurity Audit, and IT Risk Assessment.

We have provided the following samples:

- Cybersecurity Controls Audit – Report Sample
- IT General Controls – Report Sample
- IT Risk Assessment – Report Sample.

Due to varying file types, these pages will not be reflected in our Table of Contents.



Smart decisions. Lasting value.™

ABC, Inc.

Cybersecurity Audit Report

March 2023



ABC, Inc.

Cybersecurity Audit Report

Table of Contents

I. Executive Summary	1
II. Detailed Results and Remediation Plans	6
Finding #1: Logging & Monitoring – Security Information & Event Management Solution	6
Finding #2: Information Security Governance – Information Security Program	7
Finding #3: Threat & Vulnerability Management – Vulnerability Assessments	9
III. Summary of Scope	10
IV. Appendix A – Best Practice Observations	13
V. Appendix B – Risk & Remediation Effort Ratings	14

DRAFT

I. Executive Summary

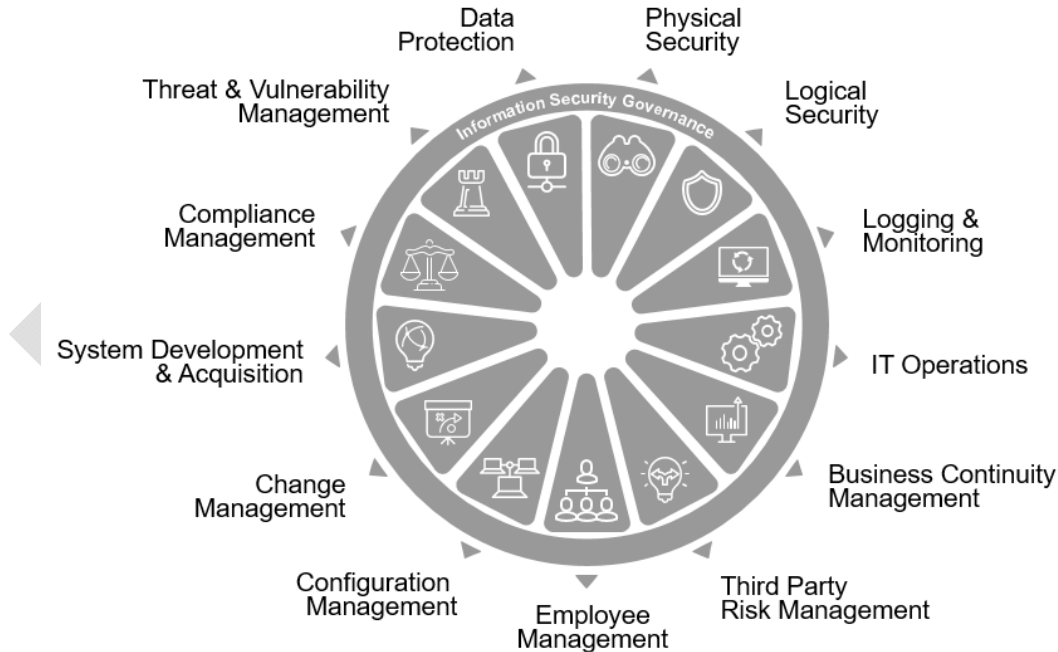
Crowe LLP (Crowe) performed a Cybersecurity Audit for ABC, Inc. (ABC) as of March 1, 2023.

Overview

Cybersecurity provides the assurance of confidentiality, integrity, and availability of critical organizational assets. Crowe performed a comprehensive analysis of your organization by evaluating the people, processes, and technologies supporting your organizations information security efforts.

The overall objective of the Cybersecurity Audit was to assess the controls over information security by utilizing Crowe’s Integrated Cybersecurity Framework (CICF), which provides balanced IT security coverage including both information security governance components that support the overall program, as well as the technical implementation of the infrastructure, applications, and endpoints within the organization. The CICF includes Cybersecurity controls for NIST (SP 800-53, Cybersecurity Framework, etc.), ISO, CIS Top 20 Critical Security Controls, various regulatory requirements (FFIEC Guidelines and Cybersecurity Assessment Tool, HIPAA, PCI, etc.), and vendor best practices.

This Cybersecurity Audit focused on Cybersecurity Governance Review (CGR) and a Technical Information Systems Review (TISR). The CGR consisted of 13 domains segmented into control categories, which are mapped at the control level with various regulations and industry frameworks. These 13 domains are surrounded by a 14th domain, Information Security Governance. This will allow Crowe to seamlessly incorporate additional control requirements, as necessary, during this engagement. The Cybersecurity Governance Review is depicted below:



The TISR review consisted of a review of technical configurations and IT processes against applicable regulatory guidance and industry best practices, including guidance from the National Institute of Standards and Technology (NIST), SANS Critical Security Controls, ISO, various

regulatory requirements (FFIEC Guidelines and Cybersecurity Assessment Tool, HIPAA, PCI, etc.), vendor guidance, and best practices Crowe has aggregated through its work with other organizations.

Crowe conducted working sessions with ABC's personnel to better understand the current state of cybersecurity controls, reviewed selected policies and procedures, identified gaps against Cybersecurity standard(s), and rated control by severity of risk. This report serves as a summary of the assessment as well as provides recommendations and proposed action plans to improve and strengthen ABC's existing IT Security controls and ultimately reduce cybersecurity risk.

Project Methodology & Approach

All controls were assessed based upon the scope approved by ABC, which covered the organizations information systems and applications. The following steps represent the actions performed to deliver the assessment:

1. Phase One – Project Planning and Kickoff

During Phase One, an information request list was submitted to gather existing policies and procedures. Additionally, a kickoff meeting was held to discuss the project timeline and expectations. Interviews were scheduled for information-gathering sessions with both business and IT management.

2. Phase Two – Assessment

A comprehensive assessment of all controls was performed to provide the most accurate understanding of the environment. Numerous interviews were conducted with Management from a cross-section of departments throughout the organization, as well as with IT subject matter experts. Crowe performed vulnerability scanning and reviewed technical configuration of systems within the environment.

3. Phase Three – Project Deliverables

Detailed results and accompanying recommendations from fieldwork are documented in this report.

Reporting Methodology

In this report, Crowe provides a summary of results and recommendations, as well as Management's responses. To assist ABC in analyzing the findings, Crowe has provided suggestions for corrective action based on the finding's exposure to loss or increased regulatory scrutiny, as follows:

High – Requires immediate remedy and, if left uncorrected, exposes ABC to significant or immediate risk of loss, asset misappropriation, data compromise or interruption, fines and penalties, or increased regulatory scrutiny.

Moderate – Requires timely remedy and, if left uncorrected, may expose ABC to risk of loss or misappropriation of company assets, compromise of data, fines and penalties, or increased regulatory scrutiny. These issues should be resolved in a timely manner, but after any high priority issues.

Low – Should be addressed as time and resources permit. While it is not considered to represent significant or immediate risk, repeated oversights without corrective action or compensating controls could lead to increased exposure or scrutiny.

Best Practice – Represents operational efficiencies or improvements for consideration by management based on industry best practices and Crowe's experiences.

Ratings have also been assigned to the level of effort required to remediate the findings. Our assignments are subjective based on the current infrastructure at ABC and our experience with other clients.

High – This will take a substantial level of effort (3 Months to 1 year) and/or significant cost to remediate. Management should consider this a project to remediate.

Moderate – This will take a reasonable level of effort (1 to 3 Months) or a moderate investment to remediate.

Low – This will take a small level of effort (1 week to 1 Month) with a small investment or no cost to remediate.

Summary of Control Gaps

The table below displays the number of recommendations identified through the procedures performed.

Area of Assessment	High	Moderate	Low	Best Practice
Cybersecurity Governance Review				
Information Security Governance	-	1	-	-
Change Management	-	-	-	-
Data Protection	-	-	-	-
Logical Security	-	-	-	-
Business Continuity Management	-	-	-	-
Threat & Vulnerability Management	-	1	-	-
Third Party Risk Management	-	-	-	-
Logging & Monitoring	1	-	-	-
IT Operations	-	-	-	-
Employee Management	-	-	-	-
Configuration Management	-	-	-	-
System Development & Acquisition	-	-	-	-
Physical Security	-	-	-	-
Compliance Management	-	-	-	-
Technical Information Systems Review				
Infrastructure Security				
Server Infrastructure				
• Windows & Active Directory	-	-	-	-
• Virtualization				
Network Infrastructure				
• Network Management & Configuration				
○ Network Intrusion Detection & Prevention Systems (IDPS)	-	-	-	-
○ Web Content Filter				
• Wireless Security				
• Voice Over IP (VoIP)				
• Storage Area Network (SAN)				
Cloud Infrastructure	-	-	-	-

<ul style="list-style-type: none"> Microsoft Azure Amazon Web Services (AWS) 				
Endpoint Security				
Workstation (Desktops & Laptops)	-	-	-	-
Mobile Device Management (MDM)	-	-	-	-
Application Security				
Database Applications				
<ul style="list-style-type: none"> Microsoft SQL Oracle 	-	-	-	-
E-Mail Applications				
<ul style="list-style-type: none"> Microsoft Exchange Microsoft Office 365 (O365) 	-	-	-	-
Threat & Vulnerability Applications				
<ul style="list-style-type: none"> Malicious Code Detection <ul style="list-style-type: none"> Anti-Virus and Anti-malware Host Intrusion Detection & Prevention Systems (IDPS) Patch Management Vulnerability Management 	-	-	-	-
Logging & Monitoring Applications				
<ul style="list-style-type: none"> Security Information & Event Management (SIEM) 	-	-	-	-
Total	1	2	-	-

Top Risks and Priorities

Based upon the interviews and technical testing performed, it was determined that ABC does not have a comprehensive Information Security Program (ISP). Cybersecurity is not a primary responsibility of an individual or department, which has led to an immature cybersecurity control environment, as well as less effective procedural and technical controls. The top risk areas identified during this engagement are summarized below:

- Security Information & Event Management Solution** – ABC’s Windows servers and networking devices are not configured to send audit, security and system logs to a centralized server. All audit, security and system related logs are currently being stored on each individual device. As a result, ABC would not be able to correlate system-related or security-related events across servers and networking devices.
- Information Security Program** – Several policies and procedures have not been documented or reviewed to reflect the current security configurations and standards. Stale policies and documented procedures may result in conflicts arising when performing tasks due to inconsistent and/or lack of documentation. If an individual is unable to perform his or her duties, a formalized and up-to-date procedure will provide guidance for another individual to complete the necessary task.
- Vulnerability Assessments** – ABC has not implemented a process for performing internal vulnerability assessments. As a result, critical vulnerabilities resulting from misconfigurations, vulnerabilities inherent to applications, or missing security patches may be found on the network. Malicious employees or attackers that obtain network access may be able to exploit these vulnerabilities.

The top risks described above will require interpretation by ABC to determine the best course of action for moving this initiative forward. Crowe has also identified additional specific findings that should be included as ABC develops its information security program. These findings are presented in detail in **Section II – Detailed Results and Remediation Plans**.

Each of the detailed findings have also been categorized by the level of risk posed to ABC, as well as the relative effort required to remediate the risk. This analysis will assist ABC in managing and prioritizing effort in remediating the risk of these findings.

Observations that do not represent significant risk at this time but offer opportunities for ABC to further strengthen controls and processes have been documented within **Appendix A – Best Practice Observations**.

Please refer to **Appendix B – Risk & Remediation Effort Ratings** for a detailed listed of remediation effort and risk for all findings.

Information security is an ongoing process and Cybersecurity Audit cannot guarantee the security of a network. Since new vulnerabilities are discovered daily, ABC should continue with ongoing security assessments.

Crowe would like to thank ABC for this opportunity to report the results of this assessment and to thank ABC's personnel for their cooperation and assistance.

II. Detailed Results and Remediation Plans

Finding #1: Logging & Monitoring – Security Information & Event Management Solution
Risk Rating: High
Remediation Effort: High

ABC’s Windows servers and networking devices are not configured to send audit, security and system logs to a centralized server. All audit, security and system related logs are currently being stored on each individual device.

As a result, ABC would not be able to correlate system-related or security-related events across servers and networking devices.

Recommendation

At a minimum, ABC should configure critical servers and networking devices to send audit, system and security logs to a centralized server. By sending all logs to a centralized server, ABC will be protected from these logs being deleted on the physical device intentionally or unintentionally. Additionally, applications which have logging capabilities should be included within the centralized logging collection.

ABC should implement a Security Information and Event Management (SIEM) solution. These log management solutions can assist ABC in managing and reporting on all event log data. These solution enabled ABC to correlate events across all devices with drill down capabilities. Such capabilities will aid in the event of an investigation and allow ABC to perform trending of security incidents. A list of SIEM solutions can be found below:

Common SIEM Vendors	
Alien Vault	http://alienvault.com/community
IBM – Q1	http://q1labs.com/
Log Rhythm	http://www.logrhythm.com/
McAfee Nitro Security	http://www.nitrosecurity.com/
SenSage	http://www.SenSage.com
HP ArcSight	http://www.arcsight.com
Solutionary	http://www.solutionary.com
RSA	http://www.rsa.com/node.aspx?id=3683

Management’s Action Plan

Individual(s) Responsible:
Due Date:

Finding #2: Information Security Governance – Information Security Program
Risk Rating: *Moderate*
Remediation Effort: *Low*

Several policies and procedures have not been documented or reviewed to reflect the current security configurations and standards.

Stale policies and documented procedures may result in conflicts arising when performing tasks due to inconsistent and/or lack of documentation. If an individual is unable to perform his or her duties, a formalized and up-to-date procedure will provide guidance for another individual to complete the necessary task.

The following policies and procedures have been identified as lacking sufficient detail:

Data Protection

- **Data Classification** – Although the organization has formally documented a customer data & handling policy, the policy does not include details for the classification of data. The policy should be enhanced to include standards for confidential, internal only, and public data. This may result in data be mishandled based on the impact which could occur in the event data is compromised. There currently is a process in place to discuss data classification and through the utilization of the Information Security Committee Meetings.

Threat & Vulnerability Management

- **Vulnerability Management Program** – The Vulnerability Management policy/procedure has been found to be lacking details for the identification of vulnerabilities, the corresponding analysis, documentation, and remediation. Without adequately documenting standards and processes, Management may not have the capacity to accurately measure the potential impact of a security vulnerability and effectively apply mitigation techniques.

Incident Response

- **Incident Response Program (IRP)** – While ABC has developed an IRP, the current plan is missing sufficient detail for key incident response activities such as detection and analysis techniques, containment strategies, eradication steps and recovery procedures to effectively respond to a security incident. The current plan does not meet industry best practice standards. Without properly defined incident response procedures there is an increased risk of mishandling data, taking incorrect actions in response to an incident, and delays in communicating information to employees, management, and law enforcement.

Recommendation

ABC should develop and review all policies and procedures to reflect the current security standards and practices within the ABC environment. At a minimum, ABC should perform a yearly review, update, and approval of the Information Security policies and if applicable, procedures.

Data Protection

- **Data Classification** – ABC should enhance the current Customer Data and Handling Policy to include how data is classified and the various levels of classification. Some considerations would be to include the various levels of classification and detail which type of data falls into which classification category, such as but not limited to, Confidential, Internal Only, and Public. Additionally, if the quantity or how the data is used affects the classification of the data then this should be included as well.

Threat & Vulnerability Management

- **Vulnerability Management Program** – With a large number of systems in the enterprise, it is important that all systems such as servers, networking devices, and workstations are being adequately monitored for any outstanding vulnerabilities. ABC should document policies and procedures for identifying vulnerabilities as they arise in order to recognize trends and take subsequent security measures. This should include basic vulnerability scanning to identify potential risks that can be exploited.

The policy should include the following standards:

- Use of Vulnerability Scanner – All devices and assets connected to the network should be scanned to ensure they are in compliance with system configuration standards.
- Scan Frequency – Scans should occur on a monthly basis (or whenever a new machine is added to the network) and the results should be documented for review of anomalies.
- Vulnerability Severity Scale – Any documented vulnerabilities should be ranked according to the severity of risk posed to the network. Response procedures and timelines should be based according to this risk ranking.
- Vulnerability Documentation – All vulnerabilities should be documented to include ratings, remediation plans, and review approvals.

Furthermore, procedures should be enhanced to detail the following steps. Scans should be performed on a monthly basis, during the deployment of new applications and networked systems, and when significant changes to the network environment are made. Ad-hoc scans should be performed as necessary and agreed upon during the change management process.

The results of all vulnerability assessments of all networked systems should be reviewed by Information Technology in order to document known vulnerabilities. All vulnerabilities must be formally tracked including, risk ratings, action plans, and remediation timelines. These risk ratings, action plans, and remediation timeframes should be documented in a vulnerability tracking log. The vulnerability tracking log should be reviewed on a basis that corresponds with Management's risk appetite (at minimum monthly reviews are recommended).

A validation scan should be performed to ensure the vulnerabilities identified are addressed. The results of this validation scan should be reviewed and stored in the vulnerability tracking log for documentation purposes.

Incident Response

- **Incident Response Program (IRP)** – While ABC has developed an IRP, the current program is missing sufficient detail for key incident response activities such as detection and analysis techniques, containment strategies, eradication steps and recovery procedures to effectively respond to a security incident. The current program does not meet industry best practice standards. Without properly defined incident response procedures there is an increased risk of mishandling data, taking incorrect actions in response to an incident, and delays in communicating information to employees, management, and law enforcement. The National Institute of Standards and Technology offers guidance on how organizations should develop and structure their IRP. Further information can be found at the following location:

- <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Management's Action Plan

Individual(s) Responsible:

Due Date:

Finding #3: Threat & Vulnerability Management – Vulnerability Assessments
Risk Rating: *Moderate*
Remediation Effort: *Moderate*

ABC has not implemented a process for performing internal vulnerability assessments.

As a result, critical vulnerabilities resulting from misconfigurations, vulnerabilities inherent to applications, or missing security patches may be found on the network. Malicious employees or attackers that obtain network access may be able to exploit these vulnerabilities.

Recommendation

ABC should implement a solution for performing vulnerability assessments for hardware and software on the network. ABC should also perform basic vulnerability scanning to identify potential risks that can be exploited, including missing patches and open ports on servers and workstations.

An automated tool should be used to perform vulnerability scanning of all devices on the ABC network, including both internally and externally facing devices. These scans should be performed on an organization defined basis. IT management should evaluate the results of the scans and determine mitigating controls for the detected vulnerabilities. These vulnerabilities should be tracked in a vulnerability management document from inception through mitigation. The vulnerability management document should be discussed in the Risk Management Committee meetings and presented to the Board of Directors during their annual meeting. The vulnerability management program, as documented in Finding #1, should be followed, including tracking process and documenting exception. Tools that can provide these capabilities include the following:

Vulnerability Assessment Tools

QualysGuard – Network device and application discovery and management as well as vulnerability identification and remediation. (<http://www.qualys.com/>)

GFI LANguard – Network vulnerability scanner and auditing tool. (<http://www.gfi.com/languard/>)

Nessus – UNIX or Windows based network vulnerability scanner. (<http://www.nessus.org/>)

Management's Action Plan

Individual(s) Responsible:
Due Date:

III. Summary of Scope

The scope of procedures, which was developed using industry Cybersecurity guidance, included inquiry and/or testing in the following activities and processes:

Cybersecurity Governance Review

Information Security Governance

- Information Security Program
- Roles & Responsibilities
- Oversight & Strategy
- IT Risk Management

Data Protection

- Data Management (Handling & Classification)
- Data Inventory
- Data Protection Controls
- Data Sanitization & Destruction
- Encryption

Threat & Vulnerability Management

- Malicious Code Detection
- Patch Management
- Threat Intelligence
- Vulnerability Management

Physical Security

- Physical Information Security
- Data Center Security
- Physical Access
- Physical Monitoring & Detection
- Physical Audit Log & Review
- Clean Desk

Logical Security

- Identification & Access Control
- Authentication
- Access Management (Least Privilege & Segregation of Duties)
- Access Reviews

Logging & Monitoring

- Audit & Logging Management
- Audit Configuration
- Audit Log Aggregation
- Audit Monitoring & Detection
- Audit Alerting
- Audit Log Review

IT Operations

- Asset Management
- Asset Lifecycle (Procurement, Transfer, Destruction)

Business Continuity Management

- Business Impact Assessment
- Business Continuity & Contingency Planning
- IT Resiliency & Backup Processes
- Disaster Recovery Planning
- Incident Response Procedures

Third Party Risk Management

- Third Party Security Oversight
- Third Party Inventory
- Third Party Network Access
- Third Party Contracts
- Third Party Due Diligence

Employee Management

- Employee Standards
- Hiring Practices
- Job Transition Practices
- Termination Practices
- Security Training

Configuration Management

- Approved Infrastructure
- Standard Build Procedures
- Configuration Certification

Change Management

- Change Control
- Maintenance

System Development & Acquisition

- Development & Acquisition Standards
- Project Management (System Security Plans)
- Coding Practices
- Testing

Compliance

- Compliance & Regulatory Standards

Technical Information Systems Review

Infrastructure Security

- Server Infrastructure
 - Windows & Active Directory
 - Virtualization
- Network Infrastructure
 - Network Management & Configuration
 - Network Intrusion Detection & Prevention Systems (IDPS)
 - Web Content Filter
 - Wireless
 - Voice Over IP (VoIP)
 - Storage Area Network (SAN)
- Cloud Infrastructure
 - Microsoft Azure
 - Amazon Web Services (AWS)

Endpoint Security

- Workstation (Desktops & Laptops)
- Mobile Device Management (MDM)

Application Security

- Database Applications
 - Microsoft SQL
 - Oracle
- E-Mail Applications
 - Microsoft Exchange
 - Microsoft Office 365 (O365)
- Threat & Vulnerability Applications
 - Malicious Code Detection
 - Anti-Virus & Anti-malware
 - Intrusion Detection & Prevention Systems (IDPS)
 - Patch Management
 - Vulnerability Management
- Logging & Monitoring Applications
 - Security Information & Event Management (SIEM)

The specific procedures performed were based on the concepts of selective testing. Although Crowe's testing was performed in some areas without exception, Crowe can provide no assurance that exceptions would not have been detected had procedures been changed or expanded.

Information technology assessments are an ongoing process. A Cybersecurity Audit does not guarantee the proper functioning of controls reviewed or security of a network or systems assessed or physical security or prevention of fraud or privacy of data or compliance with banking regulations. The nature, timing, and extent of the procedures performed were based on the concepts of selective testing. This report presents findings and recommendations resulting from the performance of these procedures. Although our testing was performed in some areas without exception, we can provide no assurance that exceptions would not have been detected had procedures been changed or expanded. While we rate our findings, we encourage management to consider addressing all findings as all findings (regardless of rating) over time may pose risk to the organization's security and controls.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data. Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate.

IV. Appendix A – Best Practice Observations

Information Security Governance

- Segregation of duties does not exist since the Information Security Officer and the Chief Information and Technology Officer, since the ISO reports to the CITO for all security activities.
- The annual report to the board that includes key risk indicators does not provide trend information or action plans based on the organization's acceptable level of risk.

Threat & Vulnerability Management

- The organization does not have a comprehensive patch management program. Noted during the assessment:
 - Ancillary patches are not applied consistently or within a timely manner based on patch reports and vulnerability scans.
 - A consistent patch management process for the core applications (i.e., the review of missing patches or patch reports pre-and-post deployment).

Logical Security

- Technical controls have not been implemented to specify or restrict concurrent and timeout sessions for VPN access.

Logging & Monitoring

- An evaluation has not been performed for the application (including the core) to determine the current audit and logging configuration and capabilities.

IT Operations

- A process has not been implemented to evaluate installed software periodically, based on the asset inventory to determine the following:
 - Required for business use; and,
 - Up-to-date or end-of-life.

Third Party Risk Management

- Although a list of third-party providers is documented, the documented list is not categorized by risk.
- The due diligence process does not include a review of security controls and security best practices to verify they follow industry and organizational security standards.

Configuration Management

- ABC has not implemented technical controls to governing the installation of software by users to prevent unauthorized software installation (e.g., Application Whitelisting \ Blacklisting).
- A process has not been implemented on a periodic basis (i.e., weekly, monthly, etc.) to recertify information systems to verify they meet industry standards and to detect unauthorized changes.

Compliance Management

- A process has not been implemented to formally monitor compliance with regulatory standards such as GDPR, HIPAA, PCI, etc.

V. Appendix B – Risk & Remediation Effort Ratings

We have assigned recommended risk and remediation ratings for each finding. Our assignments are subjective based on the current infrastructure at ABC and our experience with other clients.

Finding #	Domain	Name	Risk Rating	Remediation Effort
1	Logging & Monitoring	Security Information & Event Management Solution	High	High
2	Information Security Governance	Information Security Program	Moderate	Low
3	Threat & Vulnerability Management	Vulnerability Assessments	Moderate	Moderate



Smart decisions. Lasting value.™

ABC, Inc.

Internal Audit Report

Information Technology General Control and IT SOx Key Control Testing
October 2024

ABC, Inc.
Internal Audit Report
ITGC and SOx
October 2024

Table of Contents

I. Background.....	1
Summary of Scope.....	1
Internal Audit Reporting Timeline	2
II. Findings Summary	3
Summary of Findings in each Area of Assessment	3
Findings Results Dashboard	4
Legend of Report Symbols	5
III. Detailed Findings.....	6
IV. Appendix	11
Reporting Methodology.....	11

ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

I. Background

Crowe LLP (“Crowe”) performed an internal audit related to Information Technology General Controls for Credit First National Association (the “Company”, the “Bank”, or “ABC, Inc.”) for the audit period of September 1, 2023 to August 31, 2024. Crowe also performed applicable IT SOx key control testing for ABC, Inc.

The overall objective was to assess the controls over the audit areas listed in the Summary of Scope section below. We read selected policies and procedures, discussed these policies and procedures with the Company’s personnel, and in some cases inspected certain detailed records.

Summary of Scope

The scope of procedures included inquiry and/or testing in the following audit areas and processes:

Areas in Scope		
Information Technology General Controls (ITGC)		
Business Continuity Planning / Disaster Recovery (BCP / DR)	GLBA 501(b), Program Gap Analysis	Logical Security – First Data / MSS
<ul style="list-style-type: none"> Board and Management Oversight Existence and Coverage Business Impact Analysis Risk Monitoring 	<ul style="list-style-type: none"> Oversight and Governance Risk & Threat Assessments Policy Requirements Information Security Program Training Information Security Program Testing 	<ul style="list-style-type: none"> General Security Management System Provisioning System De-Provisioning Administrator Access Password Security Access Level Review Logging and Monitoring
Physical Security	Wire Transfer Security – FedLine Advantage	
<ul style="list-style-type: none"> Environmental Controls Physical Controls 	<ul style="list-style-type: none"> Policies & Procedures System Access Access Level Review Logging and Monitoring Wire Verification Token Security Contingency Planning 	

Areas in Scope

This document and the information in it (the “Report”) has been prepared by Crowe LLP in accordance with the terms of our written agreement. The Report is intended solely for the use of the legal entity that has engaged Crowe to perform the services and prepare the Report (the “Client”). The Report is confidential. Except for the permitted use of the Report by Client, Crowe hereby disclaims any and all responsibility and liability for the Report and the use thereof. No other person or entity may rely on the Report or the information contained in it for any purpose, and Crowe makes no representation to any other person or entity as to the accuracy, sufficiency or propriety of the information contained in the Report. Crowe also disclaims any obligation to update the Report.

ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

IT SOx Key Control Testing (IT SOx)		
Logical Security	Change Management	Computer Operations
<ul style="list-style-type: none"> • Network • MSS • Fiserv First Data • Automate • CyberArk • KeyCloak • SQL Servers & Databases • Linux Servers 	<ul style="list-style-type: none"> • Network • MSS • Fiserv • Automate • CyberArk • KeyCloak 	<ul style="list-style-type: none"> • Network • MSS • Fiserv • Automate

The specific procedures performed were based on the concepts of selective testing. Although our testing was performed in some areas without exception, we can provide no assurance that exceptions would not have been detected had procedures been changed or expanded.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that procedures are performed in accordance with management’s intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data. Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate.

Internal Audit Reporting Timeline

Draft Report Date: <>
Management’s Response Date: <>
Final Report Date: <>

This document and the information in it (the “Report”) has been prepared by Crowe LLP in accordance with the terms of our written agreement. The Report is intended solely for the use of the legal entity that has engaged Crowe to perform the services and prepare the Report (the “Client”). The Report is confidential. Except for the permitted use of the Report by Client, Crowe hereby disclaims any and all responsibility and liability for the Report and the use thereof. No other person or entity may rely on the Report or the information contained in it for any purpose, and Crowe makes no representation to any other person or entity as to the accuracy, sufficiency or propriety of the information contained in the Report. Crowe also disclaims any obligation to update the Report.

ABC, Inc.
Internal Audit Report
ITGC and SOx
October 2024

3

II. Findings Summary

Summary of Findings in each Area of Assessment

Your Chief Internal Auditor approved the scope of this audit, based on risk assessment ratings assigned to each audit area. The procedures and results of procedures were communicated to Management and your Chief Internal Auditor. The table below shows a summary of the number of findings in each area of assessment by Finding Priority Rating:

Area of Assessment	High	Moderate	Low	Best Practice
Information Technology General Controls				
Business Continuity Planning / Disaster Recovery	-	-	-	-
GLBA 501(b), Program Gap Analysis	-	-	-	1
Logical Security	-	1	1	-
Physical Security	-	-	-	-
Wire Transfer Application Security	-	-	-	-
IT SOx Key Control Testing				
Logical Security	-	1*	1*	-
Change Management	-	1	-	-
Computer Operations	-	-	-	-




*Represents a finding applicable to multiple areas of assessment.

This document and the information in it (the "Report") has been prepared by Crowe LLP in accordance with the terms of our written agreement. The Report is intended solely for the use of the legal entity that has engaged Crowe to perform the services and prepare the Report (the "Client"). The Report is confidential. Except for the permitted use of the Report by Client, Crowe hereby disclaims any and all responsibility and liability for the Report and the use thereof. No other person or entity may rely on the Report or the information contained in it for any purpose, and Crowe makes no representation to any other person or entity as to the accuracy, sufficiency or propriety of the information contained in the Report. Crowe also disclaims any obligation to update the Report.

ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

Findings Results Dashboard











A summary of the findings from this internal audit is provided in the table below:

Finding Priority Rating	Process Area	Sub-Process	Finding Title	Repeat / Recurring	Key Control	Root Cause	Due Date	Action Plan Owner(s)
 Moderate	Logical Security	Access Level Review	Finding #1: User Access Level Reviews	-		 Process	<TBD>	<TBD>
 Moderate	Change Management	Change Control Documentation	Finding #2: Change Management Approval Documentation	-		 Process	<TBD>	<TBD>
 Low	Logical Security	System Provisioning	Finding #3: Access Approval	-		 Process	<TBD>	<TBD>
 Best Practice	GLBA 501(b), Program Gap Analysis	Information Security Program Testing	Finding #4: Information Security Program Testing	-	-	 Process	N/A	N/A

This document and the information in it (the "Report") has been prepared by Crowe LLP in accordance with the terms of our written agreement. The Report is intended solely for the use of the legal entity that has engaged Crowe to perform the services and prepare the Report (the "Client"). The Report is confidential. Except for the permitted use of the Report by Client, Crowe hereby disclaims any and all responsibility and liability for the Report and the use thereof. No other person or entity may rely on the Report or the information contained in it for any purpose, and Crowe makes no representation to any other person or entity as to the accuracy, sufficiency or propriety of the information contained in the Report. Crowe also disclaims any obligation to update the Report.




ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

Legend of Report Symbols

Impact Areas		Finding Priority Rating	
Symbol	Meaning	Symbol	Meaning
	People		High
	Process		Moderate
	Technology		Low
			Best Practice
			Key Control Indicator
			Repeat Issue Indicator
			Recurring Issue Indicator

This document and the information in it (the "Report") has been prepared by Crowe LLP in accordance with the terms of our written agreement. The Report is intended solely for the use of the legal entity that has engaged Crowe to perform the services and prepare the Report (the "Client"). The Report is confidential. Except for the permitted use of the Report by Client, Crowe hereby disclaims any and all responsibility and liability for the Report and the use thereof. No other person or entity may rely on the Report or the information contained in it for any purpose, and Crowe makes no representation to any other person or entity as to the accuracy, sufficiency or propriety of the information contained in the Report. Crowe also disclaims any obligation to update the Report.

III. Detailed Findings

Finding Priority Rating	Process Area	Sub-Process	Finding Title	Repeat / Recurring	Key Control	Root Cause	Due Date	Action Plan Owner(s)
 Moderate	Logical Security	Access Level Review	Finding #1: User Access Level Reviews	-		 Process	<TBD>	<TBD>

Condition: The following issues were identified in regard to application user access reviews:

- Forty out of forty-three (~93%) users identified to be removed following the Q1 2022 MSS user access level review remained on the system, including two sampled terminated employees. Additionally, the reviewer is reviewing and approving their own access.
- The 2021 Q4 and 2022 Q1 Fiserv First Data user access level review process identified the following:
 - Reviewers reviewed their own access;
 - For departments where multiple reviewers are responsible for completing the User Access Review, reviews were incomplete and upon inquiry, management indicated that the remaining users were reviewed by an additional reviewer. However, the submitted review documentation did not indicate that certain users were to be reviewed by a different individual, resulting in the documentation of the review being incomplete.
 - An individual was missing from the reviewed Fiserv First Data user listing due to the manual process used to parse the reviewer responsibilities, therefore, the review relied upon a report that was not verified to be complete and accurate.

Criteria: Management’s SOx Key Control states, “User access is periodically reviewed.” An independent periodic review of user accounts and their privileges should be performed at least annually to identify unauthorized access and re-confirm appropriateness of existing access. Any inappropriate access rights should be promptly removed. Evidence of the review and resulting actions should be retained to support the review activities performed.

Root Cause: Management was unaware of the potential risks resulting from users reviewing their own access and did not consider that reviewers should be documenting a conclusion (approval or change request) for each user’s access, else indicate that the user will be reviewed by a different business / application owner. Further, competing priorities resulted in identified terminated employees remaining with access to the MSS system post-review.

Implication: Users may have inappropriate access to systems, programs and data, resulting in the potential for unauthorized changes to system settings and/or system data. Additionally, allowing an individual to review their own access creates a segregation of duties issue as the individual may be reviewing system/access changes that they initiated and/or allowing themselves unnecessary increased access. Further, if documentation is not maintained, management is unable to demonstrate the review activities performed, and unauthorized or elevated access rights could go undetected.

ABC, Inc.
Internal Audit Report
ITGC and SOx
October 2024


7

Recommendation: Management should perform an independent review of all users and each user's corresponding access levels on the identified systems at least annually. As Management is in the process of assessing its current access level review process, we recommend Management consider the following:

- The individual(s) performing the review should be:
 - Validating that all user accounts have permissions reflective of their job roles / functions. The reviewer should also include a review of all groups / roles on the system and the access permissions they possess.
 - Knowledgeable of the system and the corresponding access levels and groups / roles.
 - Independent from those who have administrator capabilities on the application (i.e., can create users or modify access). If this review cannot be independent, the review should be performed as a dual review. Dual reviews can be performed by two administrators or by an administrator and a non-administrator.
 - Independent from the access being reviewed (i.e., reviewer should not review and approve their own access)
- Management should maintain documentation of the review being performed, including all user listings distributed and all responses gathered from Department Managers / Supervisors (if applicable).
- Management should validate changes identified from the review have been applied to the application(s).
- Given the increased risk of review integrity when manually parsing out user lists, Management should implement verification controls around user report completeness and accuracy to confirm all users and rights are included within the review.

Management's Action Plan: <>

ABC, Inc.
Internal Audit Report
ITGC and SOx
October 2024

Finding Priority Rating	Process Area	Sub-Process	Finding Title	Repeat / Recurring	Key Control	Root Cause	Due Date	Action Plan Owner(s)
 Moderate	Change Management	Change Control Documentation	Finding #2: Change Management Approval Documentation	-		 Process	<TBD>	<TBD>

Condition: Five out of eighteen (~28%) sampled changes did not have documented approval for the change to move into production.

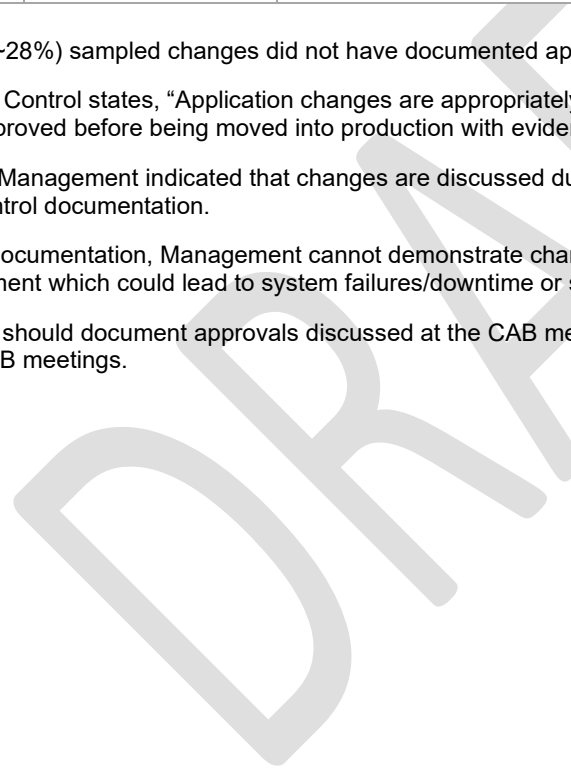
Criteria: Management’s SOx Key Control states, “Application changes are appropriately tested and approved before being moved to production.” Application changes should be tested and approved before being moved into production with evidence of these actions retained.

Root Cause: Conversations with Management indicated that changes are discussed during Change Advisory Board (CAB) meetings and approvals are not retained as part of the change control documentation.




Implication: Without supporting documentation, Management cannot demonstrate changes were approved. This may result in unapproved changes being applied to the production environment which could lead to system failures/downtime or security issues.

Recommendation: Management should document approvals discussed at the CAB meetings. This can be evidenced via existing change management tickets or via meetings minutes from the CAB meetings.

Management’s Action Plan: <>



ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

Finding Priority Rating	Process Area	Sub-Process	Finding Title	Repeat / Recurring	Key Control	Root Cause	Due Date	Action Plan Owner(s)
 Low	Logical Security	System Provisioning	Finding #3: Access Approval	-		 Process	<TBD>	<TBD>

Condition: One out of eight (12.5%) sampled new hires received access to the MSS application without documented approval. Of note, subsequent conversations with management determined the access granted is appropriate based on the employee’s job function.

Criteria: Management’s SOx Key Control states, “Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties.” Access to system resources should be provided on a business-need basis commensurate with the user’s job responsibilities and authorized by appropriate management.

Root Cause: Due to procedures not being followed, approval was not captured prior to provisioning the identified users’ access.



Implication: Without following a consistent and documented user access request process across all of the Bank’s systems, the risk exists that unnecessary or unauthorized access could be granted on the Bank’s systems.

Recommendation: Management should reinforce to employee’s that all access requests must include approval from a user’s respective supervisor. As a reminder, all of the following items should be documented as part of the Bank’s access provisioning process:

- Manager/Supervisor approval for the access request
- Systems that the Manager/Supervisor is requesting that the user being granted access to
- Access levels that the Manager/Supervisor is requesting the user be granted on each application

Management’s Action Plan: <>

ABC, Inc.
 Internal Audit Report
 ITGC and SOx
 October 2024

Finding Priority Rating	Process Area	Sub-Process	Finding Title	Repeat / Recurring	Key Control	Root Cause	Due Date	Action Plan Owner(s)
 Best Practice	GLBA 501(b), Program Gap Analysis	Information Security Program Testing	Finding #4: Information Security Program Testing	-	-	 Process	N/A	N/A

Condition: Management does not periodically test employees for compliance with the standards outlined in the Information Security or Clean Desk Policies.

Criteria: Management should conduct testing, at least annually, to assess whether employees are in compliance with the standards outlined within the Information Security and Clean Desk Policies.

Root Cause: Management noted that testing has not been performed due to limited perceived risk, as departments are accessible only to authorized personnel. Additionally, employees are required to sign-off on the Clean Desk Policy annually.

Implication: Non-compliance with Information Security Policy requirements may not be identified and addressed timely, resulting in potential breach or disclosure of sensitive information.

Recommendation: Management should perform Information Security Program testing on an annual basis to validate employees are following prescribed policies. Results of testing should be documented and discussed during Information Security update reports to the Technology Committee.

IV. Appendix

Reporting Methodology

In this report, we provide a summary of our results and recommendations as well as management's responses. To assist you in analyzing our recommendations, we have provided our suggestions to prioritize corrective action based on the finding's exposure to loss or increased regulatory scrutiny, as follows:

High – Requires immediate remedy and, if left uncorrected, exposes the organization to significant or immediate risk of loss, asset misappropriation, data compromise or interruption, fines and penalties, or increased regulatory scrutiny.

Moderate – Requires timely remedy and, if left uncorrected, may expose the organization to risk of loss or misappropriation of company assets, compromise of data, fines and penalties, or increased regulatory scrutiny. These issues should be resolved in a timely manner, but after any high priority issues.

Low – Should be addressed as time and resources permit. While it is not considered to represent significant or immediate risk, repeated oversights without corrective action or compensating controls could lead to increased exposure or scrutiny.

Best Practice – Represents operational efficiencies or improvements for consideration by management based on industry best practices and Crowe's experiences.

Key Control – Represents an issue related to one or more of the Company's key controls. We have identified these issues to assist management with their remediation actions.

Repeating Issue – Represents an issue that was previously identified but has not been corrected as planned.

Recurring Issue – Represents an issue that is similar in cause, implication, or outcome to items previously reported.



Smart decisions. Lasting value.™

ABC, Inc.

IT Risk Assessment

March 2022

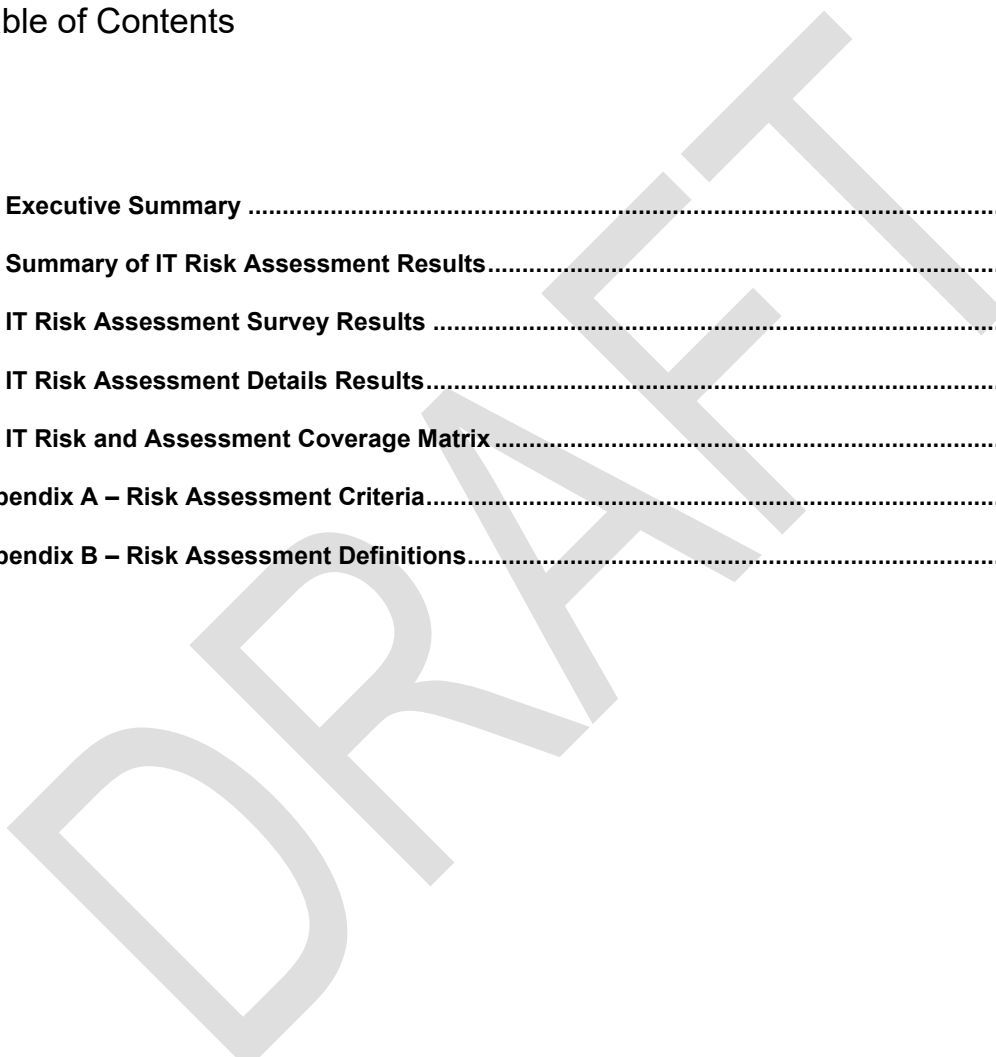


ABC, Inc.

IT Risk Assessment

Table of Contents

I. Executive Summary	1
II. Summary of IT Risk Assessment Results.....	4
III. IT Risk Assessment Survey Results	5
IV. IT Risk Assessment Details Results.....	7
V. IT Risk and Assessment Coverage Matrix.....	3
Appendix A – Risk Assessment Criteria.....	7
Appendix B – Risk Assessment Definitions.....	9



I. Executive Summary

Overview

ABC, Inc. ("ABC") engaged Crowe LLP ("Crowe") to conduct an Information Technology (IT) Risk Assessment as of March 2022.

The goal of this IT risk assessment is to:

- Identify the IT risks potentially impacting the organization;
- Determine the potential impact, likelihood, and velocity of the risks being realized;
- Gain a preliminary understanding of the design of internal controls; and,
- Develop a 3-year internal audit plan to evaluate the effectiveness of the controls mitigating the most critical risk areas.

To accomplish these objectives, the following activities were performed:

- Conducted workshops with personnel across the IT organization to understand their roles and responsibilities, key risks they have identified, and the day to day activities they perform to help manage certain risks;
- Met with Senior Leadership, department managers, and key employees across various lines of business to understand their perspective on IT risk and effectiveness of IT controls managing risk;
- Conducted a survey of IT personnel to have them rate different risk criteria (i.e. impact, likelihood, velocity, control effectiveness) to better understand employees' perception of IT risks;
- Reviewed various documents provided by ABC, including but not limited to:
 - Information security policies and procedures
 - Strategic planning materials and roadmap materials
 - Organizational charts
 - Enterprise risk management materials
 - IT project management documentation

These activities assisted with the development of the IT Risk Assessment by providing individual unique perspective on IT risk. Once all the information was gathered, an evaluation and analysis was performed to determine the overall IT risk posture of the organization, documented the results, and provided a recommended 3-year IT audit plan to evaluate control effectiveness for the most critical risk areas.

The Internal Audit Director, in conjunction with the Audit Committee, are responsible for determining and approving the risk assessments and related scope provided in this document.

Risk Assessment Methodology

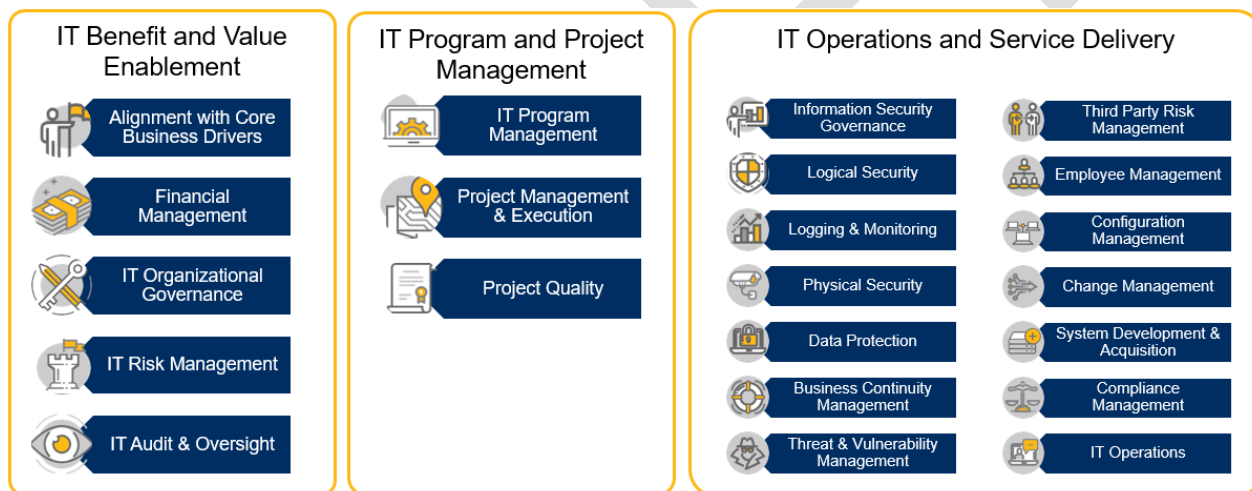
Risk is generally defined as the combination of the probability of an event occurring and the subsequent consequence if that risk is realized. IT risk is business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise. More specifically, IT risk consists of any IT-related events that could potentially impact the business and/or create challenges in meeting strategic goals and objectives.

Crowe's IT risk assessment methodology leverages multiple industry frameworks, including NIST 800-30r1, ISACA's Risk IT Framework, and COBIT 5 for Risk.

- The overall risk assessment methodology most closely aligns with NIST 800-30r1. This framework depicts four key steps:
 - Step 1: Prepare for the Assessment

- Step 2: Conduct the Assessment
- Step 3: Communication of Results
- Step 4: Maintain Assessment
- One key step to any risk assessment is to define the universe of risks that is required to be evaluated for an organization. Using a combination of regulatory requirements and industry standard frameworks, a custom IT risk universe was created that consisted of 29 unique risk components. This IT universe is based on a combination of risks derived from ISACA’s Risk IT framework and COBIT 5, as well as Crowe and ABC’s industry expertise. The universe is divided across three IT risk domains, which are further segmented into twenty-one unique risk categories.
 - IT Benefit and Value Enablement
 - IT Program and Project Management
 - IT Operations and Service Delivery
- To make sure the IT Risk Universe comprehensively considers all potential risk scenarios, each of these domains is segmented into number of IT Risk Categories which consist of several IT risk scenarios. These risks scenarios have been created based on COBIT 5 for Risk, supplemented with Crowe’s industry expertise.

This IT Risk Universe was reviewed with ABC and customized based on their specific risk profile. The final risk universe is depicted below.



Each category of the IT Risk Universe was rated a risk level of **High**, **Medium**, or **Low** based on information gathered during the interviews, the risk assessment survey, previous risk assessments, and previous audits and control assessments. The factors considered with rating the risk included

- Potential **impact** if the risk event occurred.
- **Likelihood** of the risk event occurring.
- **Velocity** of the risk events impact to the organization.
- **Perceived effectiveness** of the security controls.

The criteria utilized to determine Impact, likelihood, velocity and control effectiveness are referenced in **Appendix A – Risk Assessment Criteria**.

In addition to overall risk, the direction of the risk was rated for each category. The direction of risk is a critical consideration as it considers the environment around a risk and how that might influence the impact or likelihood of a risk over time. For example, the organization may be pursuing new market facing solutions that will be implemented in the future that could impact the risk associated with the solutions supporting that initiative. Risk direction may be Increasing (I), Decreasing (D), or Stable (S).

Once risks were evaluated, a 3-year IT Audit Plan was developed to provide independent oversight of the operating effectiveness of key controls mitigating the most critical IT risks. The plan includes a combination of operational reviews of IT processes and technical reviews of system configurations.

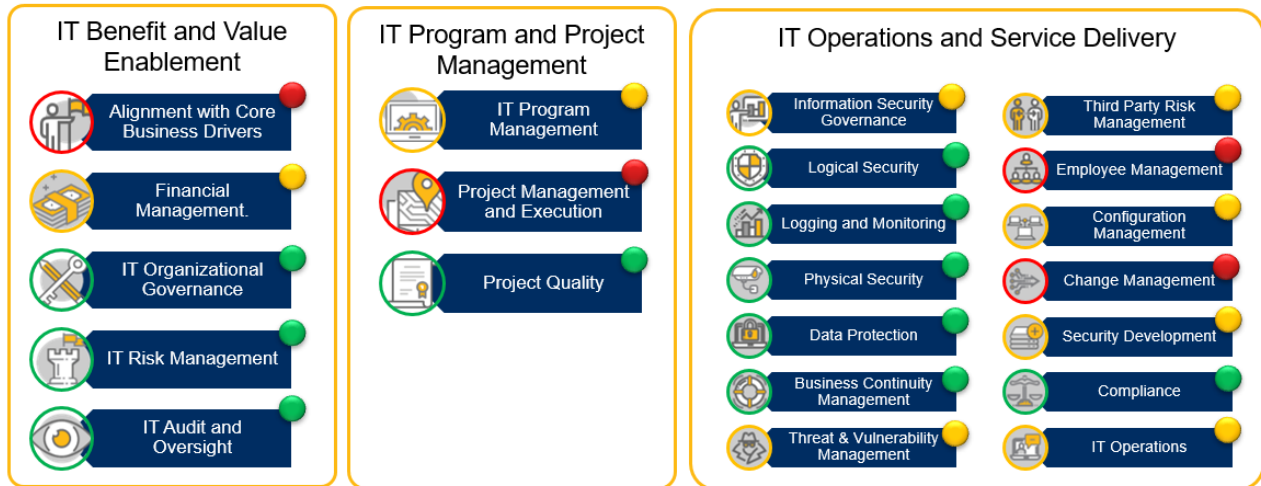
Ongoing IT Risk Assessments are a key component of an overall enterprise risk management program. ABC should perform regular IT Risk Assessments to maintain a current perspective of IT risks and to confirm programs are aligned with the most critical risks for the organization.

II. Summary of IT Risk Assessment Results

Based on all the feedback provided during the engagement, including interviews and survey results, the top risks identified during the engagement were:

- Depth of IT capabilities – Based on discussions with personnel, they did not feel the IT team was adequately staffed to support the business. Personnel felt this led to increased risk in other areas within IT, such as over-reliance on certain IT individuals for key projects and single-points-of-failure within the team. In addition, personnel felt that less critical projects and applications do not get enough support and issues are not resolved in a timely manner.
- Reliance on legacy and end-of-life technologies – There is a reliance on systems within ABC that are not running the latest available version of the solution. There are multiple current projects within IT that were initiated due to a failure within a legacy technology that was not proactively managed. Failing to maintain systems and technology with vendor supported versions increases the likelihood of unplanned downtime or other operational impacts for the organization.
- Varying perception of IT risk – These risks represent the most common themes across all the interviews; however, personnel in the business had a different perspective of the top IT risks than IT personnel. Business personnel felt that the top IT risks were related to project management and technical debt. However, IT personnel felt the top risks were related to programs that were not operating effectively, such as Change Management.

The dashboard diagram below summarizes the overall results of the risk assessment across all risk categories.



In general, the survey results support the top risk areas identified during the interviews with IT and business personnel. Interestingly, the results of the survey of IT personnel line up most closely with the results based on the interviews of business personnel across ABC. Specifically, the top Inherent Risk areas from the survey, Alignment with Core Business Drivers and IT Project Management, line up very directly with the feedback received during interviews.

III. IT Risk Assessment Survey Results

A survey was conducted in order to gather feedback from a broad range of personnel across the IT organization. Personnel were asked to rate separate criteria when analyzing each risk:

- Potential **impact** if the risk event occurred.
- **Likelihood** of the risk event occurring.
- **Velocity** of the risk events impact to the organization.
- **Perceived effectiveness** of the security controls.

The rating scales used by personnel are included in **Appendix A – Risk Assessment Criteria**.

The chart below shows the results of the risk assessment survey based on the Inherent Risk ratings for each category.



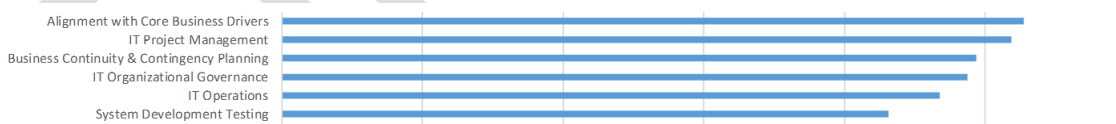
***Sample of Control Categories are presented above.**

As seen in the table, the top risk areas considering inherent risk based on the survey include:

1. Alignment with Core Business Drivers
2. Logical Attacks
3. Vulnerability Management
4. Logical Security

Personnel were also asked to rate their perception of the overall effectiveness of the controls mitigating these IT risks. The survey showed that the control effectiveness for every risk category was rated Highly Effective. This showed that IT personnel have a high level of confidence in the controls in place to manage these IT risks.

However, a deeper analysis shows some nuance in the levels of confidence in the controls across the categories.



***Sample of Control Categories are presented above.**

An analysis of the top residual risks shows a slight shift in the top 5 risk categories:

1. Alignment with Core Business Drivers
2. IT Project Management
3. Business Continuity Management and Planning
4. IT Organizational Governance
5. IT Operations

While respondents were confident in the overall control environment, overall, there was less confidence in the control effectiveness across these categories.

ABC, Inc.
IT Risk Assessment
March 2022

6

The chart compares the Inherent Risk ranking against the Residual Risk ranking based on the survey responses. In the chart, a negative number in the comparison column shows a risk category whose residual risk ranking is higher than the inherent risk ranking, meaning there is, in general, less confidence comparatively in the controls around this area. In general A positive number depicts more confidence in controls.

Please note, the lowest negative numbers do not necessarily reflect a category that was viewed as the lowest control effectiveness (or positive numbers reflect the strongest controls). These just represent the most significant movement when comparing the different rating criteria.

In this chart, you see the areas with the most significant increases in Residual Risk comparative to Inherent Risk are around System Development Testing and Project Quality. Conversely, the areas with the most significant drop include Logical Security and Malicious Code Detection, which demonstrates a general confidence in the controls in these risk areas.

IT Risk Category	Inherent Risk Rank	Residual Risk Rank	IR vs RR Comparison
System Development Testing	12	6	-6
Project Quality	24	20	-4
IT Risk Management	8	7	-1
IT Operations	11	11	-0
Only a sample of IT Risk Categories are presented above.			

Interestingly, the results of the survey of IT personnel line up most closely with the qualitative results from the interviews of business personnel across ABC, specifically that the top Inherent Risk areas are Alignment with Core Business Drivers and IT Project Management. However, some of the top risk areas expressed by IT personnel during interviews, such as Change Management, were rated much lower comparatively within the surveys.

IV. IT Risk Assessment Details Results

The following section summarizes the results for each risk category based on all the feedback provided during the engagement, including interviews and survey results. The results are broken down across each of the three domains:

- IT Benefit and Value Enablement
- IT Program and Project Management
- IT Operations and Service Delivery

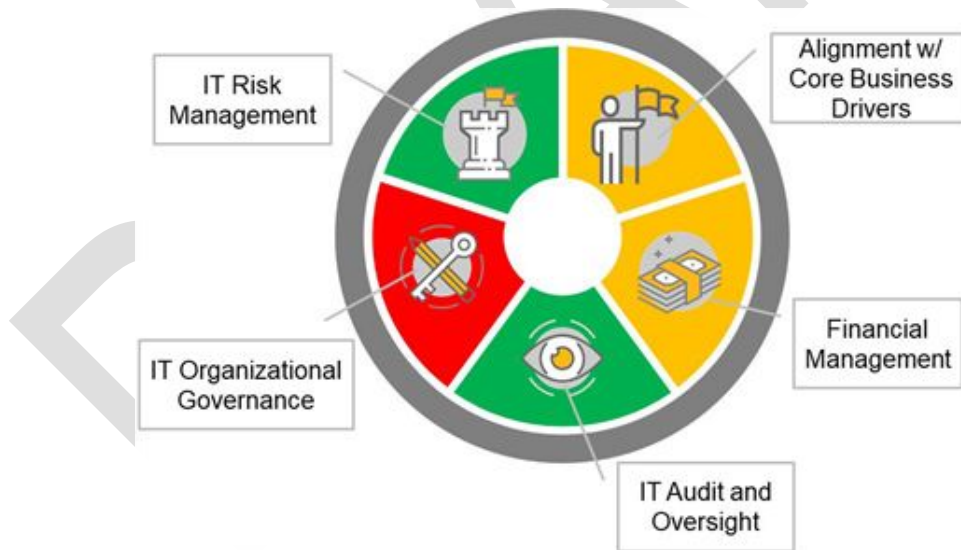
IT Benefit and Value Enablement

The IT Benefit and Value Enablement domain considers risks associated with opportunities to use technology to improve the efficiency or effectiveness of business processes or as an enabler for new business initiatives.

IT Benefit and Value Enablement is segmented into five (5) risk categories:

- **Alignment with Core Business Drivers**
- Financial Management
- IT Organizational Governance
- IT Risk Management
- IT Audit and Oversight

A dashboard view of the IT Risk Assessment results is provided below:



IT Risk Component	Risk Level	Direction of Risk
Alignment with Core Business Drivers	Medium	Stable

The organization has defined an IT strategy for the support of business initiatives that meets performance expectations. Areas for consideration include:

- Vision & Roadmap
- Business Drivers
- Readiness Planning
- Business Enablement
- Policies and Procedures
- Business Relationship Management

Description

Policies are documented, reviewed, and approved on a regular basis for key tasks, such as network security management, acceptable use of company assets, data protection principles, password creation, remote use of enterprise assets, and various other day-to-day actions and operations. However, procedures to facilitate the management of various solutions and execution of policy requirements throughout the IT teams is not consistent.

Audit Considerations

Procedures to consider include:

- Review the appropriateness of the IT Strategic Plan and Performance Reporting
- Assess IT policies and procedures
- Evaluate Collaboration and Knowledge Transfer Tools

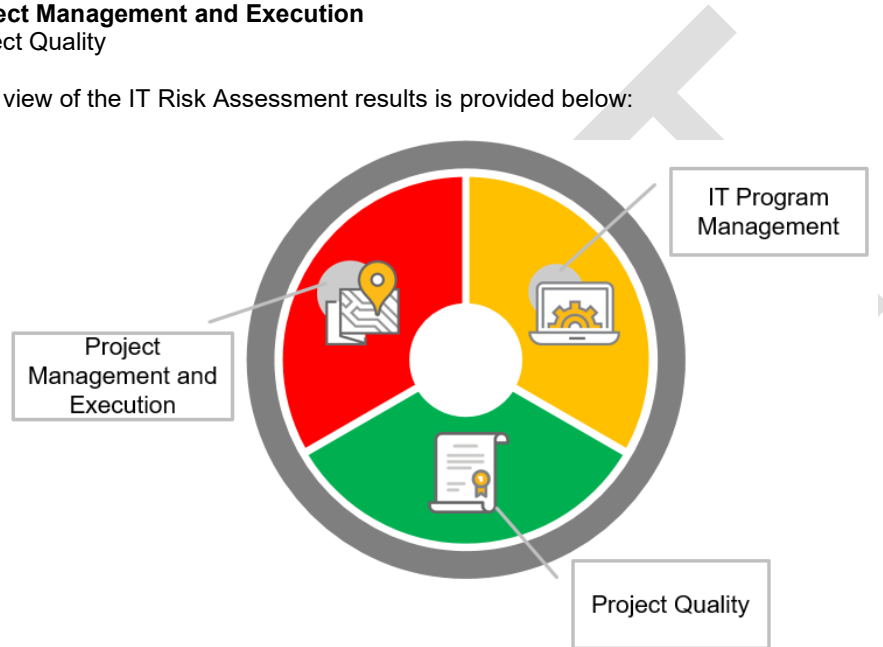
IT Program and Project Management

The IT Program and Project Management domain considers risks associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs. This ties to investment portfolio management.

IT Program and Project Management is segmented into three (3) risk categories:

- IT Program Management
- **Project Management and Execution**
- Project Quality

A dashboard view of the IT Risk Assessment results is provided below:



IT Risk Component	Risk Level	Direction of Risk
Project Management and Execution	High	Increasing

A formal approach for project management has been defined to identify/manage changing project requirements and allocate appropriate resources correspondingly. Areas for consideration include:

- Project Management Guidelines
- Project Tracking Documentation

Description

ABC utilizes a distributed model to support Project Management for IT initiatives. While there are management tools, there are no centralized standards or programs on expectations for these distributed teams to use these tools, leading to inconsistency in execution.

Audit Considerations

Procedures to consider include:

- Evaluation of Project Management Capabilities
- Review of the Project Timelines and Effectiveness

IT Operations and Service Delivery

The IT Operations and Service Delivery domain considers risks associated with the operational stability, availability, protection and recoverability of IT services that can bring destruction or reduction of value to the enterprise.

IT Operations and Service Delivery is segmented into fourteen (14) risk categories:

- Information Security Governance
- Logical Security
- Logging and Monitoring
- Physical Security
- IT Operations
- Data Protection
- Business Continuity Management
- Threat & Vulnerability Management
- Third Party Risk Management
- Employee Management
- Configuration Management
- Change Management
- System Development and Acquisition
- Compliance Management

A dashboard view of the IT Risk Assessment results is provided below:



Controls governing user identification and authentication are adequately designed, documented, and in compliance with applicable regulations and industry standards. Determine if access management and review procedures are appropriate and align with the concepts of principle of least privilege and segregation of duties. Areas for consideration include:

- User Provisioning
- User Deprovisioning
- Authentication & Password Management
- Authorization & User Access Rights
- Remote Access

Description

All system access, including user provisioning and deprovisioning, is handled via Service Desk and Human Resource processes. The organization operates on the principles of least privilege and a general “need-to-know” basis.

ABC has implemented workflows to ensure that when a user is terminated all network and system access is revoked immediately to ensure that disgruntled former employees cannot access sensitive systems or data. Required minimum password parameters at ABC have documented within a Password Policy, which dictates standards for mainframes, network access, application access, and IT-maintained system passwords (such as service accounts and administrator accounts).

The IT Security team also leverages internally developed applications for the management of privileged credentials throughout the enterprise to ensure that password parameters adhere to the organizational standards and can be easily rotated as needed. Remote access to ABC resources is granted on a case-by-case basis for users and associated groups, and all instances of remote access must be reviewed and approved prior to remote SSLVPN access and other remote access mechanisms being used.

Audit Considerations

Procedures to consider including:

- Access Request / Termination Process Review
- User Access Review
- Remote Access Review
- Password Security Review

ABC, Inc.
Internal Audit Report
IT Risk Assessment
June 2022

3

V. IT Risk and Assessment Coverage Matrix

Audit Area	Audit Objective	Year		
		FY21	FY22	FY23
IT Process Audits				
IT Benefit and Value Enablement				
IT Governance Audit	Assess the organization's IT Governance programs to evaluate: <ul style="list-style-type: none"> • How IT's goals are aligned with and support business objectives • Whether IT is optimizing costs and improving the value of IT • How IT is tracking and monitoring IT risks • That IT assets are being used effectively and efficiently • How IT measures and reports on performance 		X	
IT Program and Project Management				
Project Management Audit	Perform a review of the Project Management Process to determine if a project management framework for IT projects is established and operating effectively.			X
IT Operations and Service Delivery				
Remote Workforce Security Assessment	With recent events related to COVID-19, many organizations had to expedite or create new solutions to support broad access to remote working solutions. These organizations were initially focused on operational challenges to maintain business operations. However, information security controls are a critical component for long term viability to minimize the risk of data breaches and unplanned downtime. The goals of this audit is to review the solutions in place to support remote workers, including remote access solutions, remote administration, and personal use standards.	X		
Logical Access Reviews	Access to computer resources should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of computer programs, and improper use of computer resources. The goal of this audit is to evaluate the process for onboarding employee access, periodic user access reviews, authentication and authorization controls, and user deprovisioning.	X		X
Logging and Monitoring Audit	Logging and monitoring controls are a critical aspect of a cybersecurity program, helping organizations identify potentially malicious activity to improve response time and minimize impacts of a security incident. The goal of the audit is to evaluate the		X	

ABC, Inc.
Internal Audit Report
IT Risk Assessment
June 2022

4

Audit Area	Audit Objective	Year		
		FY21	FY22	FY23
	effectiveness of logging procedures, technology and process controls in place to monitor security logs, and reporting methodologies to management.			
Data Protection Audit	The goal of the Data Protection Audit is to determine whether the organization has implemented adequate policies and procedures to secure personal data at rest and in transit. Areas of coverage include data classification standards, data inventory, data protection controls, data loss prevention controls, and encryption.		X	
Incident Response Audit	The objective of this audit is to provide management with an independent assessment relating to the effectiveness of security incident management governance and operational procedures. Specifically, the audit takes into consideration assurance around: <ul style="list-style-type: none"> • Program design and implementation, from information security management awareness and training, to insurance and third-party due diligence • Tools and technologies, inclusive of software and server and workstation configuration • Reporting best practices, considering the balance of incident details and potentially sensitive information • Lessons learned, ensuring protocols that include input from all stakeholders. 	X		X
Vulnerability Management Audit	Properly planned and implemented threat and vulnerability management programs represent a key element in an organization's Information Technology security program to detect cyber threats and to provide an approach to manage the risks. The objective of the audit is to assess the existence, design and effectiveness of information security controls implemented by the organization to detect, evaluate and remediate IT security-related threats and vulnerabilities. Areas of coverage include malicious code detection, endpoint protection, vulnerability management programs, patch management, and incident response.	X		X
Configuration Management Audit	Configuration management is the process of defining approved information technology, defining acceptable configuration standards, certifying production systems compliance with the standards, and managing the process to request exceptions to the standards. The goal of this audit is to evaluate the adequacy of the configuration management programs within the organization.	X		X
Third Party Oversight Review	Organizations leverage and rely on third-party providers, as well as subservice or "fourth-party" providers, to conduct business activities. These relationships continue to expand and evolve, introducing numerous risks that must be continuously assessed and appropriately managed by the organization to achieve desired		X	

Audit Area	Audit Objective	Year		
		FY21	FY22	FY23
	business outcomes. The goal of this audit is to assess the organization's third-party management program to confirm these risks are properly identified and managed.			
Disaster Recovery Audit	The objective of the audit is to provide reasonable assurance that the management control framework in place to support disaster preparedness for information technology systems is adequate and effective in the event of a disruption. Areas of coverage will include business impact assessment / recovery objectives, system and network resiliency, backup procedures, and recovery procedures.		X	
Asset Management Audit	The objective of the audit is to provide reasonable assurance that the IT asset management procedures are complete and effective. The key components examined during this audit will include: <ul style="list-style-type: none"> • Compliance with industry and contractual standards • Understanding of roles, responsibilities and authorities • Acquisition and tracking of IT assets • Disposal activities 		X	
Technology Audits				
Application Security				
ERP Security Review	Targeted testing of the IT/security controls around the ERP application, including detailed application testing of both the internal and external interfaces, as well as backend databases as applicable. Testing should include penetration testing of the application from both unauthenticated and authenticated perspectives.		X	
Infrastructure Security Review				
Cloud (AWS/Azure) Security Audit	The Cloud security assessment will review documentation and implemented features of the desired cloud platform(s). Administration, networking, data connections and data flows will be identified and compared to vendor and industry best practices. Any recommendations for improvements will be provided for consideration and implementation as deemed necessary.		X	
Network Architecture Review	The objective of the audit is to review the implementation of the network architecture, including the configuration of the identified switches, routers, hubs, and firewalls, to assess their impact on the security of the network. The team will also review any connections with the network, including connections to the Internet and any other third-party vendors.	X		
Windows Security Review	The goal of the audit is to review the current configuration settings for the Windows operating systems and review access policies and controls on the network. The review should include both Windows system as well as the Active Directory	X		X

Audit Area	Audit Objective	Year		
		FY21	FY22	FY23
	environment, evaluating topics such as service management, file system and share permissions, group policy settings, patching, and AD design and trusts.			
Database Security Review	The goal of the audit is to review configuration settings and operational procedures to assess to the database servers' ability to prevent unauthorized individuals from gaining access to the server and data stored within. Procedures to be performed included evaluating patching, authentication and password security, service accounts, stored procedures, and connections to remote servers.		X	
Endpoint Security				
Endpoint Security Review	This goal of this review is to evaluate end user workstations configurations to confirm risks are effectively managed. In addition, the assessment will evaluate whether personnel are adhering to documented policies. This audit will examine a sample of workstations, including laptops, on the internal network, to evaluate patch levels, local user accounts, sensitive data storage, remote administration, and unauthorized hardware and software.		X	
Mobile Device Management Review	The goal of this review is to assess the infrastructure in place to manage, deploy, and maintain mobile devices in the organization. This review will include coverage of policies and procedures, network and server connectivity, and device management and settings.		X	
Penetration Testing				
External Penetration Testing - Technical Testing - Email Social Engineering	Conduct penetration testing on externally accessible systems from the perspective of an outside threat, including email based social engineering.	X	X	X
Internal Penetration Testing	Conduct penetration testing on the internal accessible systems from the perspective of an outside threat.	X		X

Appendix A – Risk Assessment Criteria

The following tables provide criteria for the assessment team’s rating of Impact, Likelihood, Velocity, and Control Effectiveness.

Impact Area	Impact Rating			
	Lower Risk <-----> Higher Risk			
	1- Low	2 - Moderate	3 - High	4 - Critical
Financial Operations	Loss of less than \$10,000 in revenue lost	Loss of revenue between \$10K - \$100K	Loss of revenue between \$100K - \$250K	Greater than \$250K revenue loss
Confidentiality	No disclosure of confidential records	Disclosure of below 500 confidential records	Disclosure of between 500 to 5,000 confidential records	Disclosure of 5,000 or more confidential records
Integrity	No additional access to production systems or resources	Unauthorized access to business systems	Unauthorized access with ability to modify sensitive data	Unauthorized remote or privileged access breach
Operations	Little to no operational impacts	Localized (single department) disruption to service levels or business activities No impact to critical processes	Multi-department disruption to service levels or business activities Minor impact to critical processes	Significant enterprise-wide disruption to service levels or business activities, and or critical processes
Reputation	Unlikely to generate more than limited short-term local media attention Limited effect on reputation/ image	Likely to generate negative media attention in major outlets or that is longer than short-term Moderate damage to reputation/image	Potential long-term negative media attention at national or international outlets High damage to reputation/image	Significant long-term negative media attention at national or international outlets Significant damage to reputation/image
Strategic	Little or no impact on strategies, objectives, or scope	Moderate impact on strategies, objectives, or scope such that one (or more) of the outcomes will fall short of expectations	Significant impact on strategies, objectives, or scope such that <u>one</u> of the outcomes will not be achieved	Significant impact on strategies, objectives, or scope to such that <u>multiple</u> outcomes will not be achieved

Likelihood			
Lower Risk <-----		-----> Higher Risk	
1-Slight	2-Likely	3-Certain	4-Imminent
Remotely likely and has a slight probability to occur in 2 to 3 years.	Possible and is likely to occur in 1 to 2 years.	Probable and is certain to occur within one year.	The event is ongoing or certain to occur within three months.

Velocity			
Lower Risk <-----		-----> Higher Risk	
1-Low	2-Moderate	3-High	4-Critical
Risk impact will be felt more than one year after occurrence. There will be enough time for reaction, response, mitigation and/or corrective actions to take place before the impact.	Risk impact will be felt between 6-12 months after occurrence. There will be time for reaction and response planning before the impact.	Risk impact will be felt in 3 to 6 months after occurrence. There will be limited time for reaction and response planning before the impact.	Risk impact will be felt immediately to less than 3 months after occurrence. There will be very little or no time for reaction and response planning before the impact.

Control Effectiveness			
Lower Risk <-----		-----> Higher Risk	
1-Highly Effective	2-Moderately Effective	3-Low Effectiveness	4-Ineffective
The control is operating in a manner that completely satisfies the control objective, significantly mitigating the likelihood or impact of the risk.	The control has been implemented and it is moderately mitigating the likelihood or impact of the risk, but it does not represent the best practice control environment.	The control is operating in a manner that is better than no control, but it is not significantly mitigating the likelihood or impact of the risk.	The control effectiveness is unknown, the control has not been implemented, or the control is not effective.

Appendix B – Risk Assessment Definitions

The below table outlines definitions for common risk assessment terminology used throughout the report:

Term	Definition
Control	Any action taken to manage risks and reduce the Impact and Likelihood of the cause/event occurring
Control Effectiveness	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
Impact	The overall loss expected (financial, regulatory, loss of reputation, etc.) or consequences when a risk event occurs.
Inherent Risk	The amount of risk that exists in the absence of controls.
Likelihood	The possibility that a risk event will occur.
Residual Risk	The amount of risk that remains after controls are applied.
Risk	The possibility that an event will occur and adversely affect the achievement of business objectives.
Risk Assessment	The process of identifying, analyzing, and evaluating organizational risks.
Velocity	The measurement of time until the effect of a realized risk impacts an objective
Threat	Anything that is capable of acting against an asset in a manner that can result in harm.

Appendix D: Exceptions to Agreement for Services

Crowe has reviewed the **Orange County Employees’ Retirement System (“OCERS”) Information Technology Audit & Consulting Services Request for Proposal**. Crowe understands that both OCERS and Crowe reserve the right to negotiate final contract terms upon selection. Should Crowe be selected to engage in negotiations for a final agreement, Crowe requests the opportunity to discuss and negotiate the contractual terms. The below table identifies certain specific provisions of the RFP materials which Crowe will seek to negotiate and modify.

Crowe hereby submits the following clarifications/exceptions. Pursuant to the terms of the RFP materials, Crowe is prepared to negotiate final terms with OCERS and sees no impediment to reaching mutually acceptable terms.

Areas to be negotiated include the following:

Document and Section	Subject/Exception	Exception Reasoning
Agreement for Services 2.4.5. – Conformance to Applicable Requirements	Crowe respectfully requests the deletion of this provision in its entirety.	This provision should not apply to a professional services contract as it may impair independence
Agreement for Services 2.4.8 – Laws and Regulations	Contractor shall keep itself fully informed of and in compliance with all local, state, and federal laws, rules, and regulations in any manner affecting the performance of the Services, including all Cal/OSHA requirements, and shall give all notices required by law. Contractor shall be liable for all violations of such laws and regulations in connection with Services. If Contractor performs any work knowing it to be contrary to such laws, rules, and regulations, Contractor shall be solely responsible for all costs arising therefrom.	Crowe respectfully requests the language be modified to remove a clause that is later addressed in the indemnification provision.
Agreement for Services 2.4.10 – Accounting Records	Contractor shall maintain complete and accurate records with respect to all costs and expenses incurred under this Agreement. All such records shall be clearly identifiable. Contractor shall allow a representative of OCERS during normal business hours to examine, audit, and make transcripts or copies of such records relating solely to costs and expenses incurred and any other documents created pursuant to this Agreement. Contractor shall allow inspection of all work, data, documents, proceedings, and activities related to the Agreement for a period of four (4) years from the date of final payment under this Agreement. Pursuant to California Government Code Section 8546.7, the parties acknowledge that every contract involving the expenditure of public funds in excess of \$10,000 shall be subject to audit, in the same manner , by the California State Auditor. Notwithstanding the foregoing, the Contractor may provide the OCERS summary-level or redacted records and other written materials to protect the confidentiality of the Contractor’s personnel and other clients or customers.	Due to independence requirements, Crowe’s amends this provision to provide invoicing and payment records as well as summary or redacted reports.

Information Technology Audit & Consulting Services
 Orange County Employees Retirement System

<p>Agreement for Services</p> <p>2.4.11 – Business Continuity Plan</p>	<p>Contractor warrants covenants that it has and will maintain throughout the term of this Agreement a written business continuity plan (“BCP”) to enable it to recover and resume the Services provided by it to OCERS within one (1) Business Day in the event of any disruptive event. Contractor further represents and warrants covenants that it has tested its BCP and will continue to conduct sufficient ongoing verification testing for the recovery and resumption of services provided to OCERS and will update its BCP at least annually. Contractor will notify OCERS within thirty (30) days of any material alterations to its BCP that would impair its ability to recover and resume any interrupted Services it provides to OCERS. Upon request by OCERS, Contractor will provide to OCERS a description of its BCP procedures as they relate to the recovery and resumption of the Services accompanied by a written certification that the BCP has undergone review and testing to account for any changes to such Services. Contractor shall promptly notify OCERS of any actual, threatened, or anticipated event that does or may disrupt or impact the Services provided by Contractor and will cooperate fully with OCERS to minimize any such disruption and promptly restore and recover the Services.</p>	<p>Crowe respectfully requests the following revisions to address and comply with professional standards requirements</p>
<p>Agreement for Services</p> <p>2.6 – Indemnification</p>	<p>Crowe will agree to indemnify the OCERS from third party claims only for bodily injuries, tangible property damages and IP infringement, subject to restrictions, to the extent caused by Crowe.</p>	<p>Consistent with accounting industry practice and the purpose of these requested services, Crowe will seek to modify and limit the indemnification provisions in the following manner.</p>
<p>Agreement for Services</p> <p>2.7.3 (A) (II) – All Coverages</p>	<p>Policies may provide coverage which contains deductible or self- insured retentions. Such deductible and/or self-insured retentions shall not be applicable with respect to the coverage provided to the OCERS Indemnitees under such policies. Contractor shall be solely responsible for deductible and/or self-insured retention and OCERS, at its sole discretion, may require Contractor to secure the payment of such deductible or self-insured retentions by a surety bond or an irrevocable and unconditional letter of credit. The insurance policies that contain deductibles or self-insured retentions in excess of \$25,000 per occurrence shall not be acceptable without the prior approval of OCERS.</p>	<p>Crowe seeks to remove a disclosure requirement related to Crowe’s insurance deductibles/self-insured retentions.</p>
<p>Agreement for Services</p> <p>2.7.3 (A) (V) – All Coverages</p>	<p>Insurance required by Section 2.7.2 shall be placed with insurers licensed by the State of California to transact insurance business of the types required herein. Each insurer shall have a current Best Insurance Guide rating of not less than A: VII unless prior approval is secured from OCERS as to the use of such insurer.</p>	<p>Crowe respectfully requests the following revision to align with Crowe’s existing insurance coverage.</p>
<p>Agreement for Services</p> <p>2.9.1 – 2.9.3 – Ownership of Work Product</p>	<p>Crowe seeks to replace provisions 2.9.1 – 2.9.3 with the following language:</p> <p>Except as set forth in the applicable SOW, any deliverables, works, inventions, working papers, or other work product conceived, made or created by Contractor in rendering the Services under this Agreement (“Work</p>	<p>Crowe has ownership rights of all its methodologies, inventions, know-how, and techniques underlying all of the Deliverables. Upon full payment of invoices, OCERS will own its copy of the written Deliverable and</p>

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

	Product”), and all intellectual property rights in such Work Product will be owned exclusively by Contractor. Upon full payment by OCERS, Contractor grants to OCERS a license to use for its business purposes any Deliverables, including any other Work Product incorporated in such Deliverables. Further, Contractor provides the same or similar services to other clients; therefore, OCERS agrees (a) that nothing in this Agreement shall preclude Contractor from developing for itself, having developed, or developing for others, anything that is similar or competitive with the deliverables, irrespective of the similarity to the deliverables, and (b) Contractor retains exclusive ownership or control of all intellectual property rights in any ideas, concepts, methodologies, data, software, designs, utilities, tools, models, techniques, systems, reports, or other know-how that it develops, owns or licenses in connection with this Agreement as well as any enhancements to any of the above, (“Materials”). The foregoing ownership will be without any duty of accounting.	have a perpetual license to use the Work Product incorporated in the Deliverable to the extent necessary to be able to use the Deliverable as set forth in this Agreement.
Agreement for Services 2.9.8 – Non-Infringement	Crowe respectfully requests the deletion of this provision it its entirety.	Crowe can provide an indemnity for IP Infringement.
Agreement for Services 3.3 – Time is of the Essence	Crowe respectfully requests the deletion of this provision it its entirety.	Crowe respectfully requests the deletion of this provision as it is not appropriate for these professional services.
Agreement for Services 3.4 – OCERS’ Right to Employ Other Contractors	Crowe respectfully requests the deletion of this provision it its entirety.	Crowe respectfully requests the deletion of this provision as it is not appropriate for these professional services.
Agreement for Services 3.12 – Injunctive Relief for Breach	Contractor’s obligations under this Agreement are of a unique character that gives them particular value; breach of any of such obligations will may result in irreparable and continuing damage to OCERS for which there will be no adequate remedy at law; and, in the event of such breach, OCERS will be entitled to seek injunctive relief and/or a decree for specific performance, and such other and further relief as may be proper (including monetary damages if appropriate).	Crowe respectfully requests the following revisions to align with current Crowe practices.
Additions:	If Crowe is awarded the RFP, Crowe will respectfully seek the inclusion of the below terms as party of the final Agreement between the parties.	
Addition	Limit of Liability: Except where it is judicially determined that Contractor performed its services with recklessness or willful misconduct, Contractor’s liability will not exceed fees paid by OCERS to Contractor for that portion of the work giving rise to the claimed liability. A claim for a return of fees paid is the exclusive remedy for any damages. This limit of liability will apply to the fullest extent allowed by	In addition to the liability limitation set forth in the agreement, Crowe seeks a reasonable cap on direct damages. These types of clauses permit Crowe to continue to offer the

Information Technology Audit & Consulting Services
Orange County Employees Retirement System

51

	law, regardless of the grounds or nature of any claim asserted, including, without limitation, to claims based on principles of contract, negligence or other tort, fiduciary duty, warranty, indemnity, statute or common law. This limit of liability will also apply after this Agreement.	competitive rate structure which we offer.
Addition	Time Limit on Claims: In no event will any action against Contractor, arising from or relating to this Agreement or the services provided by Contractor relating to this Agreement, be brought after the earlier of 1) one (1) year after the date on which occurred the act or omission alleged to have been the cause of the injury alleged; or 2) the expiration of the applicable statute of limitations or repose.	Crowe believes in finality to any claims and seeks this type of clause in our agreements with clients.
Addition	Response to Legal Process: If Contractor is requested by subpoena, request for information, or other legal process to produce documents or testimony pertaining to OCERS or Contractor's services, and Contractor is not named as a party in the applicable proceeding, then OCERS will reimburse Contractor for its professional time, plus out-of-pocket expenses and reasonable attorney fees that Contractor incurs in responding to the request.	Crowe simply seeks reasonable compensation for any such requirements where Crowe is not a named party to the suit.
Addition	Jury Trial Waiver: As a supplement to the dispute resolution processes already in the agreement, Contractor will seek to include a jury trial waiver for any disputes that may require court involvement.	Crowe believes that such a clause promotes efficiency and cost-effectiveness in the unlikely event of any dispute between the parties.
Addition	Use of Third-Party Service Providers: Contractor may also utilize third-party providers used in the ordinary course of Contractor's business operations, including without limitation, providers such as Microsoft, Rackspace, Crowe Horwath IT Services LLP (a subsidiary owned and controlled by Contractor), information security providers, and other ordinary-course third-party providers.	Crowe wishes to clarify that Crowe may use third-party providers in the ordinary course of its business operations.
Addition	Professional Standards: As a regulated professional services firm, Contractor must follow professional standards when applicable. Thus, if circumstances arise that, in Contractor's professional judgment, prevent it from completing the engagement, Contractor retains the right to take any course of action permitted by professional standards, including declining to express an opinion or issue other work product or terminating the engagement.	This provision is specific to Crowe's industry and sets forth the types of professional standards Crowe must abide by

November 22, 2024

Jim Doezie
Contracts, Risk and Performance Administrator
The Orange County Employees Retirement System
2223 E Wellington Ave., Suite 100
Santa Ana, CA 92701

Submitted via email to jdoezie@ocers.org.

Dear Jim:

We appreciate the time OCERS has spent providing an overview of your organization and responding to submitted questions. The following proposal reflects our understanding of your needs and illustrates the approach we will take in providing professional services for The Orange County Employees Retirement System (OCERS).

Highlights of this approach include the following:

- OCERS will be served by professionals based both locally and nationally across the United States. The mix of local and national resources allows for RSM to bring in the right subject matter experts for the audit areas while providing a local touch.
- To promote efficient service for OCERS, your engagement team's experience reflects our firm's long-standing relationship with OCERS as well as our commitment to serving public employee retirement systems.
- Your team members will coordinate all aspects of the services we perform for OCERS. They will actively share information, as appropriate, to streamline efforts and avoid unnecessary distractions for your personnel.


Your RSM US LLP (RSM) engagement team looks forward to continuing our long-term relationship with OCERS and delivering value for your organization now and well into the future.

Once you have had the opportunity to review this response, we would be pleased to discuss your needs in greater detail or make a presentation to your team. In the meantime, please feel free to contact us with any questions.

Sincerely,



Alfred Ko
Partner, Risk Consulting
+1 213 330 4670



Victor Kao
Partner, Risk Consulting
+1 949 255 6689



Joseph (Joe) Strain
Director, Risk Consulting
+1 267 419 2229

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING



Proposal to provide information technology audit and consulting services

The Orange County Employees
Retirement System

November 22, 2024

Table of contents

Exhibit B..... 1

Exhibit C..... 2

 Affirmations..... 3

 Exceptions for OCERS 4

Executive summary 7

About RSM 19

About your engagement team 24

Client references 27

Licenses 28

Pricing 29

Conflicts of interest 31

Additional information 32

Appendices 34

 Appendix A—Engagement team biographies 34

 Appendix B—Writing samples 44

 Appendix C—About RSM 45

 Appendix D—Culture of Inclusion at RSM 46



Exhibit B

1. The "Minimum Qualifications Certification," attached as Exhibit "B."

Exhibit B MINIMUM QUALIFICATIONS CERTIFICATION

All firms submitting a proposal in response to this RFP are required to sign and return this attachment, along with written evidence of how the respondent meets each qualification.

The undersigned hereby certifies that it fulfills the minimum qualifications outlined below, as well as the requirements contained in the RFP.

Minimum Qualifications include:

1. The auditor should have professional certifications such as CISA, CIA, CISSP, CRISC, or similar.
2. Minimum 7+ years of IT Audit experience: The auditor should have substantial experience in conducting both ITGC and Cybersecurity audits.
3. Experience in conducting risk-based ITGC audits: The auditor should use a risk-based approach in their audit methodology, focusing on areas with higher risks to the organization.
4. Experience conducting risk-based Cybersecurity audits: The auditor should adopt a risk-based approach, focusing on high-risk areas, critical assets, and potential vulnerabilities.
5. Familiarity with recognized security frameworks: The auditor should be proficient in assessing against the NIST Cybersecurity Framework and CIS Controls.
6. Ability to develop control matrices and test plans: Experience in designing and implementing IT control matrices and audit test plans for IT audits.
7. Proven track record in delivering audit reports: Ability to write clear, concise, and actionable audit reports suitable for presentation to senior management and audit committees.

The undersigned hereby certifies that they are an individual authorized to bind the Firm contractually, and said signature authorizes verification of this information.

	11/13/2024
Authorized Signature	Date

Alfred Ko, Partner, Risk Consulting
Name and Title (please print)

RSM US LLP
Name of Firm



Exhibit C

2. The "Proposal Cover Page and Check List," attached as Exhibit "C."

I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements, **except for the exceptions and affirmations noted on the following pages.**

Exhibit C

PROPOSAL COVER PAGE AND CHECK LIST (TO BE SUBMITTED IN FIRM'S LETTERHEAD)

Respondent Name: Alfred Ko
Respondent Signature: *Alfred Ko*
Respondent Address: Los Angeles, California

By submitting this response, the undersigned hereby affirms and represents that they have reviewed the proposal requirements and have submitted a complete and accurate response to the best of their knowledge. By signing below, I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements.

Respondent specifically acknowledges the following:

1. Respondent possesses the required technical expertise and has sufficient capacity to provide the services outlined in the RFP.
2. Respondent has no unresolved questions regarding the RFP and believes that there are no ambiguities in the scope of services.
3. The fee schedule submitted in response to the RFP is for the entire scope of services and no extra charges or expenses will be paid by OCERS.
4. Respondent has completely disclosed to OCERS all facts bearing upon any possible interests, direct or indirect, that Respondent believes any member of OCERS, or other officer, agent, or employee of OCERS presently has, or will have, in this contract, or in the performance thereof, or in any portion of the profits thereunder.
5. Materials contained in the proposal and all correspondence and written questions submitted during the RFP process are subject to disclosure pursuant to the California Public Records Act.
- ~~6. Respondent is not currently under investigation by any state or federal regulatory agency for any reason.~~
7. Except as specifically noted in the proposal, respondent agrees to all of the terms and conditions included in OCERS Services Agreement.
8. The signatory above is authorized to bind the respondent contractually.



Affirmations

The candidate shall provide an affirmative statement that if he/she is selected to serve as a consultant, he/she will be independent of OCERS and not related in any way to OCERS' business operations. The candidate should also provide an affirmative statement that he/she is not currently in litigation with OCERS or any of OCERS plan sponsor agencies.

As a licensed certified public accounting firm, RSM must maintain its independence from its clients. Further, as is customary within the accounting profession and with other professional practices, RSM US does not discuss ongoing litigation. Litigation often involves matters that are bound by confidentiality agreements and orders on which we cannot comment. There are no claims currently in process that are expected to impact our ability to serve our clients.

The Respondent specifically acknowledges that the Respondent is not currently under investigation by any state or federal regulatory agency for any reason.

RSM is a national provider of accounting, tax and consulting services. Like other professional services firms, we engage in matters with legal and regulatory implications as a part of doing business. At any given time, most public accounting firms have ongoing legal activity.

As is customary within the accounting profession and other professional practices, RSM does not disclose information pertaining to legal proceedings. Settlements and regulatory activity often involve matters that are subject to confidentiality agreements and orders that prohibit comment. However, there are no pending or actual claims that could reasonably be expected to impact our ability to serve our clients generally, or to provide the services contemplated by this proposal, specifically.

The candidate shall provide an affirmative statement that he/she has not given a gift or political campaign contribution to any officer, Board member, or employee of OCERS within the past twenty-four (24) months.

RSM has not given a gift or political campaign contribution to any officer, board member, or employee of OCERS within the past twenty-four (24) months.

Exceptions for OCERS

Orange County Employees Retirement System Request for Proposal Exceptions and Clarifications

We ("Contractor") have reviewed the Orange County Employees Retirement System ("OCERS") Request for Proposal ("RFP") for Information Technology Audit & Consulting Services, including Exhibit D Services Agreement Template, which contains the general terms and conditions ("Terms and Conditions") expected to be incorporated into a negotiated contract ("Agreement").

Except as indicated below, we are prepared to accept such Terms and Conditions. If the OCERS selects us based upon our response to the RFP, we would seek to negotiate in good faith modifications, additions, or clarifications of the Terms and Conditions of the Agreement in the areas discussed below and other potential areas, provided that such revisions are consistent with the exceptions noted herein and in accordance with standard industry practices. Given our experience in contracting with OCERS, we are confident that we can reach an agreement with you on these issues. Notwithstanding anything to the contrary contained in the RFP or this response thereto, our obligation to perform any services shall follow the execution by both parties of a mutually agreed upon definitive agreement.

Exhibit D: Services Agreement Template

2.4.10. Accounting Records: We request this provision be modified to state: "...Contractor shall allow a representative of OCERS during normal business hours to examine, audit, and make transcripts or copies of the time, billing and reimbursable expense records for the services performed under the Agreement. Contractor shall allow inspection of the time, billing and reimbursable expense records related to the Agreement for a period of four (4) years from the date of final payment under this Agreement. *All audits and inspections will be performed off-site.*..." This modified language protects the confidentiality of other clients' information and data and ensures our compliance with applicable professional standards. We will cooperate with the California State Auditor and their audits of books and records under this Agreement as needed.

2.4.11. Business Continuity Plan: We request this provision be modified to state: "...to enable it to recover and resume the Services provided by it to OCERS within **seventy-two (72 hours)**..."

- We also request the removal of this language from the provision: "Contractor will notify OCERS within thirty (30) days of any material alterations to its BCP that would impair its ability to recover and resume any interrupted Services it provides to OCERS."
- We also request this provision be modified to state: "...Contractor will provide to OCERS **a summary of its BCP procedures.**"

RSM does not share its full Business Continuity Plan with clients, as our Business Continuity Plan is considered confidential information.

2.6.1. Indemnity by Contractor: We request this provision be modified to state: "...in any manner arising out of, pertaining to, or incident to **any third-party claims based on the negligence or willful misconduct** by Contractor..." Limiting the indemnification to third-party claims was agreed upon in previous agreements between the parties.

We also request the inclusion of the following limitation of liability language: "**The Contractor's total aggregate liability under this Agreement, except for its indemnification obligations under this Section 2.6, shall be limited to an amount equal to the fees Contractor receives under the Agreement, and shall exclude indirect, consequential, exemplary or similar such damages.**" A limit/cap on our liability for each engagement tied to the fees paid for services performed is fair and reasonable and standard in professional services engagements.

2.7.2.(E). Excess Liability: We request the inclusion of the following language: "**The excess or umbrella liability coverage can be combined with, and follows the form of, the Commercial General Liability, Automobile Liability, and Employer's Liability policies.**" RSM's umbrella policy does not provide any coverage for our Professional Liability policy.

- We also request this provision be modified to state: "...Any umbrella or excess coverage for the **Commercial General Liability and Automobile Liability coverage** shall contain or be endorsed to contain..." and "The policy shall be endorsed to **provide** that OCERS Indemnitees shall be covered as additional insured **via a blanket endorsement** when being used for **Commercial General Liability or Automobile Liability coverage.**" Our umbrella policy follows form, and the only policies RSM can

Orange County Employees Retirement System
Request for Proposal
Exceptions and Clarifications

¶ contain... and "The policy shall be endorsed to **provide** that OCERS Indemnitees shall be covered as additional insured **via a blanket endorsement** when being used **for Commercial-General-Liability or Automobile-Liability coverage**. Our umbrella policy follows form, and the only policies RSM can include Additional Insureds and a waiver of subrogation in favor of the client are the Commercial General Liability and Automobile Liability policies. ¶

- → We also request this provision be modified to state: "...The coverage shall be in the amount not less than five million dollars (\$5,000,000) **per occurrence** and aggregate. Our umbrella policy applies on a "per occurrence" basis. ¶

2.7.3.-All-Coverages; No-Contribution: We request this provision be modified to state: "**The Commercial-General-Liability and Automobile-Liability policies** shall include or be endorsed to state that: (1) the OCERS Indemnitees shall be covered as additional insured **via a blanket endorsement** with respect to work by...". The only policies under which RSM can include Additional Insureds are the Commercial General Liability and Automobile Liability policies. ¶

- → (A)(I). We request this provision be modified to state: "**The Commercial-General-Liability and Automobile-Liability policies** shall contain a waiver of transfer rights of recovery ("waiver of subrogation")..." RSM can only provide a waiver of subrogation in favor of the client under its Commercial General Liability and Automobile Liability policies. ¶
- → (A)(IV). We request this provision be modified to state: "**Contractor will provide client with at least thirty (30) days prior written notice of any termination, cancellation or non-renewal of the policies required under this Agreement where such termination, cancellation or non-renewal does not result in equal or great coverage.**" RSM's insurance carriers will not agree to provide notice to any third party. ¶
- → (A)(VI). We request this provision be modified to state: "**Contractor shall also require all its subcontractors to procure and maintain the same insurance for the duration of the Agreement. Such subcontractors shall furnish separate certificates and endorsements evidencing their own insurance.**" RSM's policies do not cover subcontractors. ¶

2.8.1.-Termination: We request the addition of language in this section stating: "**Contractor may terminate this Agreement upon reasonable written notice to the Authority for the Authority's material breach of contract which remains uncured or where continued performance would be contrary to applicable law, rule or regulation.**" This termination right is needed to ensure we comply with applicable professional standards for public accounting firms. ¶

2.9.1.-Ownership of Work Product; Licensing of Intellectual Property: We request this provision be modified to state: "Contractor hereby irrevocably assigns to OCERS, **except for any Pre-Existing IP and/or third-party product incorporated therein or provided for use therewith**, all right, title, and interest..." RSM cannot transfer ownership rights or title to a third-party product incorporated into the Work Product. Further, RSM's Pre-Existing IP consists of our proprietary methodologies, templates, techniques, and know-how. ¶

2.9.3.-License to Preexisting IP: We request this provision be modified to state: "In the event Contractor uses or incorporates Preexisting IP into Work Product, Contractor hereby grants to OCERS a **nontransferable**, worldwide, fully-paid and royalty-free, perpetual license, **without the right to grant sublicenses, to use, copy and modify any Pre-Existing IP incorporated in, or provided for use with, the Work Product solely for use with the Work Product and solely for the purpose of using such materials in OCERS internal business**". The Work Product we provide to you under this Agreement is for your sole use and benefit. This is in accord with the professional standards for the performance of consulting services by licensed CPA firms. ¶

2.9.5.(G).-Customer Data: We request the addition of language in this section stating: "**Notwithstanding the preceding, Contractor shall not be required to destroy information that may be stored in archived electronic back-up files or similar electronic storage systems. Further, OCERS acknowledges that RSM may maintain a copy of any Customer Data necessary to support its work product generated as a result of its engagement for professional services, solely for reference and archival purposes in accordance with all applicable professional standards. Any Customer Data retained will remain subject to the confidentiality obligations of this Agreement and will be destroyed in accordance with Contractor's**

¶

Orange County Employees Retirement System[]
Request for Proposal[]
Exceptions and Clarifications[]

¶
record-retention-policies. Professional standards require us to exercise due care, including documenting the basis for our conclusions and recommendations arising out of our services. ¶

3.6-Assignment-or-Transfer: We would request this provision be modified to state: "**Neither-Party** shall assign, hypothecate, or transfer, either directly or indirectly (including by operation of law), this Agreement or any interest herein without the prior-written consent of **the-other-Party**." RSM is a certified public accounting firm and must consent to the assignment of its professional services agreements in order to avoid independence conflicts. ¶

¶

¶

¶

6



Executive summary

3. An executive summary that provides the respondent’s background, experience, and other qualifications to provide the services included in the Scope of Services.

In recent conversations, you shared with us the qualities OCERS values in a professional services relationship. Based on our understanding of your expectations, we are confident that RSM has the right capabilities, qualifications and client-service culture to serve as your advisor.

To illustrate this alignment, we would like to highlight the following:

Your priorities	Our response	Outcomes
<ul style="list-style-type: none"> Confidence that your professional service needs will be fully supported by a team that knows the challenges facing your organization and can grow as those challenges evolve. 	<ul style="list-style-type: none"> Our team has successfully served OCERS’s IT internal audit needs since 2019 and Sage Intacct implementation needs since 2021. We bring significant experience in providing professional services to organizations like OCERS, so we understand what you need now and into the future. 	<ul style="list-style-type: none"> OCERS will be well served by professionals who deeply understand your IT and information security environment, allowing us to anticipate potential issues. We will leverage our experience with our nationwide resources to deliver the service levels your organization deserves.
<ul style="list-style-type: none"> Working with a provider who can get to work without a learning curve, while offering fresh perspectives on the best approaches. 	<ul style="list-style-type: none"> The RSM team we propose will provide continuity in IT internal audit coverage and will not require a transition period or disruptions to your staff to begin delivering meaningful work products. Our team includes members with previous OCERS experience as well as new members to offer a diverse set of viewpoints while effectively continuing with our institutional knowledge for the most efficient approach. 	<ul style="list-style-type: none"> OCERS will benefit from working with an experienced internal audit team with a deep understanding of your audit committee’s unique expectations, while receiving fresh perspectives that help ensure comprehensive attention to what’s possible.



Your priorities	Our response	Outcomes
<ul style="list-style-type: none"> Excellent client service based on communication and responsiveness. 	<ul style="list-style-type: none"> Facilitate open and ongoing dialogue to address your questions and concerns, learn about changes in OCERS’s business and support your continual improvement. 	<ul style="list-style-type: none"> Year-round access to a trusted advisor—throughout the engagement and during the year whenever you need us, while committing to flexibility and least disruption when delivering value-added internal audits.
<ul style="list-style-type: none"> A firm with expertise in auditing governmental organizations, including public employee retirement systems. 	<ul style="list-style-type: none"> The public sector is a strategic industry for RSM, with more than 2,500 public sector clients nationally, including more than 500 state and local governmental entities, and public employee retirement systems with assets ranging between \$50 million to greater than \$50 billion. 	<ul style="list-style-type: none"> Bespoke internal audit experience with a trusted business advisor who truly understands public employee retirement systems and pension administration systems. We have a proven history of helping our clients in evaluating the impact of cybersecurity standards and events, new GASB standards, and potential legislative/regulatory changes that impact the system’s operating environment.
<ul style="list-style-type: none"> Competitive fees and consistently high-quality results. 	<ul style="list-style-type: none"> Leverage highly experienced professionals to plan the engagement and direct and oversee all work phases. 	<ul style="list-style-type: none"> On-time delivery of services, results that fully align with your expectations and fees that reflect an optimized staffing approach.



Focused on organizations like OCERS

OCERS needs to work with a respected national firm that you will not outgrow. You also deserve a professional services firm that is committed to providing you with an experienced, knowledgeable engagement team.

Ranked as the nation’s fifth largest accounting firm, we understand that day-to-day partner interaction and a core client service team will be paramount to success. We are large enough to provide you with the level of expertise you have come to expect, but small enough that you receive the level of partner attention that an entity like OCERS deserves.

Public employee retirement systems are being challenged by a broader range of constituencies to deliver more transparency, efficiency and accountability than ever before. Funding shortfalls, investment risks, and regulatory and legislative changes present constant challenges that public employee retirement systems must navigate. Leaders are under considerable pressure to help ensure that retirement systems function like an efficient financial business—delivering quality member experiences, implementing efficient processes and demonstrating prudent financial stewardship. At the same time, in the face of ever-changing economic and political conditions, public employee retirement systems must function productively and show results, all while focused on achieving a higher mission: to preserve public confidence in the system.

Internal auditors are a critical—and, at times, misunderstood—piece of the public employee retirement puzzle. High quality internal audits play a crucial role in ensuring the financial health, compliance, and operational efficiency of retirement systems. Quality studies from a variety of sources suggest that experience drives quality. At RSM, we have individuals who dedicate their time to public employee retirement system, with an emphasized focus on retirement systems with assets ranging between \$50 million to greater than \$50 billion. To demonstrate our experience and focus, we are proud to have a current working relationship with the following systems and funds:

Public ERS		
Indiana Public Retirement System	School Employees’ Retirement System of Ohio	Cook County Pension Fund—Forest Preserve
Illinois Municipal Retirement Fund	Cook County Pension Fund – County Employees	General Assembly Retirement System of Illinois
State Universities Retirement System of Illinois	Maryland Teachers’ and State Employees’ Supplemental Retirement Plans	Utah Retirement Systems
State Employees’ Retirement System of Illinois	Judges’ Retirement System of Illinois	State of Hawaii Employees’ Retirement System
Ohio Police & Fire Pension Fund*	Indiana State Police Pension Trust	
Orange County Employees Retirement System	Regional Transportation Authority Pension Plan of Northeastern Illinois	



OCERS deserves to work with a service provider that can help you address challenges and anticipate future changes. Leveraging the experience and perspectives of our public sector professionals—RSM can assist OCERS in a variety of meaningful ways.

Giving you attentive, yet flexible year-round service

OCERS will be served by leaders based in our Orange County and Los Angeles offices, augmented with national resources that possess state and local government employee retirement systems experience—positioning this engagement team to truly understand your business plans, operating challenges and day-to-day activities.



We are committed to a dedicated yet flexible service delivery approach, not only during fieldwork, but throughout the year. We pride ourselves in being a service provider that is easy to work with. When it comes to IT internal audit ideas, operational improvement recommendations, updates related to new cybersecurity guidance, you will learn about a range of ideas gathered from our experience as the largest U.S. provider of assurance, tax, and consulting services focused on the middle market. As it relates to public employee retirement systems, this focus includes plans with assets ranging from \$50 million to over \$50 billion.

In working with us, OCERS will have access to advisors who understand the specific aspects of your business and are committed to effectively serving your needs.

Continuing our longstanding relationship

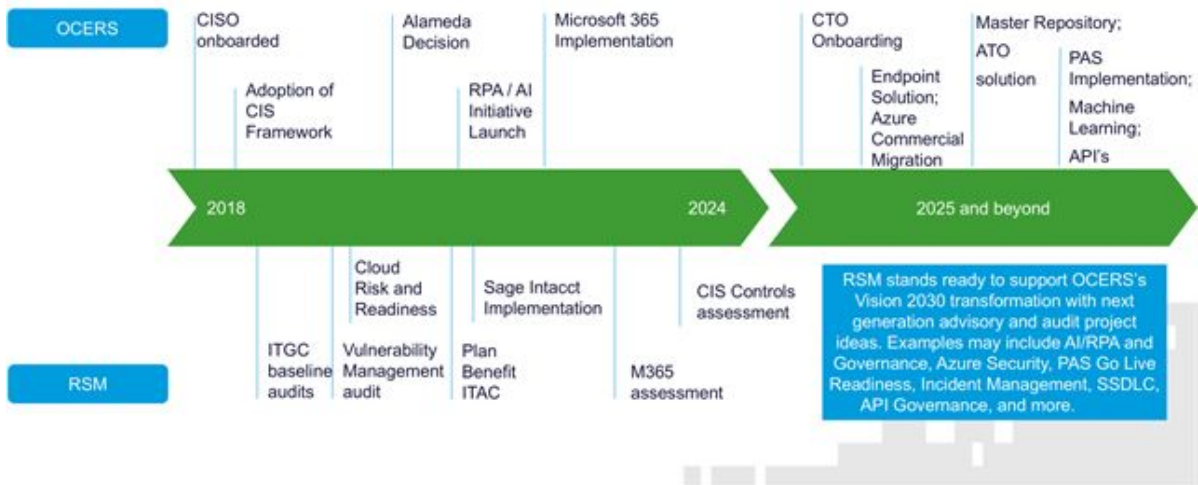
We look forward to continuing the relationship we have built with OCERS, using the knowledge we have gained of your history and business. This continuation will allow your personnel to avoid the distractions of a transition and benefit from a provider that hits the ground running.

RSM has been a trusted partner with OCERS since 2019. Over the past more than five years, we've taken to heart the role of being OCERS's first-choice advisor. We followed the organization closely through its transformational changes, and proudly assisted in the audit committee's risk oversight through the following IT internal audit and compliance projects: annual Internal IT Audit Risk Assessments, Limited Access Death Master File attestations, and internal audits over a wide array of IT and cybersecurity topics including IT general controls, cloud risk and readiness, vulnerability management, Microsoft 365, and CIS Top 18 controls. We have compiled the diagram below to demonstrate our history together and our steadfast commitment to assisting the organization reduce risk as it transforms its digital landscape:





OCERS's Digital Journey with RSM



In addition to IT and cybersecurity audits, we've had the honor to serve OCERS in various financial and business process related projects, including the successful implementation of Sage Intacct—OCERS's financial application, a securities lending audit, and a plan benefit IT automated controls audit that validated the accuracy of OCERS's pension administration system and related design specifications over the final average salary calculation. Our understanding of your business and your financial and pension administration processes lays a strong foundation for a continued successful relationship.

As OCERS continues to embark on its strategic roadmap, RSM stands ready to continue as OCERS's trusted partner in cultivating compliance and risk management functions, and supporting the organization's unwavering dedication to Vision 2030. We pledge to continue innovating in the internal audit ideas that we present to OCERS, including next generation advisory and audit ideas that address artificial intelligence and robotic process automation, Azure Commercial cloud security, secure software development lifecycle, API governance, new pension administration system go-live readiness, and more.

Internal audit qualifications

RSM's qualified team of internal audit advisors is well equipped to develop and execute an effective internal audit strategy to address OCERS's specific risk challenges and enhance business performance. Through decades of successful internal audit experience, our advisors understand your business needs and objectives, and take a holistic perspective to address your immediate and underlying concerns. Our people, depth of resources, differentiated methodology and experience in your industry combine to provide thorough and effective approaches for your internal audit needs.

We provide a complete range of internal audit solutions to companies across various industries, from initial startup functions to outsourcing the entire internal audit function for multibillion-dollar multinational organizations. Our internal audit services contribute directly to the efficient functioning of companies with a wide variety of business structures, including privately owned businesses, private equity groups and state and local governments. Therefore, we understand the risk drivers and business demands of a myriad of different organizations and have the tools and experience to address your specific needs.

RSM continually invests in technical training for our internal audit and risk advisory practitioners, helping to ensure that they are applying leading practices, emerging technological advancements and internal controls process improvements to internal audit engagements. In addition, we also make ongoing investments in refining our methodologies and introducing innovative process enablers, such as our proprietary RSM Risk Monitor audit management platform.

In addition, RSM maintains partnerships with various governance, risk, and compliance (GRC) solutions to enable clients to bring their internal audit and risk management processes into a single cloud-based platform. An example of this is RSM's gold-level strategic partnership of AuditBoard, where RSM helps clients assess, install, maintain, and optimize the performance of AuditBoard's six products. We are well positioned to serve OCERS with sophisticated GRC partnership and solutions when it's the appropriate time for the organization.

Why RSM?

RSM will provide the hands-on service that has driven our firm's growth. We provide internal audit, assurance services, IT consulting, and tax services to numerous clients similar to OCERS and have assembled a team with significant capabilities. Our approach is focused to help ensure that controls are optimized for a highly efficient compliance effort, including enhancing reliance on the testing by independent auditors where possible. As OCERS has experienced in its relationship with RSM, we are committed to the following:

- **Proactive insights.** Our proposed team knows your industry, as well as regulatory hot buttons, and can, therefore, be able to guide you through the audit of controls proactively rather than in a reactive manner.
- **Focus and attention.** OCERS fits squarely in our focus and will be an important client for our firm. We will strive to exceed your client service expectations.
- **Value.** We believe that our approach and fee estimate combine to enhance quality and effectiveness at a reasonable price point.
- **Informed perspective.** Several members of our proposed team not only provide internal audit and controls services on behalf of their clients. This affords them the perspective to understand what the auditors need to be able to maximize their reliance on our work and helps us provide actionable advice regarding design of controls, acceptable levels of documentation, etc.

Scope of engagement

As described on the following pages, RSM has the resources and capabilities to assist OCERS with your needs in the areas you have identified:

- IT general controls (ITGC)
 - Developing and building audit policies and procedures
 - Developing risk controls matrix (RCM) based on applicable control criteria/frameworks
 - Understanding risk in key audit areas such as governance, identity and access management, data protection, data privacy, threat intelligence, vulnerability management, network security, endpoint security, application security, cloud security, incident response, security operations, third-party risk management
 - Use the risk assessment and industry trends to determine what risk areas should be audited
- Cybersecurity
 - A current Curriculum Vitae of the lead consultant(s) must be included in the proposal.
 - 2. The candidate shall submit writing samples for review that demonstrate the candidate's ability to create an adequate IT risk assessment, IT audit plan, and cybersecurity audit plan.
 - 3. The candidate shall provide as much information as possible about past experience as an IT Auditor/Consultant with direct experience relevant to the scope of work identified
- Internal audit IT risk assessment/Audit program
 - Conducting interviews with key stakeholders to understand risk in various domains and assist Internal Audit with their audit plan.

Specifically, as OCERS's current IT internal audit provider, we propose that the organization consider one of the following IT and cyber audits in 2025:

1. Ransomware assessment

Ransomware remains one of the most pertinent threats for organizations across all industry verticals. As such, it is best practice for organizations to assess controls that are in place to prevent, detect, and respond to a ransomware attack. This internal audit is designed to assess the current operational state of OCERS's ransomware identification, containment, and eradication capabilities.

We will use the following approach to perform this assessment:

- Evaluate the risk of an infection:

This phase is performed to determine the overall risk of your organization becoming a victim of a ransomware attack. During this phase, we will leverage the penetration testing and social engineering results performed by OCERS to determine potential threats. Further, we will perform a design-level controls analysis to evaluate the ease with which ransomware may be able to enter your organization through sophisticated social engineering attacks, and the controls in place at the endpoint to prevent and detect the execution of this type of malware.

Some controls reviewed during this phase included:

- Cyber threat intelligence
- Spam filtering
- Email filtering
- Endpoint security review
- Device deployment and hardening practices

- Endpoint detection and response practices
 - Employee social engineering testing and associated tools
 - Assessment of key risk indicators for security awareness programs
 - Data backup procedures
 - System information and event management (SIEM) capabilities
- Evaluate the spread of infection:

This phase will be based on the assumption that an attacker is able to successfully implement ransomware on a target endpoint. The objective is to determine the overall impact of such a scenario. During this phase, we will evaluate the most common ways that sensitive data was stored within your organization, as well as how end users access network share drives and what permissions are defined. This phase also evaluates your overall vulnerability and patch management posture, with a specific focus on ransomware. Ransomware often uses unpatched systems as a means of lateral movement across environments.

- Evaluate business continuity and incident management programs:

This phase will evaluate business continuity and incident response plans, policies and other relevant documentation to determine your ability to recover and respond to a successful ransomware attack. As part of this phase, we will evaluate your backup strategy and associated technology, restoration procedures and incident response policies and procedures. It should be noted that this review focused specifically on controls related to ransomware as opposed to other types of incidents/disasters.

2. Third party risk management audit

The engagement objective is to provide third-party risk management (TPRM) audit services. Over the past 6 years, OCERS's third-party arrangements have evolved to include a number of critical vendors, including vendors such as Cylance, Rapid7, Microsoft Azure, who all possess critical access to OCERS's data. This transformation highlights the important of TPRM in the safeguarding of OCERS against risks associated with third-party relationships.

RSM will review existing document inputs, including, but not limited to:

- Vendor inventory
- TPRM policies
- TPRM procedures and/or operating guides
- Vendor risk criteria
- A sampling of vendor contracts
- A sampling of completed vendor due diligence questionnaires and/or risk assessments, including supporting evidence

The audit will focus on the current state of OCERS' TPRM program and will employ the TPRM target operating model:

TPRM Target Operating Model	TPRM activities	Illustrative control objective
Oversight, accountability and reporting	Program governance and oversight	TPRM activities are reported to and reviewed by the board or an authorized committee of the board at least annually. Vendor incidents and issues identified in a regulatory or external exam/audit are communicated to management and monitored through resolution.
	Program policy and procedures	Policies have been established to provide for the overall direction of TPRM, including the governance model, TPRM program ownership, risk management steps, reporting and alignment across multiple groups involved in the onboarding and monitoring of vendor relationships.
	Documentation and reporting	Standardized use of technology should be used across business units to effectively execute third-party risk activities throughout TRPM life cycle and provide objective reporting on the onboarding, risk ranking, monitoring and termination of vendor relationships.
Planning	Business need assessment	Management should gain an understanding of the needs and business objectives that require the use of a third party and have criteria in place to evaluate the population for qualified parties. A process should be in place to create requests for proposals or quotations with assigned levels of approval based on the determined risk to OCERS' operations.
	Risk assessment	Establish a process to rank third-party service providers based on the data classification, regulatory requirements, financial risk and operational criticality to client. Critical outsourced or vendor-supported applications have been identified based on upstream and downstream critically dependent processes/connections.



TPRM Target Operating Model	TPRM activities	Illustrative control objective
Due diligence	Screening and risk rating	Management should conduct appropriate due diligence in selecting and sourcing third-party service providers. Management should be responsible for ensuring that third parties can meet minimum information security controls and checks are performed, per policy, prior to signing a vendor contract.
Contracting (with a focus on risk management)	Contracting management and negotiation	Client should use well-constructed contracts, developed with legal counsel, to mitigate its risks from third parties. Contracts should be appropriate for Client's specific technology and should clearly identify each party's roles and responsibilities.
Monitoring	Ongoing risk monitoring	Management has a process to evaluate and review high-risk technology service providers on a periodic basis for financial stability, information security, regulatory changes, issue management (including customer complaints), IT operations, business continuity and disaster recovery System and Organization Controls (SOC) 1 or SOC 2 user controls review and service-level agreements.
	Incident response	Incident management security policies assign ownership with regard to outsourced third-party service providers. Furthermore, policies provide guidelines for classifying events, tracking, escalating and documenting management responses and post-incident analysis of vendor incidents.
	Business continuity management	Vendor risk management is appropriately integrated into business continuity management approaches and plans. Management has a strategy in place for managing business interruptions where Client relies on a single partner for services, should the vendor fail to deliver.



TPRM Target Operating Model	TPRM activities	Illustrative control objective
Termination	Offboarding and removal of access	A vendor termination process has been established to ensure that vendor offboarding tasks are performed consistently to validate data and equipment collection/destruction, billing closure, portfolio tracking/provider replacement, removal of access, remote connections and decommissioning standards were met for any shared company data.

RSM will use a sampling methodology to test the effectiveness of contracting and due diligence controls.

Future proof internal audit

As OCERS continues its digital transformation journey, we are well equipped to provide OCERS with sophisticated internal audits over emerging risk areas. To demonstrate our capabilities over nascent risks, we have included a collection of potential internal audit areas and ideas for OCERS's future consideration in 2026 and beyond:

RSM AI Service Catalog



Our SecSDLC Services

Secure Software Development Advisory

Gap and Maturity Assessments: Ensuring your software development processes adhere to industry recognized frameworks like NIST SSDF and OWASP SAMM.

NIST SSDF Custom-Built Maturity Scale: Utilizing a proprietary maturity scale to assess and enhance your software development practices.

Language-Specific Best Practices: Advising on best practices tailored to the specific programming languages used in your projects.



DevSecOps Advisory

Integrated Security: Embedding security practices into your DevOps processes to ensure continuous, automated security across the development lifecycle.

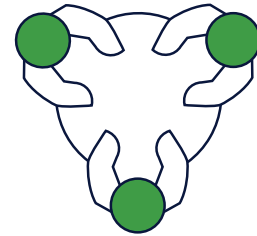
Best Practices & Compliance: Advising on the best practices for secure software delivery and ensuring compliance with industry standards.



Client service relationship

Our relationship with OCERS will be based on certain long-standing principles, including:

- An outstanding client service experience, focused on efficient and well-coordinated services
- Commitment to completing work within the agreed-upon time frame, assuming your preparation of requested schedules and other supporting documentation before we commence fieldwork and assuming no unforeseen technical issues
- Staffing of the engagement team based on industry-specific qualifications and technical experience
- Hands-on approach to planning, with management meetings and conference calls held routinely to discuss changes to the business, industry issues, new accounting pronouncements, etc.
- Fees that are reasonable based on the scope of work
- Transparent approach to billing, with clear communication and an emphasis on avoiding surprises



About RSM

4. A description of the respondent including:

a. Brief history, including year the respondent firm was formed.

Our founder Ira B. McGladrey had a vision to build a great accounting firm with a solid foundation of client service. RSM traces its history to 1926 when the I.B. McGladrey Company was established through the purchase of a seven-person office in Cedar Rapids, Iowa, and a one-man practice in Davenport, Iowa.

Over the years, McGladrey grew his firm both organically and by acquiring firms like his own—with down-to-earth attitudes and roots in the community. We continued this trend of joining forces with like-minded firms to become the fifth largest provider of assurance, tax and consulting services in the U.S. and the leading firm focused on the middle market. The principles on which McGladrey founded his firm are the foundation of RSM's past success and our future strategy.

b. Ownership structure.

RSM is a limited liability partnership and is well capitalized with significant partner and principal investment by its 1,150 partners and principals. All partners and principals are individuals, and no one partner, or principal has more than 1% of the total capital investment in the firm. RSM is not government owned.

c. Office locations.

RSM has office locations in 79 U.S. cities, including five offices in California. RSM also has six locations in Canada, one in El Salvador and four in India. It is a licensed CPA firm and the U.S. member of RSM International, a global network of independent assurance, tax and consulting firms with 64,000 people in 120 countries.

Our Irvine office is located only 15 minutes' drive from the OCERS headquarter, allowing for our leadership team to meet with OCERS management in person.

Our Irvine office has been recognized by the [Orange County Business Journal for 2023 Companies That Care](#) and [2023 Embracing Diversity, Equity & Inclusion Champion](#)

Community:

At the core of RSM's values is stewardship, and we are dedicated to giving back to the communities where we live and work. RSM provides numerous opportunities for our employees to actively engage in community initiatives.

On November 16, 2023, a check for more than \$4.7 million was presented to the Davis Love Foundation from RSM's employee-led [Power of Love](#) program, bringing the grand total raised to date through the tournament to \$41,185,590.

Throughout 2023, Orange County employees participated in the Power of Love program through financial and time donations, with the following results:

19

281



Local charities supported:

- Olive Crest
- Big Brothers Big Sisters of Orange County
- Total employee participation (financial and volunteering): 180 participants out of 213 total employees
- Total volunteer hours: 317.5 hours, including partners and interns

2023 dollars donated within Orange County:

- \$31,850 total dollars donated
- \$3,900 Dollars for Doers grant from the RSM US Foundation for local volunteer hours
- A match of \$20,000 by the RSM US Foundation is expected by year-end 2023

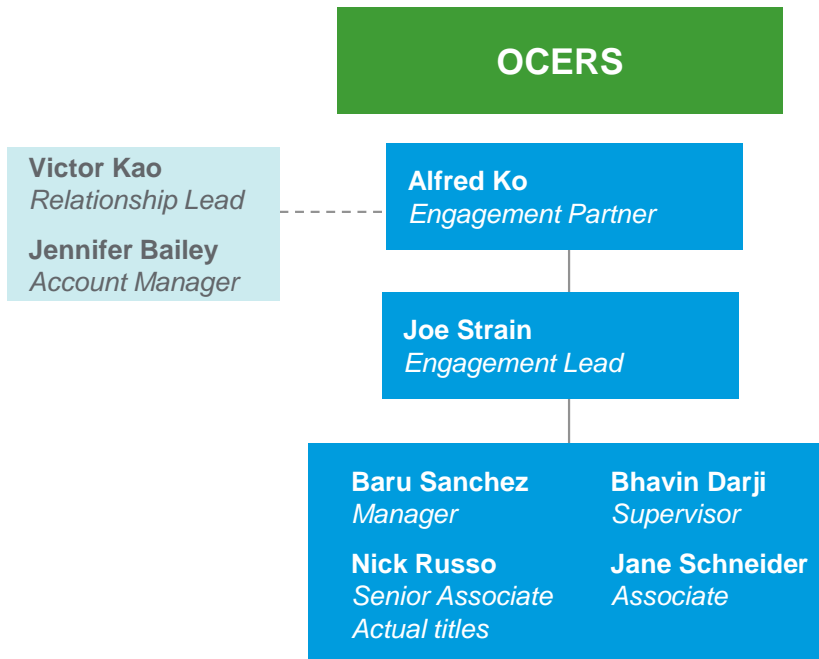
Tommy Bahama Golf Tournament (June 2023):

- \$3,044.85 in-kind donations of RSM promotional items
- \$1,036 of supplies were donated in support of RSM volunteer activities.

RSM played a key role in sponsoring the 2023 Tommy Bahama Golf Tournament, which raised funds for Olive Crest children and families. The Orange County RSM team actively participates by setting up spaces for Olive Crest's holiday parties and assisting in the organization and distribution of gifts to the children and families.

d. Organization chart

The following organizational chart specifically represents the engagement team that will serve OCERS.



e. Number of employees.

RSM is the leading provider of assurance, tax and consulting services focused on the middle market, with more than 17,000 professionals in the U.S. and 64,000 people globally.

f. Annual revenues.

RSM's total revenues for the fiscal year ended April 30, 2024, were \$4.0 billion.

g. Scope of services offered.

The table below highlights the depth of our service offerings in assurance, tax and consulting.

Assurance services	Tax services
<ul style="list-style-type: none"> • Financial statement audits • Employee benefit plan audits • Service organization control reporting • Reviews and compilations • Current accounting and reporting developments advisory services • Global statutory assurance services 	<ul style="list-style-type: none"> • Accounting methods and periods • Compensation and benefits • Credit and incentives • Indirect tax • International tax • State and local tax • Tax compliance • Tax controversy • Tax outsourcing services • Tax services for exempt organizations • Tax technology consulting • Transfer pricing • Washington National Tax
Consulting services	
<p>Business applications</p> <ul style="list-style-type: none"> • Association management systems • Blockchain and digital asset • Customer relationship management • E-commerce • Enterprise resource planning • Managed application services • Strategic technology alliances • iMIS by Advanced Solutions International 	<p>Data and digital</p> <ul style="list-style-type: none"> • Application development and integration • Automation and automation solutions • Corporate performance management • Data analytics solutions • Oracle PBCS • Lease accounting technology • Professional services automation
<p>Financial consulting</p> <ul style="list-style-type: none"> • Actuarial • ASC 842 compliance • Finance and accounting outsourcing 	<p>Management consulting</p> <ul style="list-style-type: none"> • Chief financial officer advisory • Change enablement advisory • Chief information officer services • Digital marketing

<ul style="list-style-type: none"> • Financial investigations and dispute advisory • Financial institution advisory • Lease accounting • Restructuring and bankruptcy • Technical accounting • Valuation services 	<ul style="list-style-type: none"> • Enterprise strategy • Environmental, social and governance • Government contracting strategy and regulatory advisory • Human capital • Mergers and acquisitions advisory • Operational excellence and resilience • Supply chain
<p>Managed IT Cloud and infrastructure</p> <ul style="list-style-type: none"> • Cloud solutions • IT infrastructure • Managed IT • RSM Hyperbox 	<p>Risk consulting</p> <ul style="list-style-type: none"> • ERP risk and automation • Process risk controls • Regulatory risk • Cyber compliance • Cyber testing and response • Cyber transformation • Cyber strategy • Internal audit and controls • AML and regulatory compliance • Technology risk and security transformation • Risk management process automation • Sarbanes-Oxley compliance • System and organization controls solutions
<p>Transaction advisory services</p> <ul style="list-style-type: none"> • Financial Due diligence • Buy-side/Sell-side due diligence • M&A integration planning and execution • Divestitures and carve-outs 	

h. Respondent's specialties, strengths, and limitations.

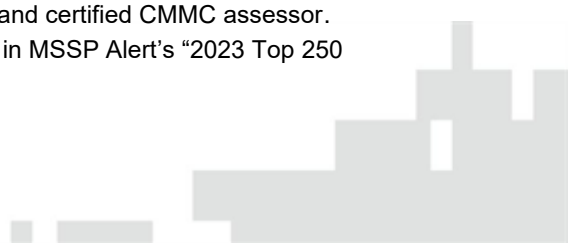
Our firm's overview:

- RSM is the fifth-largest audit, tax and consulting firm in the United States.
- RSM's internal audit practice serves over 2,500 clients across the United States through various resource models that range from fully outsourced to co-sourced, to staff augmentation to project-based internal audits.
- RSM is one of the largest Microsoft Gold Partners in the United States.
- RSM has been named five times as Sage Intacct Partner Award Winner, with 10 North American offices and 25 trained Sage Intacct consultants
- RSM is #1 on Bob Scott's Top 100 VARs (value added resellers) list for nine consecutive years.

Relevant technical experience

OCERS will have direct and seamless access to RSM professionals. Along with the ability to coordinate with regional and national subject matter resources, as needed, to bring you the depth of expertise you need to meet your strategic and operational risk management objectives. In particular, our Cyber Insights include:

- RSM has a team of over 270 certified cyber professionals with a global footprint across the United States, India and El Salvador.
- Seat on the PCI Council's Global Executive Assessor Roundtable and certified CMMC assessor.
- RSM Defense named top 100 managed security services provider in MSSP Alert's "2023 Top 250 MSSPs" report.



- Partner with over 20 leading cyber vendors including Okta, Tenable, AWS, SentinelOne, and Microsoft.
- Perform over 500 risk and control assessments annually across various leading frameworks.
- Our Security, Privacy and Risk Consulting team has over 150 AWS certified employees.
- Over 500 advisors involved in the Institute of Internal Auditors (IIA).

Being the right size. Ranked as the nation’s fifth largest accounting firm, we understand that day-to-day partner interaction and a core client service team will be paramount to success. We are large enough to provide you with the level of expertise you have come to expect, but small enough that you receive the level of partner attention that an entity like OCERS deserves.

Demonstrated service to the public sector. At a time when many of our peer firms are scaling back or walking away from the public sector, RSM is making a significant investment to grow this segment of our practice. RSM serves more than 2,500 public sector entities. We create meaningful value for our clients through better advice, more efficient and cost-effective audit processes and real insight into large government organizations.

High caliber of professionals. As the fifth largest accounting, tax and business consulting firm in the nation—the largest outside of the Big Four, RSM maintains highly skilled and experienced staff of professionals. These professionals are accustomed to operating under the highest professional standards with respect to audit methodology, quality control and independence. This typically distinguishes RSM from our competitors, who may not have the same caliber of professional staff, offer the breadth and depth of training or adhere to the high-quality audit standards that make up the very foundation of our organization

The right team to serve YOU

We are committed to providing OCERS with a **core delivery team** that balances the benefits and efficiencies of **audit**, while also introducing **diversity of thought, perspective, and expertise** through the additional of dedicated professions who have the skills and capabilities to elevate our delivery team to be the **best internal audit partner for OCERS.**



About your engagement team

5. The names and qualifications of the staff that will be assigned to OCERS work, including a detailed profile of each person’s background and relevant individual experience.

We are committed to serving OCERS and its needs fully. With a mix of senior-level professionals, our proposed engagement team will address your unique internal audit challenges through effective, transparent communication with your team. Our partners and directors have an average of 20 years of internal audit experience and maintain ongoing training standards to enhance their qualifications to deliver an efficient and thorough internal audit.

Your engagement team will be led by Alfred Ko and Victor Kao, relationship lead, who will serve as your single point of contact throughout the engagement. They will serve as your primary contacts on day-to-day matters, keep you informed about our progress and promptly address your questions and concerns. With over 16 years of professional experience, both Alfred and Victor have extensive experience in the state and local government industry, serving numerous clients similar to OCERS.

Alfred and Victor will be augmented by Joe Strain, engagement director, and Bhavin Darji, engagement supervisor.

The following professionals have the qualifications and experience to handle your needs for this engagement and are committed to exceeding your expectations. Please refer to [Appendix A](#) for detailed biographies.

Team member, engagement role	Qualifications to serve OCERS
<p>Alfred Ko Partner, Risk Consulting alfred.ko@rsmus.com</p> <p><i>Engagement partner.</i> As engagement partner, Alfred will have responsibility for the overall quality of RSM’s internal audit services. He will be responsible for ascertaining that professional and regulatory standards have been complied with throughout the engagement.</p>	<ul style="list-style-type: none"> • Over 20 years of experience in business process analysis and IT control assessments • Focuses on the assessment of information technology (IT) risks in support of IT internal audit co-sourcing and outsourcing engagements, financial statement and integrated audits, and service organization control (SOC) reporting • Certified public accountant in Michigan, Illinois, California and Hawaii
<p>Victor Kao Partner, Risk Consulting victor.kao@rsmus.com</p> <p><i>Relationship lead.</i> Victor leads RSM’s overall relationship with OCERS, including consulting services outside of internal audit. He will be responsible for your complete satisfaction with the services we provide and for ascertaining that your client experience is optimized.</p>	<ul style="list-style-type: none"> • Experience with accounting, operations, and IT subject matter expertise • Expertise in the technology, media and telecom industry • Certified public accountant, California



Team member, engagement role	Qualifications to serve OCERS
<p>Joseph (Joe) Strain Director, Risk Consulting joe.strain@rsmus.com</p> <p><i>Engagement lead.</i> Joe will oversee the quality of our cybersecurity internal audits with OCERS and monitor all phases of the audit to promote timely completion.</p>	<ul style="list-style-type: none"> • Experience analyzing network traffic, configuring intrusion detection, firewall systems and evaluating security controls • Over 10 years of internal audit experience • Certified information systems auditor
<p>Baru Sanchez Manager, Risk Consulting baru.sanchez@rsmus.com</p> <p><i>Engagement manager.</i> Baru will be responsible for performing detailed reviews of all work done by the engagement team to help ensure compliance with OCERS's internal audit professional standards. He will work closely with Alfred and Joe throughout the internal audit process to help ensure that all relevant information is communicated timely between management and our engagement team, and audit documentation and artifacts comply with OCERS's requirements and expectations.</p>	<ul style="list-style-type: none"> • Over 14 years in audit and consulting experience • Deep passion in serving state and local governments, based on a shared commitment to public service as former mayor and councilmember for Cudahy, California • Certified public accountant, California
<p>Bhavin Darji Supervisor, Risk Consulting bhavin.darji@rsmus.com</p> <p><i>Engagement supervisor.</i> As your engagement supervisor, Bhavin will serve as your primary contact on day-to-day matters, keep you informed about our progress and promptly address your questions and concerns.</p>	<ul style="list-style-type: none"> • Bhavin comes from industry where he served as the system administrator where he implemented security controls and therefore is experienced in analyzing various security tools • Bhavin is experienced in leading assessments against the following frameworks: CIS 18, NIST 800-53, NYDFS, HITRUST, HIPAA, PCI DSS and FFIEC



Team member, engagement role	Qualifications to serve OCERS
<p>Nick Russo Senior Associate, Risk Consulting nick.russo@rsmus.com</p> <p><i>Engagement team member.</i> Nick will serve as a specialty resource to the team, and participate in quality control of deliverables provided to OCERS.</p>	<ul style="list-style-type: none"> Nick has been working in cybersecurity internal audit for more than three years and has passed his Certified Information Systems Auditor (CISA) exam Nick’s focus is around cybersecurity internal audit including general reviews for ITGCs and FFIECS that include reviewing multiple cybersecurity processes including cybersecurity, business continuity, architecture, infrastructure, and operations, network virtualization, IT governance, data security, and more Nick also has experience with assisting clients with building out their internal audit plans (1–3 years) and identifying areas that present the most risk within the organization and help assess how often these areas of risk will be tested
<p>Jane Schneider Associate, Risk Consulting jane.schneider@rsmus.com</p> <p><i>Engagement team member.</i> Jane will serve as a specialty resource to the team, and participate in quality control of deliverables provided to OCERS.</p>	<ul style="list-style-type: none"> Jane is experienced in performing assessments against the NIST CSF and HIPAA frameworks and cybersecurity internal audit assessments, including general reviews for ITGCs and FFIECs with focus on vulnerability and patch management, IT asset management, cybersecurity governance and oversight, network and data security, identity and access management, SDLC, incident response, and cybersecurity resilience.
<p>Jennifer Bailey Account Manager, Sales jennifer.bailey@rsmus.com</p> <p><i>Account manager.</i> Jennifer will support Victor in helping to ensure your complete satisfaction with the services we provide. She will serve as your primary contact on day-to-day account relationship matters, keep you informed about our progress across all disciplines and services with OCERS, and promptly address your questions and concerns.</p>	<ul style="list-style-type: none"> Over 30 years of business management and client services experience Experience in business development, transaction management, partner relations, business operations and regulatory compliance ERP sales specialist, Sage Intacct



Client references

6. At least three (3) references for which the respondent has provided services similar to those included in the Scope of Services. Please include for each reference the individual point of contact, a summary of the work performed, and the length of time the respondent provided each service.

We encourage you to contact our references to learn more about us, our team and our process, in addition to their first-hand knowledge of our proposed services to OCERS.

Name of organization	Contact information	Work performed
State of Hawaii Employees' Retirement System \$22B public employees' retirement system	Thom Williams Executive Director thomas.williams@hawaii.gov	<ul style="list-style-type: none"> Co-sourced IT internal audit function since 2015, conducting internal audit IT risks assessments and developing IT audit plans IT audits delivered included network security reviews and penetration testing, data privacy review, cloud risk and security assessment, business continuity planning and testing Other consulting services included IT governance content development support, virtual CISO advisory services, and continuous monitoring proof of concept implementation
Utah Retirement Systems \$54B public employees' retirement system	Mike Gleue Senior Investment Analyst mike.Gleue@urs.org	<ul style="list-style-type: none"> Various asset management reviews since 2019
State Employees' Retirement System of Illinois \$24B public employees' retirement system	Timothy Blair Executive Director tim.blair@srs.illinois.gov	<ul style="list-style-type: none"> Financial statement audit GASB 68 pension allocation schedules Participating employer census attestation State compliance examination
Cook County Pension Fund \$13B public employees' retirement system	Sharon Tegegne Deputy Executive Director stegegne@countypension.com	<ul style="list-style-type: none"> Financial statement audit GASB 68 pension allocation schedules GASB 75 OPEB allocation schedules

Licenses

7. Copies of any pertinent licenses required to deliver respondent's product or service (e.g., business license).

RSM is legally authorized to do business in all 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands. The firm holds a Certificate of Registration as a limited liability partnership in every state except Delaware.

As a professional services assurance, tax and consulting firm, we have professionals with various certifications and licenses. RSM professionals specializing in providing services to the state and local government industry have the following relevant certifications:

- Accredited valuation analyst
- Certified risk management assurance professional
- Certified bank auditor
- Certified fiduciary and investment risk specialist
- Certified fiduciary and investment risk manager
- Certified financial forensics professional
- Certified financial services auditor
- Certified fraud examiner
- Certified governmental financial manager
- Certified information security manager
- Certified information systems auditor
- Certified Information systems security professional
- Certified internal auditor
- Certified investments and derivative auditor
- Certified management accountant
- Certified procurement manager
- Certified public accountant
- Certified regulatory compliance manager
- Certified risk professional
- Certified trust auditor
- Chartered certified accountant
- Professional designation in logistics and supply chain management
- Professional engineer
- Enrolled agent (specifically for tax-related services)
- GIAC-certified incident handler
- ISACA-certified information security manager
- Licensed actuary (specifically for actuarial services)
- Member of the Royal Institution of Chartered Surveyors
- EnCase® Certified Examiner in EnCase® Forensic Edition
- National security agency information security professional

Pricing

8. An explanation of the pricing proposal for the scope of work, including pricing of fees and costs, billing practices, and payment terms that would apply. OCERS does limit the pricing approach to pricing and will consider alternative pricing methods for the scope of work, or portions of it. This section of the response should include an explanation as to how the pricing approach(es) will be managed to provide the best value to OCERS. The respondent should represent that the pricing offered to OCERS is, and will remain, equivalent to or better than that provided to other public pension fund or institutional investor clients or explain why this representation cannot be provided. All pricing proposals should be “best and final,” although OCERS reserves the right to negotiate on pricing.

The broad description included in the RFP’s scope of services suggested the desire for a general ITGC and cybersecurity audit. Based on our understanding of your IT internal audit needs and your IT internal audit plans in the past six years, we propose that OCERS consider one of the following audits, in lieu of a general ITGC and cybersecurity audit. We believe that these options would provide OCERS with the most value and return given the organization’s current control environment and strong cybersecurity posture. However, should OCERS prefer a general ITGC and cybersecurity audit consistent with the RFP’s scope of services, we are confident that we can work closely with you to craft a meaningful audit scope that meets the committee’s expectations, for a similar fees range as follows:

Summary of deliverables	Estimated fee
Services—Option 1	
Ransomware assessment	\$57,500
Internal audit IT risk assessment refresh/Audit program	\$7,500
Total	\$65,000
Services—Option 2	
Third-party risk management audit	\$50,000
Internal audit IT risk assessment refresh/Audit program	\$7,500
Total	\$57,500

First-year costs

Due to the relationship that RSM and OCERS have built over the past six years, RSM will absorb the first-year costs of gathering historical information, building permanent files and understanding your business objectives.

Significant changes in your business

Significant changes in the nature and scope of your business will result in annual professional fee increases. Significant changes may include the addition of new locations, businesses or lines of business; unpreparedness on the part of OCERS; material changes in financial reporting; an unusual number of adjustments to the financial statements; and changes in the scope of work due to regulations, audit or accounting standards, or income tax laws.



Administrative expense

Our fees for the services described above are based upon the value of the services performed and the time required by the individuals assigned to the engagement plus directly billed expenses, including report processing, travel, meals and fees for services from other professionals, as well as other expenses, including indirect administrative expenses such as technology, research and library databases, communications, photocopying, postage and clerical assistance.

Fee assumptions

Any proposed fees are based on the following assumptions:

- Assistance will be supplied by OCERS personnel, including preparation of requested schedules and analyses of accounts before we commence fieldwork.
- There will be no significant changes in the nature and scope of the audit.

Our acceptance of this engagement is subject to completion of our acceptance procedures.



Conflicts of interest

9. An explanation of all actual or potential conflicts of interest that the respondent may have in contracting with OCERS.

All RSM partners and client service employees are provided access to our policies and procedures relating to independence and conflicts of interest and are educated about prohibited non-audit services, including consulting services. We obtain annual written acknowledgment regarding their understanding of, and compliance with, these policies.

Our firm uses our proprietary Client Engagement Assessment of Risks (CLEAR) application, which assists engagement teams in performing consistent and comprehensive evaluations of engagement risk, integrates our independence and business conflict checks process, helps assure that the engagement team has the requisite competency and experience, and provides our audit leadership with deeper insight into the risk profile of our client portfolio.

RSM is not aware of any actual or potential conflicts of interest regarding contracting with OCERS.

10. A description of all past, pending, or threatened litigation, including malpractice claims, administrative, state ethics, disciplinary proceedings, and other claims against respondent and/or any of the individuals proposed to provide services to OCERS.

RSM is a large national accounting/professional services firm. As with other national professional services firms, legal and regulatory activity is part of doing business. At any given time, most public accounting firms will have ongoing legal activity. As is customary within the accounting profession and with other professional practices, RSM US does not disclose its litigation history. Settlements and regulatory activity often involve matters that are bound by confidentiality agreements and orders on which we cannot comment. There are no claims currently in process that are expected to impact our ability to serve our clients.

Additional information

11. Any other information that the respondent deems relevant to OCERS' selection process.

The RSM internal audit methodology

RSM has a thorough internal audit methodology with a holistic approach to assessing your most critical risks. We understand that there is no one-size-fits-all internal audit project; therefore, we have a flexible methodology that helps internal audit evolve from a necessary process to assume a more strategic role within OCERS.

We leverage proven processes and advanced technology to help you mitigate risk, monitor compliance and add value to your organization. Our methodology is grounded in understanding your needs and working with you to develop a responsive approach to meet and exceed your expectations. In addition, we integrate quality assurance and project management resources to increase visibility into your internal audit project, providing real-time results and insight into progress.



Methodology elements

The RSM methodology is built upon five key components, working together to provide effective risk identification, mitigation processes and enhanced value to OCERS.

- **Planning.** We understand your business and needs, developing key reporting and project management strategies.
- **Risk assessment.** Our team evaluates and prioritizes your critical risks.

- **Strategy.** We establish an effective internal audit plan, leveraging industry knowledge and technology to properly scope your project.
- **Execution.** RSM advisors evaluate your key processes to assess compliance and analyze data.
- **Reporting.** We communicate what we have learned, comparing results to the plan, identifying root causes and providing steps for remediation.
- **Close-out.** We conclude your project, demonstrating benefits with our value scorecard and begin planning for next year's audit.

Our focused approach

Your experienced RSM internal audit team will begin your engagement with client needs assessments. These help our team go beyond getting to know OCERS's expectations, to understand your risk tolerance, motivations and what you need the audit to focus on. During these processes, we co-develop metrics to measure our performance against your expectations, positioning you to obtain optimal value during your audit cycle.

In addition, our internal audit methodology includes several key facets, including:

- **A national focus.** RSM has adopted a consistent national methodology, meaning that no matter where you operate, we have internal audit resources to meet your needs. This model allows you to receive consistent, effective internal audit services from a national bench of subject matter experts to help alleviate your domestic risks.
- **Timely, efficient processes.** As your current IT internal audit provider, RSM is well positioned to hit the ground running, initiating risk assessments and other key tools and activities to prepare your audit team members before they enter the field, saving you time and delivering results quicker.
- **Comprehensive project management.** RSM integrates project management and quality assurance processes directly into the methodology, rather than bolting those key processes on. Our engagement delivery technology has built-in quality assurance functionality and provides you with real-time status updates to monitor progress anywhere at any time.
- **A focused approach.** Our focused risk assessment helps to target your most pressing issues and risk exposures. We utilize an automated, customizable risk model, augmented by other automated accelerators and tools that are specific to your industry to efficiently identify your vulnerabilities.
- **Alignment with leading practices.** To provide you with consistent, effective audit service, our internal audit methodology aligns with the guidelines from the Institute of Internal Auditors' (IIA) *Global Internal Audit Standards*.

Appendices

Appendix A—Engagement team biographies



Alfred Ko

Partner, Risk Consulting
RSM US LLP
alfred.ko@rsmus.com



Summary of experience

Alfred focuses on the assessment of information technology (IT) risks in support of IT internal audit co-sourcing and outsourcing engagements, financial statement and integrated audits, Sarbanes-Oxley (SOX) 404, and service organization control (SOC) reporting. Nationally, he collaborates with the assurance standards methodology practice by leading the development and continuous enhancement of RSM's IT assurance methodology and supports the firm's response to the Public Company Accounting Oversight Board's (PCAOB) inspection of RSM's system of quality control. Alfred has over 20 years of experience in business process analysis and general IT control assessments, focusing on state and local governments and financial institutions. Alfred's representative experience includes:

- Managed IT internal audit co-sourcing or outsourcing engagements by overseeing clients' IT internal audit function, leading internal controls and financial reporting compliance projects, as well as operational IT projects that tackle emerging risks such as cybersecurity, Sheltered Harbor data vault and resiliency plan implementation and certification, digital banking, and system implementations
- Led numerous IT audits for middle market as well as Fortune 1000 organizations, directing the design, implementation, and operating effectiveness testing of IT application and general controls in support of annual financial statement and integrated audits and assessments of internal controls over financial reporting
- Conducted over 100 SOC examinations and readiness assessments, developed thought leadership materials on the introduction of SOC, and built marketplace eminence through webcasts and presentations at local ISACA chapters

Professional affiliations and credentials

- Certified public accountant, Michigan, Illinois, California and Hawaii
- Certified information systems auditor
- Certification in risk management assurance

Education

- Master of Accounting, University of Southern California
- Bachelor of Science, computer science and economics, University of Michigan



Victor Kao

Partner, Risk Consulting
RSM US LLP
victor.kao@rsmus.com

Summary of experience

Victor provides a unique blend of accounting, operations, and IT subject matter expertise, and leads a wide spectrum of projects including internal audit, Sarbanes-Oxley (SOX) compliance, system and organization controls (SOC) readiness and attestation, business process improvement and information technology assessment services. Prior to joining RSM, he served in senior management roles in a variety of industries, including technology, media and entertainment, consumer products, banking and financial services.

Currently, Victor's core industry and subject matter expertise lies within the technology, media and telecom industry. He was recently selected as an industry leader in RSM's Industry Eminence Program, which positions its fellows to understand, predict and communicate economic, business and technology trends shaping the industries RSM serves. Through the program, Victor advises and consults clients on conditions impacting middle market and global leaders within technology, and provides thought leadership, guidance, and industry insights as a catalyst to innovate, differentiate, and transform the industry.

Victor has substantial IT risk advisory experience leading and coordinating enterprise resource planning (ERP) software selections and implementations, IT general controls review, segregation of duties (SOD) analysis, cybersecurity, and SOC readiness and attestation. His experience includes:

- Led and implemented SOX readiness and application control development to achieve 404(a) and 404(b) compliance ranging from non-accelerated to large, accelerated filers
- Advised senior management, board of directors and audit committees in the design and implementation of financial, operational and IT internal controls across numerous system implementations and internal control frameworks such as Committee of Sponsoring Organizations (COSO), control objectives for information and related technology (COBIT) and IT infrastructure library (ITIL), and improved overall efficiencies
- Prepared, facilitated, and led the development of SOC reports (e.g., SOC 1, SOC 2, and SOC 3) to achieve readiness and attestation reports ranging from small start-up to large global service organizations
- Developed best practice SOD framework, tools and policy and procedures for large ERP packages to help management identify SOD conflicts and risk mitigation tactics
- Led business transformational efforts to formalize internal controls and improve process efficiencies for a large manufacturing and distribution company with over \$5 billion in revenue

- Developed a comprehensive risk and compliance model for regulatory statutes, such as SOX, Federal Deposit Insurance Corporation Improvement Act (FDICIA), Department of Insurance, OSHA, Food and Drug Administration and California Dairy Institute
- Revamped IT system development life cycles, including program change management to incorporate formal documentation, reviews and approval
- Implemented end-user computing framework to identify, assess and monitor critical information
- Reviewed and consolidated financial statements and supporting industry metrics

Professional affiliations and credentials

- Certified public accountant, California
- Certified information systems auditor
- Certified in risk and information systems control
- Certified in risk management assurance

Education

- Master of Science, accounting, University of Virginia
- Bachelor of Arts, business economics with accounting emphasis, University of California, Santa Barbara
- Bachelor of Arts, mathematics, University of California, Santa Barbara
- Certificate in Food Industry Management, University of Southern California





Joseph Strain

Director, Risk Consulting
RSM US LLP
joe.strain@rsmus.com

Summary of experience

Joe is a system security specialist with experience analyzing network traffic, configuring intrusion detection, firewall systems and evaluating security controls. His experience in system administration and computer security allows him to provide valuable insight in understanding and evaluating information systems security controls, and understanding the security and risk implications of IT-connected business processes. Joe has experience in a variety of system administration and security-related tasks and has pursued applied research related to human factors and IS security. Joe also has over 10 years of internal audit experience which includes performing IA risk assessments, executing audits, and presenting to and training audit committees and boards. His highlights include:

- Investigating and analyzing network traffic for known vulnerabilities
- Deploying and administrating virtual environments across multiple platforms
- Configuring and monitoring intrusion detection systems on multiple platforms
- Evaluating and configuring Windows server, including Active Directory
- Writing policies and documents, which include disaster recovery, business continuity and risk analyses reports
- Performing vulnerability and penetration testing against a wide variety of systems
- Performing system and organization controls attestation engagements, which includes formulating IT controls for multiple business types
- Performing FFIEC driven IT audits to discover control weaknesses in audit areas, such as vendor management and IT governance
- Planning, scoping, and delivering cyber security reviews as part of an internal audit program
- Performing payment card industry gap assessments to help clients achieve compliance while reducing scope
- Performing social engineering testing including custom phishing emails, phone calls and physical impersonations
- Performing NIST and ISO gap assessments for a broad range of industries

Professional affiliations and credentials

- Certified information systems auditor
- Certified information security manager
- Payment card industry qualified security assessor
- Information Systems Audit and Control Association
- InfraGard
- Institute of Internal Auditors
- NJ Bankers

Education

- Bachelor of Science, computing technology, Drexel University
- Associate of Applied Science, networking and system administration, Rowan College at Burlington County

38

300





Baru Sanchez

Manager, Risk Consulting
RSM US LLP
baru.sanchez@rsmus.com

Summary of experience

Baru has over 14 years in audit and consulting experience in public, private, and government sectors. He brings a wealth of knowledge and expertise, particularly in the Public Sector, SOX 404, and IT. Based in the greater Los Angeles area, Baru has successfully served clients across a variety of industries including government, manufacturing, property management, retail, and nonprofit organizations.

Baru has a proven track record of identifying critical risk areas and collaborating with clients to develop and enhance controls over their IT and business processes. His areas of expertise include evaluation of the effectiveness of clients accounting and IT controls environments, implementation and monitoring of IT controls relating to Segregation of duties (SOD) and regulatory compliance programs.

In addition to his professional career, Baru served his community as Mayor and Councilmember for his hometown city of Cudahy, California from 2013 through 2018. During this time, he championed transparency, compliance, and effective governance. He also contributed his expertise to several keyboards, including:

- HUB Cities consortium
- Gateway cities council of governments I-710 EIS/EIR project committee
- Southern California Association of Governments
- Greater Los Angeles Vector Control District
- California Contract Cities Association

Through these roles, Baru developed a deep understanding of government operations, public policy, and inter-agency collaboration. Fluent in Spanish and highly knowledgeable in governmental affairs, Baru brings a unique and valuable perspective to his work.

Professional affiliations and credentials

- Certified public accountant, California
- American Institute of Certified Public Accountants
- Information Systems Audit and Control Association

Education

- Bachelor of Science, accountancy, California State University Long Beach





Bhavin Darji

Supervisor, Risk Consulting
RSM US LLP
bhavin.darji@rsmus.com

Summary of experience

Bhavin joined RSM in October 2020, in the security and privacy risk consulting practice, where he has been providing consulting services to firms all over the world. Bhavin has assisted various Fortune 500 clients achieve pay card industry (PCI) and HITRUST compliance. He has experience leading and performing analysis work with various frameworks such as PCI, HITRUST, HIPAA, NIST 800-53, and NYDFS.

Bhavin focuses on the PCI and has achieved his associate qualified security assessor certification. With this certification, Bhavin has been able to lead interviews and analysis work for large retail store clients and assist them in achieving PCI compliance.

Prior to joining RSM, Bhavin was a systems administrator at a real estate company where he oversaw the IT infrastructure for the firm along with its affiliates.

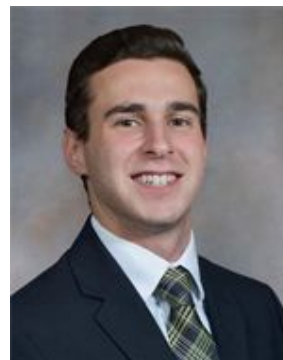
Professional affiliations and credentials

- Certified AWS cloud practitioner
- Certified Cisco entry networking technician
- Certified Cisco network associate
- Certified HITRUST CSF practitioner
- Microsoft technical associate: networking fundamentals
- PCI associate qualified security assessor
- PCI professional

Education

- Bachelor of Business Administration, information risk management and cybersecurity, Baruch College





Nicholas Russo

Senior Associate, Risk Consulting
RSM US LLP
nick.russo@rsmus.com

Summary of experience

Nick provides security and privacy risk consulting services, specifically cyber strategy, risk and compliance. In his current role, Nick assists and helps clients stay safe by making sure they are following the proper cybersecurity procedures and best practices, so that if an issue is detected, the clients will be better prepared for how to handle it. Nick has focused assisting clients located within financial services and banking strengthen their information security programs, identify and remediate potential vulnerabilities, stay on top of compliance with evolving regulations, and much more.

Additionally, Nick has experience within the cybersecurity internal audit field and is well versed in IA strategies like work program development, detail testing, and leading audit walkthrough meetings. Nick has participated in a vast range of cybersecurity internal audits that involved components such as patch and vulnerability management, secure development life cycle, information security, disaster recovery readiness, incident response preparedness, cyber insurance coverage, and much more. Nick is looking forward to using the information gained from experience and dedicated research to help clients stay protected from the many evolving threats and vulnerabilities networks can encounter on a daily basis.

Professional affiliations and credentials

- Certified CompTIA Security +
- Certified information systems auditor
- AWS certified cloud practitioner

Education

- Bachelor of Science, security and risk analysis, information systems technology, Penn State University



Jane Schneider

Associate, Risk Consulting
RSM US LLP
jane.schneider@rsmus.com

Summary of experience

Jane serves as a consultant in RSM's security and privacy risk consulting practice and is experienced in cybersecurity and IT audit assessments. Her experience includes performing assessments against the NIST cybersecurity framework and HIPAA frameworks, as well as conducting internal audits for IT general controls and Federal Financial Institutions Examination Council standards. Her areas of focus include vulnerability and patch management, IT asset management, cybersecurity governance and oversight, network and data security, identity and access management, software development life cycle, incident response, and cybersecurity resilience.

Jane earned her Bachelor of Science in applied data sciences with a concentration in information and cybersecurity sciences and a minor in security and risk analysis from The Pennsylvania State University in May 2023. During her time at Penn State, she contributed as a teaching assistant for courses in statistics and probability, information sciences, and data sciences.

Professional affiliations and credentials

- Amazon Web Services, certified cloud practitioner
- Information Systems Audit and Control Association
- Institute for Internal Auditors

Education

- Bachelor of Science, applied data sciences, minor in security and risk analysis, The Pennsylvania State University





Jennifer Bailey

Account Manager, Sales
RSM US LLP
jennifer.bailey@rsmus.com

Summary of experience

Jennifer contributes over 30 years of business management and client services experience with ten years focused on health care as the co-owner of an Atlanta-based assisted living community. She spent 10 years serving clients as an M&A advisor and sales executive in the financial software space, with four years focused on the Sage software portfolio, including Sage Intacct.

Throughout her career, she has put her effective management and leadership abilities to work helping profit and nonprofit organizations further enhance their business efficiencies to ultimately achieve their corporate missions. She has strategically positioned herself to be a first-choice advisor in the middle market sector with experience in the health care, nonprofit, construction real estate, fintech, manufacturing and distribution industries. She brings experience in business development, transaction management, partner relations, business operations and regulatory compliance.

As an RSM team member, Jennifer looks forward to guiding clients as they navigate the ever-evolving technology landscape. Together we deliver technology investment optimization to support business growth while maximizing ROI.

Professional affiliations and credentials

- ERP sales specialist, Sage Intacct
- Sage Intacct community user



Appendix B—Writing samples

Please refer to the attached Appendix B—IT Risk Assessment Report Sample.pdf and Appendix B—NIST CSF 2.0 Maturity Assessment Sample Report.pdf.



Appendix B - IT Risk
Assessment Report Sa



Appendix B - NIST
CSF 2.0 Maturity Asse:

Here are the instructions to open up the sample writings in the PDF file.

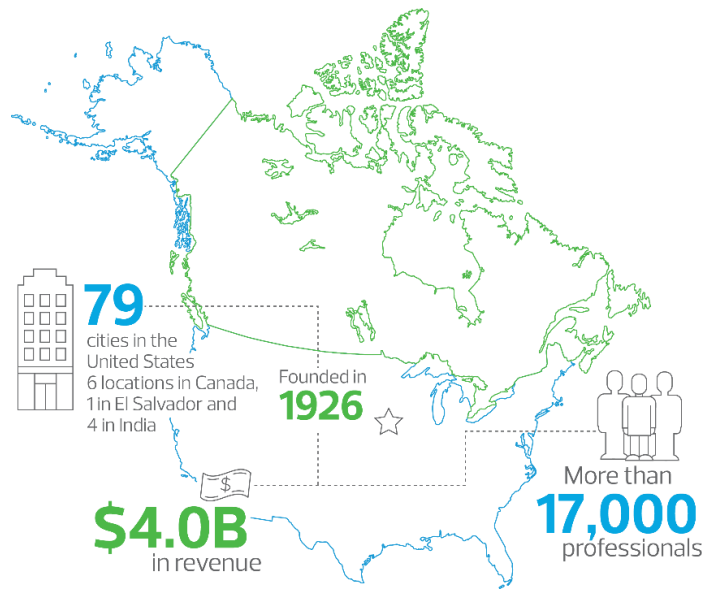
- *Download and save the PDF file*
- *Now, open a PDF reader*
- *Once you open the PDF reader, open the PDF file*
- *You should now be in read and edit mode*
- *Click on the attachment paperclip on the left side menu bar*
- *Click on the attachments paperclip icon*
- *You'll now see both sample writing icons*



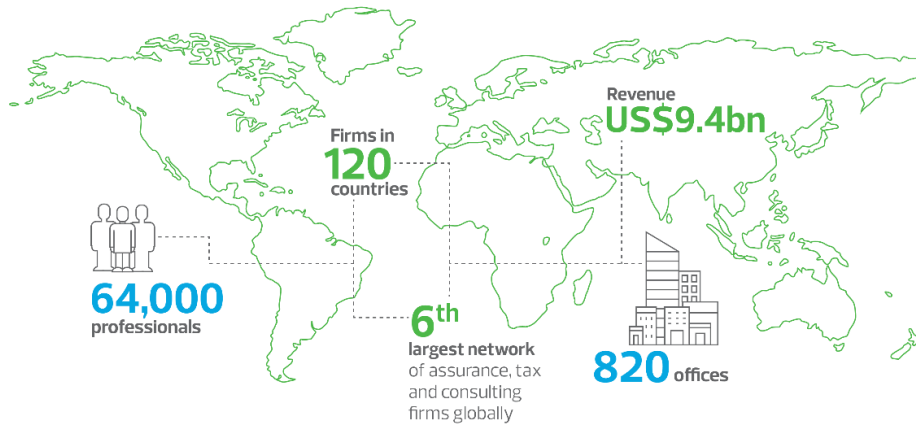
Appendix C—About RSM

RSM's purpose is to deliver the power of being understood to our clients, colleagues and communities through world-class assurance, tax and consulting services focused on middle market businesses. The clients we serve are the engine of global commerce and economic growth, and we are focused on developing leading professionals and services to meet their evolving needs in today's ever-changing business environment.

RSM is the leading provider of assurance, tax and consulting services focused on the middle market, with more than 17,000 professionals in 79 U.S. cities, six locations in Canada, one in El Salvador and four in India. It is a licensed CPA firm and the U.S. member of RSM International, a global network of independent assurance, tax and consulting firms with 64,000 people in 120 countries. RSM uses its deep understanding of the needs and aspirations of clients to help them succeed.



RSM International is a global network of independent assurance, tax and consulting firms.



Appendix D—Culture of Inclusion at RSM

RSM is a thought leader in the profession concerning the imperatives of culture, diversity and inclusion. These imperatives are not only part of our values, but also how we foster a diverse workforce, help the middle market address an ever-changing world and generate better business results for our firm and our clients. Internally, RSM invests over \$3 million annually, with nine full-time resources and over 200 professionals serving in volunteer roles executing our Culture of Inclusion programming. The Culture of Inclusion focus at RSM spans four strategic pillars:

People



The recruitment, advancement and retention of underrepresented women and minorities and the inclusive talent experience for all professionals is a key goal. RSM funds 12 employee network groups (ENGs) to address the needs of our diverse talent population and, by extension, to increase cultural competency in our client service.

Firm



Our enterprise-wide Culture of Inclusion Council, which comprises our CEO and other executive leaders, help ensure inclusion is a funded and strategic priority. RSM further provides that inclusion is driven into our policies and the fabric of our business. Culture of Inclusion collaborates with our human resources, recruiting and professional development teams as well as the assurance, tax and consulting teams.

Markets



RSM supports diverse suppliers and organizations across the profession, including the National Association of Black Accountants (NABA), Association of Latino Professionals for America (ALPFA), Ascend (a Pan-Asian organization for business professionals), Student Veterans of America (SVA) and AICPA Women's Leadership, among others.

Community



RSM's Culture of Inclusion program supports non-profit efforts and organizations in the communities where we do business. Culture of Inclusion corporate social responsibility includes scholarships, sponsorships and volunteerism with hundreds of entities annually.

www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2024 RSM US LLP. All Rights Reserved.



Memorandum

DATE: February 11, 2025
TO: Members of the Audit Committee
FROM: Philip Lam, Director of Internal Audit
SUBJECT: CONSIDERATION OF THE 2025 RISK ASSESSMENT AND AUDIT PLAN

Recommendation

Approve the 2025 Risk Assessment and Audit Plan.

Background/Discussion

Attached are Internal Audit's 2025 Risk Assessment and Audit Plan. The projects include:

1st half of 2025

- Finalizing testing and audit reports for (carryover from 2024 Audit plan):
 - Employer Audit – Orange County Local Agency Formation Commission (LAFCO)
 - Finance Payroll Process for Retirees
 - Alameda Phase 2 Recalculations
- Investment Due Diligence: Review due diligence procedures performed by the Investment department staff and Investment consultants.
- Investment Compensation Calculation Review: Review and validate the calculation of the Investment Division's incentive payments to ensure the calculations are complete and accurate.
- Employer Audit – Orange County Sanitation District: Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.
 - Last audited in 2019

2nd half of 2025

- Finance Contributions Process: Review the Finance Department's controls over the recording of contributions in the general ledger.
 - Last audited in 2019
- Service Credit Purchases: Review Member Services' controls over Service Credit Purchase contracts and calculations.
 - Last audited in 2016



Memorandum

- Employer Audit – County of Orange (District Attorney): Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system (PAS); review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.
 - First time audit
- Employer Audit – Orange Country Cemetery District: Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.
 - Last audited in 2020
- Final Average Salary Benefit Calculation:
 - Audit of FAS calculations during one quarter in 2025. Selection TBD.

On-Going throughout 2025

- Management Action Plan Verification: Confirm management action plans from prior audits have been implemented.

Submitted by:

PL - Approved

Philip Lam

Director of Internal Audit

**Orange County Employees Retirement System
2025 Internal Audit Plan**



Audit Activity	Description	Planned Hours	Comments
Internal Audit/Consulting/Planning/QAIP		4,875	
Internal Audits - Assurance		3,675	
Employer (Orange County - Local Agency Formation Commission - LAFCO)	Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.	80	Carryover from 2024
Alameda 2 Implementation	Perform an independent review of the controls in place to ensure the recalculation of contribution refunds and retirement benefits related to the Alameda decision are complete and accurate for Alameda phase 2.	200	Carryover from 2024
Payroll for Retirees	Review the Finance Department's controls over the general ledger recording of monthly benefit payments.	100	Carryover from 2024
Investment Compensation Review	Perform independent review of annual investment compensation calculations.	250	Annual audit per policy
Finance contributions process	Review the Finance Department's controls over the recording of contributions in the general ledger.	350	Last audited in 2019
Investment due diligence	Review due diligence procedures performed by the Investment department.	375	Last audited in 2019
Service Credit Purchases	Review Member Services controls over Service Credit Purchase contracts and calculations.	375	Focus area of Audit Chair. Last audited in 2016
Continuous Audit - Final Average Salary (FAS) Calculation	Continuous audit of FAS calculations. Sample quarter TBD.	375	As directed by Audit Chair, audit one quarter in 2025.
Employer (County of Orange - District Attorney)	Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.	400	First time audit

**Orange County Employees Retirement System
2025 Internal Audit Plan**

Audit Activity	Description	Planned Hours	Comments
Employer (Orange County Sanitation District)	Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.	375	Last audited in 2019
Employer (Orange County Cemetary District)	Review employer's supporting documentation to verify accuracy and completeness of payroll data transmitted to OCERS pension administration system; review employer's controls to ensure compliance with OCERS Membership Eligibility Requirements Policy.	375	Last audited in 2020
IT Info Sec Audit	Perform an independent assessment of Information Security's controls	160	Co-sourced audit with IT audit vendor

**Orange County Employees Retirement System
2025 Internal Audit Plan**

Audit Activity	Description	Planned Hours	Comments
Intenal Audit - Management Action Plan Follow-up	Action Plan Follow-up - Perform MAP follow-ups with management	260	Ongoing review of implemented MAPs from completed audits
Internal Audits - Consulting		400	
Consulting/Ad-hoc projects	Open for any ad-hoc project TBD	400	Includes time to assist with ACFR, management or committee requests
Internal Audits - Planning		500	
Annual Audit Planning	Review and update Risk and Control Matrix.	200	Update throughout 2025
	Annual preparation of the Audit Plan, updates to the current Audit Plan.	300	2025 Audit Plan to be presented for approval in early 1st quarter 2025 AC meeting
Internal Audits - Quality Assurance and Improvement Program		300	
Quality Assurance and Improvement Program	IA Quality Review- Self Assessment - Internal Quality Assurance and Improvement Program (QAIP)	300	Implement IIA's new Global Standards with our QAIP program
Vision and Values		90	
	Vision and Values Committee (Internal OCERS Committee)	90	
Board, AC, OCERS Executive Meetings		623	
	Board meetings, Audit Committee, Personnel Committee, Governance Committee, Executive meeting, Strategic Planning	510	-
	Weekly meetings with CEO	50	-
	Monthly meeting with Audit Committee Chair	63	-
General admin time		700	
	General admin time	700	9% of total hours
Leave (Holiday/Annual) and Training		1,104	
	Holidays (12 days), Annual Leave (15 days)	864	-
	Training and Continuing Education	240	-
Grand Total Hours		<u>7,392</u>	

Internal Audit 2025 Risk Assessment Matrix

Risk Rankings	High	High to Medium	Medium	Medium to Low	Low
Definitions	5	4	3	2	1

2025 Audit Topic
Potential 2026 Audit Topic

Department	Auditable Process	Materiality / Financial Impact / Compliance	Strategic / Operational Impact	Change / Stability	Complexity of Operations or Regulations	Political / Reputation	Last Audit - Time and Results	Average Risk Ranking	Last Audited	Rotational Cycle
0010 - EXECUTIVE	Automation (AI/RPA) Governance	5	5	5	5	4	5	4.8		1
0011 - INVESTMENTS	Due diligence	5	5	5	5	5	3	4.7	1/13/2020	2
0001 - BOARD	Governance	5	5	3	4	5	5	4.5		3
0080 - INTERNAL AUDIT	Action plan follow-up	5	5	5	3	4	5	4.5		1
0040 - FINANCE	Investment accounting and valuation	5	5	4	4	4	4	4.3	11/23/2020	3
0070 - INFORMATION TECHNOLOGY	Network Security	5	5	5	5	5	1	4.3	1/19/2024	3
0010 - EXECUTIVE	Actuarial extract	5	5	3	4	5	4	4.3	10/13/2020	3
0030 - MEMBER SERVICES	COLA adjustments	5	4	3	5	4	5	4.3		4
0030 - MEMBER SERVICES	Final Average Salary Review	5	5	5	5	5	1	4.3	12/12/2024	1
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (County, including eligibility, pension spiking) - OC District Attorney	5	5	3	5	5	3	4.3	First time audit for OC District Attorney	2
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (All other active plan sponsors, including eligibility, pension spiking) - OC Sanitation District - OC Cemetery District	5	5	3	4	5	4	4.3	OC SD: 5/26/2020 OC CD: 3/22/2021	3
0010 - EXECUTIVE	System Implementation	5	5	5	5	5	1	4.3	1/19/2024	3
0040 - FINANCE	Contributions - member, employer	5	5	4	4	4	3	4.2	6/6/2019	3
0040 - FINANCE	General Ledger	5	5	5	4	3	3	4.2	11/23/2020	3
0040 - FINANCE	Payroll for retirees	5	5	4	5	5	1	4.2	2/11/2025	1
0011 - INVESTMENTS	Investment manager fee reporting	5	4	5	4	5	2	4.2	3/30/2022	3
0011 - INVESTMENTS	Investment reconciliations	5	5	3	4	5	3	4.2	11/23/2020	3
0030 - MEMBER SERVICES	1099 reporting	5	3	4	4	4	5	4.2		4
0030 - MEMBER SERVICES	Disability process	4	4	5	4	5	3	4.2	1/28/2019	3

Internal Audit 2025 Risk Assessment Matrix

Department	Auditable Process	Materiality / Financial Impact / Compliance	Strategic / Operational Impact	Change / Stability	Complexity of Operations or Regulations	Political / Reputation	Last Audit - Time and Results	Average Risk Ranking	Last Audited	Rotational Cycle
0090 - INFORMATION SECURITY	Data Privacy and Protection	5	5	1	4	5	5	4.2		3
0090 - INFORMATION SECURITY	Information Security	5	5	5	4	5	1	4.2	10/9/2024	3
0030 - MEMBER SERVICES	Transmittal error clearing	5	5	5	5	4	1	4.2	3/28/2024	4
0020 - LEGAL	Compliance Department	5	4	4	3	4	5	4.2		3
0020 - LEGAL	Compliance Program	5	4	4	3	4	5	4.2		3
0030 - MEMBER SERVICES	Call Center management	2	4	5	5	4	5	4.2		3
0040 - FINANCE	Financial reporting	5	4	4	4	4	3	4.0	3/26/2020	3
0060 - HUMAN RESOURCES	HR Processes	2	5	4	4	4	5	4.0		4
0010 - EXECUTIVE	Business continuity / disaster recovery	5	5	3	5	5	1	4.0	10/9/2024	4
0040 - FINANCE	Budgeting	5	4	3	3	4	5	4.0		3
0070 - INFORMATION TECHNOLOGY	Data security 3rd party vendors	5	5	5	3	5	1	4.0	1/19/2024	4
0020 - LEGAL	Form 700 Compliance review	3	4	4	3	5	5	4.0		4
0030 - MEMBER SERVICES	Benefit setup (including eligibility, pension spiking)	5	5	3	5	5	1	4.0	12/12/2024	1
0011 - INVESTMENTS	Investment consultant review	5	5	2	4	5	3	4.0	10/4/2021	3
0030 - MEMBER SERVICES	Death matching process	3	3	4	4	5	5	4.0	6/14/2016	5
0030 - MEMBER SERVICES	Survivor claims	5	5	3	4	4	3	4.0	10/4/2021	3
0030 - MEMBER SERVICES	Service Credit Purchases	3	3	5	4	4	5	4.0	11/29/2016	5
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (Sanitation District)	4	5	3	4	5	3	4.0	6/4/2020	3
0070 - INFORMATION TECHNOLOGY	IT Governance, Strategy, and Planning	3	5	5	5	3	3	4.0	11/30/2020	4
0070 - INFORMATION TECHNOLOGY	IT Vendor / Third Party Management	5	5	4	4	5	1	4.0	10/9/2024	4
0090 - INFORMATION SECURITY	Event, Incident, and Problem Management	5	5	4	5	4	1	4.0	10/19/2024	4
0015 - COMMUNICATIONS	External media/communication oversight	3	4	4	3	5	5	4.0		1

Internal Audit 2025 Risk Assessment Matrix

Department	Auditable Process	Materiality / Financial Impact / Compliance	Strategic / Operational Impact	Change / Stability	Complexity of Operations or Regulations	Political / Reputation	Last Audit - Time and Results	Average Risk Ranking	Last Audited	Rotational Cycle
0065 - OPERATIONS SUPPORT SERVICES	HQ management	3	3	5	3	4	5	3.8		3
0065 - OPERATIONS SUPPORT SERVICES	Procurement	5	4	4	3	5	2	3.8	10/3/2022	3
0060 - HUMAN RESOURCES	Succession Planning	2	5	3	3	5	5	3.8		4
0010 - EXECUTIVE	Ethics Policy	5	5	3	3	5	2	3.8	10/11/2023	4
0065 - OPERATIONS SUPPORT SERVICES	Contract Management (e.g. Vendor contract compliance)	5	5	3	3	5	2	3.8	10/3/2022	4
0011 - INVESTMENTS	Asset allocation/rebalancing - Governance	5	5	4	3	5	1	3.8	3/28/2024	2
0011 - INVESTMENTS	Cash/Wire Processing	5	5	4	3	4	2	3.8	12/30/2021	3
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (Superior Court)	4	5	3	4	5	2	3.8	4/5/2023	3
0040 - FINANCE	Cash management	5	5	3	4	3	2	3.7	1/27/2022	3
0065 - OPERATIONS SUPPORT SERVICES	Physical security	2	4	3	3	5	5	3.7		4
0020 - LEGAL	Record management and retention	3	5	5	3	4	2	3.7	10/11/2023	1
0030 - MEMBER SERVICES	IRS 415 benefit payment limits	3	3	3	3	5	5	3.7		5
0080 - INTERNAL AUDIT	QAIP (Internal)	1	3	5	3	5	5	3.7		1
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (OCTA)	4	5	3	4	5	1	3.7	6/6/2024	3
0060 - HUMAN RESOURCES	Hiring	2	5	4	4	4	2	3.5	10/11/2023	4
0030 - MEMBER SERVICES	Reciprocity	3	3	3	4	3	5	3.5	8/2/2017	5
0070 - INFORMATION TECHNOLOGY	Software Development Life Cycle / Change Management	4	4	2	4	3	4	3.5	12/30/2019	5
0011 - INVESTMENTS	Securities Lending fees	2	5	3	4	4	3	3.5	12/14/2020	5
0030 - MEMBER SERVICES	Lump sum payments (death benefits, refunds)	4	3	3	4	4	2	3.3	10/4/2021	4
0030 - MEMBER SERVICES	Member Enrollment	3	5	3	3	4	2	3.3	10/13/2023	4
0030 - MEMBER SERVICES	IRS 401 contribution limits	3	3	3	3	3	5	3.3		5
0070 - INFORMATION TECHNOLOGY	Knowledge Management	2	3	5	4	1	5	3.3		5

Internal Audit 2025 Risk Assessment Matrix

Department	Auditable Process	Materiality / Financial Impact / Compliance	Strategic / Operational Impact	Change / Stability	Complexity of Operations or Regulations	Political / Reputation	Last Audit - Time and Results	Average Risk Ranking	Last Audited	Rotational Cycle
0070 - INFORMATION TECHNOLOGY	IT Operations	3	4	2	3	4	4	3.3	12/30/2019	5
0030 - MEMBER SERVICES	Interest posting / crediting	5	4	2	3	2	3	3.2	6/6/2019	5
0030 - MEMBER SERVICES	Dependent eligibility	4	4	2	2	4	3	3.2	10/4/2021	5
0030 - MEMBER SERVICES	Contribution transmittals Plan Sponsors (All other active plan sponsors)	4	5	3	3	3	1	3.2	12/12/2024	4
0070 - INFORMATION TECHNOLOGY	IT Asset Management	3	5	4	4	2	1	3.2	10/9/2024	5
0070 - INFORMATION TECHNOLOGY	IT Availability and Capacity	3	4	2	2	3	5	3.2		5
0040 - FINANCE	Custodian Bank Fees	2	3	4	2	3	5	3.2		5
0080 - INTERNAL AUDIT	QAIP (External)	1	3	5	3	5	1	3.0		4
0030 - MEMBER SERVICES	Member Data Maintenance	2	4	2	3	5	2	3.0	6/1/2023	5
0040 - FINANCE	Accounts Payable	3	3	3	4	2	2	2.8	3/28/2024	5
0070 - INFORMATION TECHNOLOGY	Data Retention and Backup	4	4	1	3	4	1	2.8	10/9/2024	5
0030 - MEMBER SERVICES	Domestic Relations Order (DRO)	2	3	2	3	2	5	2.8		5
0030 - MEMBER SERVICES	Retiree Rehires (PEPRA)	3	2	2	1	5	2	2.5	10/13/2023	5
0040 - FINANCE	Travel expenses	2	1	2	1	5	3	2.3	12/6/2017	5

Internal Audit 2025 Risk Assessment Matrix

Department	Auditable Process	Materiality / Financial Impact / Compliance	Strategic / Operational Impact	Change / Stability	Complexity of Operations or Regulations	Political / Reputation	Last Audit - Time and Results	Average Risk Ranking	Last Audited	Rotational Cycle
------------	-------------------	---	--------------------------------------	--------------------	---	---------------------------	----------------------------------	-------------------------	-----------------	---------------------

Risk Assessment Methodology:

Internal Audit established the structure of the risk assessment by identifying key programs, projects, and processes (auditable entities). We then identified the following categories of risk:

1. **Materiality / Financial Impact / Compliance** – The magnitude of financial exposure, the degree of regulatory oversight, possible financial penalties.
2. **Strategic / Operational Impact** – The significance of this process to OCERS’ strategic success, impact of process disruption.
3. **Change / Stability** – How much the process has been altered and the change of personnel carrying out the process.
4. **Complexity of Operations or Regulations** – The number of individuals, entities, and processes involved, and the degree to which professional judgment or technical expertise is applied.
5. **Political / Reputation** – The degree of public interest and awareness, the visibility of the process to the media.
6. **Last Audit: Time and Results** – The length of time since the last audit or review was conducted and the results of that audit or review.



Memorandum

DATE: February 11, 2025
TO: Members of the Audit Committee
FROM: Philip Lam, Director of Internal Audit
SUBJECT: REPORTING OF INTERNAL AUDIT KEY PERFORMANCE INDICATORS

Presentation

Background/Discussion

Formal key performance indicators (KPIs) were established for Internal Audit at the December 2022 Audit Committee meeting. The KPIs are used to measure our performance by ensuring quality and risk-based assurance services. Additionally, the KPIs help ensure staff skills are current and relevant to the audit profession.

The results of the Internal Audit KPIs are reported below:

1. Annual Audit Plan Approved by Audit Committee
 - The Annual Internal Audit plan is prepared on a risk-based approach. The Annual Internal Audit plan is submitted to the Audit Committee for review and approval.
 - **Met** – The 2024 Annual Internal Audit plan was approved by the Audit Committee at the January 2024 Committee meeting.
2. Audit workpapers are reviewed within four weeks after initial draft audit report.
 - Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.
 - **Met** – The audit workpapers from the eight audit reports issued to management in 2024 were reviewed on average of two weeks within initial draft report issuance.
3. Timely report issuance – 80% of draft audit reports are issued to management within four months from the start of fieldwork.
 - Internal Auditors must communicate the results of engagements. Timely reporting indicates effective engagement management and provides management with more timely recommendations to implement management action plans.
 - **Met** – 100% of the eight audits presented to management in 2024 were issued to management within four months of start of field work.
4. Team members complete at least 20 hours for professional development training each year.
 - Training ensures each team member's skill set remains current and relevant.
 - **Met** – Each member had at least 20 hours, with an average of 60 hours of training per auditor in 2024.
5. Complete an external quality assessment review at least once every five years.



Memorandum

- A quality assessment review (QAR) compares OCERS' internal audit activities against the International Standards for the Professional Practice of Internal Auditing (the Standards). Compliance with the Standards speaks to the effectiveness and efficiency of our internal audit function.
- **Met** – The QAR was performed in 2023 and reported at the January 2024 Audit Committee meeting.

Submitted by:



PL- Approved

Philip Lam
Director of Internal Audit



Memorandum

DATE: February 11, 2025
TO: Members of the Audit Committee
FROM: Philip Lam, Director of Internal Audit
SUBJECT: MANAGEMENT ACTION PLAN VERIFICATION REPORT

Written Report

Background/Discussion

Under the International Standards for the Professional Practice of Internal Auditing (“Standards”), Internal Audit must establish and maintain a system to monitor the disposition of prior results communicated to management. This includes a follow-up process to monitor and ensure that management action plans have been implemented or that management and the Audit Committee has accepted the risk of not taking action.

The follow-up on management action plans (MAPs) involves:

- Confirming management has implemented an action plan and no further action is required.
- Internal Audit has tested the operational effectiveness of the MAPs.

The following report contains the status of the MAPs that have been reported to the Audit Committee:

- For the MAPs noted as Open, Internal Audit will continue to work with the respective parties until the MAP is closed and verified.
- For the MAPs noted as Closed – No Further Action Required (YTD), Internal Audit has confirmed the MAPs have been implemented and are operating effectively during the current year.
- For the MAPs noted as Closed – No Further Action Required (Prior Years), MAPs that have been implemented and confirmed as operating effectively prior to the current year.

Submitted by:



PL - Approved

Philip Lam
Director of Internal Audit



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



REPORTING FOR: 2018, 2019, 2020, 2021, 2022, 2023, 2024, ARCHIVED	OPEN	Closed - No Further Action Required (YTD)	Closed - No Further Action Required (Prior Years)	Total
Process Owner				
EMPLOYER	1	0	25	26
EXECUTIVE	0	0	8	8
FINANCE	0	0	3	3
HUMAN RESOURCES	0	1	4	5
INFORMATION SECURITY	2	1	16	19
INFORMATION TECHNOLOGY	0	0	15	15
INVESTMENTS	0	0	4	4
MEMBER SERVICES	1	0	39	40
Total Count:	4	2	114	120

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 83 - 2491 - CIS Controls Assessment

REPORT DATE: 10/09/2024 OPEN

Open Observations: 2

OBSERVATION #5 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	On Schedule
Due Date:		
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:		

OBSERVATION #6 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	On Schedule
Due Date:		
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:		

Project: 86 - 2436 - Quarterly FAS Review (Q3 2024)

REPORT DATE: 12/12/2024 OPEN

Open Observations: 1

OBSERVATION #1 - IN OUR SAMPLE, SIX FAS CALCULATION EXCEL FILES DID NOT HAVE FORMAL EVIDENCE OF A SECONDARY QA (QUALITY ASSURANCE) REVIEW PERFORMED BY STAFF.

Process Owner:	MEMBER SERVICES	On Schedule
Due Date:	03/31/2025	



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."

Action Plan: Management will update our current procedure document (in process with Master Repository Project) to include a secondary review of calculation (if necessary) based on team members experience.
 Management will also add a secondary QA sign off section on the excel calculation template, so it is clear when a secondary QA review is processed.

IA Follow-Up:

Project: 89 - 2433- OCERS Employer Audit

REPORT DATE: 12/12/2024

OPEN

Open Observations: 1

OBSERVATION #2 - 2. THE OCERS DIRECT EMPLOYEE HANDBOOK CURRENTLY LACKS A SECTION DETAILING THE PREMIUM PAY ITEMS AVAILABLE TO OCERS DIRECT EMPLOYEES.

Process Owner: EMPLOYER

Due Date: 12/31/2025

On Schedule

Action Plan: OCERS is set to review the OCERS Direct handbook in 2025. This information will be included.

IA Follow-Up:

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 3 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 5 - Audit of the Benefit Setup Process (2012)

REPORT DATE: 12/04/2012

CLOSED

Closed Observations: 2

OBSERVATION #1 - MANUAL FAS OVERRIDE

Process Owner:	MEMBER SERVICES	
Completion Date:	09/13/2022	MAP Status Unassigned
Action Plan:	Management agreed to the following recommendation: Subsequent changes made to FAS after the initial benefit setup process should require a supervisory approval prior to making an override in the system. Additionally, management should use a system-generated report from V3 that lists all manual overrides to identify all such changes made in the system. Management should review and sign off on each manual override on that report for propriety and accuracy to mitigate the risk of unauthorized or incorrect amounts being entered in the system.	
IA Follow-Up:	IA to confirmed the new QA process reviews all manual FAS overrides with the new 100% accruacy process	

OBSERVATION #8 - MANUAL FAS SUPPORTING DOCUMENTATION

Process Owner:	MEMBER SERVICES	
Completion Date:	09/16/2021	MAP Status Unassigned
Action Plan:	Management agreed to the following recommendation: All manual overrides to data should be fully documented with the staff that made the change, date the change was made, prior amount, revised amount, and reason for the change with supervisory approval documented in V3 in accordance with the current method of maintaining supporting documentation for benefits calculation. Member Services personnel are required to document V3 via note for any member file that requires a manual override.	
IA Follow-Up:	IA to confirmed the FAS Review process contains steps to review the supporting documentation.	

Project: 17 - Audit of OCERS' Due Diligence Process (2015)

REPORT DATE: 08/06/2015

CLOSED

Closed Observations: 2

OBSERVATION #1 - NO DUE DILIGENCE POLICY

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 4 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Process Owner:	INVESTMENTS	
Completion Date:	01/07/2021	MAP Status Unassigned
Action Plan:	Management has agreed to the recommendation: The CIO and his staff should create written procedures that specifically document the steps necessary to conduct adequate due diligence. We concur with the recommendation that written procedures are desirable, and staff is working on the development of a document that would fulfill this objective.	
IA Follow-Up:	The CIO and Investment Team developed Investment due diligence procedural documents including the Contract Due Diligence Checklist Procedure document and the Contract Due Diligence Checklist document.	

OBSERVATION #4 - MANAGER RFP STANDARDIZED QUESTIONING

Process Owner:	INVESTMENTS	
Completion Date:	01/07/2021	MAP Status Unassigned
Action Plan:	Management has agreed to the recommendation: Future RFP questionnaires should include interrogatories regarding a manager's operational infrastructure and negative findings disclosed from their annual external audit. We agree that future RFPs should include standard (first-stage or second stage) provisions and questions that are relatively uniform regarding due diligence, operations, and related legal, regulatory and compliance risks. The cited incident was an oversight that need not recur. Written procedures and a process to review those routinely will be helpful to assure consistency.	
IA Follow-Up:	Investments included in the Contract Due Diligence Checklist document and the Compliance Report document steps to validate operational infrastructure of money managers.	

Project:	8 - Audit of OCERS' Private Equity Managers Abbott Capital and Pantheon (2016)	
REPORT DATE:	03/21/2016	CLOSED
Closed Observations:	1	

OBSERVATION #4 - CONSIDERATION OF ILPA BEST PRACTICES

Process Owner:	INVESTMENTS	
Completion Date:	01/25/2021	MAP Status Unassigned
Action Plan:	OCERS should implement Institute of Limited Partners Association (ILPA) best practices in LPAs with direct investment private equity funds if OCERS goes into direct private equity program. In considering whether OCERS should adopt a direct private equity program, OCERS' Investments management should consider the cost of implementing the ILPA best practices. OCERS investment staff will first work with our private equity fund of funds managers to monitor their use of ILPA guidelines and best practices, as we further our own internal education about these evolving standards.	
IA Follow-Up:	Investment Team developed a guide to track and assess the key legal and ILPA-related terms OCERS negotiates through the private markets investment manager contracting processes.	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 16 - Audit of OCERS' Death Match Process (2016)

REPORT DATE: 06/24/2016

CLOSED

Closed Observations: 6

OBSERVATION #1 - OVERPAYMENT TO DECEASED MEMBERS

Process Owner:	MEMBER SERVICES	
Completion Date:	12/21/2021	MAP Status Unassigned
Action Plan:	The deceased members identified by Internal Audit will be processed immediately according to the specific circumstances of the accounts. Overpayments will be processed according to policy and beneficiaries will be contacted regarding lump sum payment options for refunds. Management will investigate possible options for instituting a multi-step review process to ensure entries are made into V3 or a quarterly/annually comparison of the database with the information from a death match service provider.	
IA Follow-Up:	Member Services has repaid or wrote off \$421,402 of the \$990,694 of the 24 deferred members. Additionally, Member Services has recovered \$16,008 of the \$20,620 from the four deceased payees. Process is in place to review updates from death data vendor. Member Services will provide updates to the remaining overpayments bi-annually to Internal Audit, starting June 2022	

OBSERVATION #2 - MANUAL QUERY OF V3 UNTIL NEW REPORT IS CREATED

Process Owner:	MEMBER SERVICES	
Completion Date:	12/21/2021	MAP Status Unassigned
Action Plan:	The overpayment to the specific member and DRO payee identified by Internal Audit will be dealt with immediately according to current policy. As V3 is currently configured the system will prevent future overpayments from occurring by suspending the benefit once a death date is entered. The items on the overpayment log need to be reconciled with V3 as a post-go live project but it was envisioned that V3 will replace the need for a manual spreadsheet outside of the system. A query or report may be needed during the transition period.	
IA Follow-Up:	Query has been implemented. Recoupment of overpayment to be reviewed biannually with Internal Audit. The Benefit Recoupment Report has been created, refer to Benefit Recoupment Report 2021.pdf	

OBSERVATION #3 - CERTIFICATION LETTERS

Process Owner:	MEMBER SERVICES	
Completion Date:	04/07/2021	MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 6 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Management agreed to the following recommendation: OCERS' management should consider sending a certification letter to payees over a selected age to confirm the status of the payee. Management should consider stopping benefit payments if OCERS does not receive a response after a reasonable number of attempts in order to incentivize the payee to return the letter. OCERS' management should also consider the costs/benefits of hiring a third party to perform random physical alive and well checks with payees that meet a given profile. However clear communication will need to be developed as the payees within this demographic may be the hardest to reach. In addition, the implications to payee's medical insurance needs to be considered any time a benefit is suspended.

IA Follow-Up: After Member Services management discussed formulating a formal policy addressing when such certification letters should be sent and to whom after the result of a cost benefit analysis to be performed. Certification letters are sent to all international payees. Member Services relies on the death match file for updates to domestic members.

OBSERVATION #4 - DEATH DATA VENDORS

Process Owner: MEMBER SERVICES

Completion Date: MAP Status Unassigned

Action Plan: Management agreed to the following recommendation: OCERS management should consider using only death audit vendors that hire external auditors to review its client data security controls. OCERS should require that death audit vendors provide copies of the audit report and the audit results to OCERS on an annual basis for review. OCERS management should consider using the RFF process to compare the services of death audit vendors and obituary review service vendors. Quality of services, price, and data security controls of vendors should be compared.

IA Follow-Up: Management to discuss the approach for obtaining and reviewing vendor security report on an entity wide approach, with a completion date of 6/30/2023. This observation and action plan will be tracked under the ITGC audit

OBSERVATION #5 - MEMBER BANKING INFORMATION WITHIN V3

Process Owner: MEMBER SERVICES

Completion Date: 09/23/2021 MAP Status Unassigned

Action Plan: Management agreed to the following recommendation: To reduce the possibility of fraudulently diverting benefit payments for deceased members, OCERS should implement automated checks and balances within the V3 system to ensure that no one employee can unilaterally change a payee's banking information without supervisory approval. The resulting change to V3 may require an additional change order to reconfigure the V3 system. However, the headline risk to OCERS outweighs the financial cost of making such a change.

IA Follow-Up: Workflow approvals were reviewed by Internal Audit. An audit in member banking to be proposed as a future audit.

OBSERVATION #6 - PRO-RATING FINAL PAYMENT FOR DECEASED MEMBERS

Process Owner: MEMBER SERVICES

Completion Date: 02/25/2021 MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 7 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan:	<p>OCERS' management should consider the costs versus benefits of prorating a deceased member's final monthly benefit payment based upon the actual date of death versus making a full payment. V3 is not configured to calculate a prorated final benefit payment and a prorated initial continuance benefit payment effective the day after death for the remainder of the month. OCERS would have to pay additional costs to have Vitech reconfigure V3 and for OCERS' employees and consultants to test the changes. The estimated cost of reconfiguring and testing V3 to prorate the final benefit payment, the initial continuance payment, and payroll deductions is estimated by Vitech at \$144,000. In addition, management estimates that testing of the system changes would need to be done by staff or consultants at an estimated cost of \$150,000.</p> <p>A prorated final benefit policy would also result in more overpayments for Member Services to pursue for collection since the benefit payment is paid on the first of the month. Under current policy, deaths reported to OCERS in the month following death allows enough time for Member Services to terminate the benefit with no need to prorate. Under a prorated policy, it would be impossible for Member Services to prorate the final payment on the 1st of the month if the death was reported in the month after death. Member Services would possibly need to cross train staff in collection efforts to accommodate such an increase in collection efforts.</p> <p>Management Response Management considered the costs versus benefits of adopting a proration of the final benefit payment policy, but determined to continue the current practice of paying in full the final month's benefit. Prorating the member's final payment and survivor continuance first payment introduces additional complexity to the administration of the system and would require additional staff in Member Services and possibly Finance, in addition to the V3 configuration changes. Retiree payroll is typically</p>
IA Follow-Up:	<p>Management considered the costs versus benefits of adopting a proration of the final benefit payment policy, but determined to continue the current practice of paying in full the final month's benefit.</p>

Project: 20 - Audit of OCERS' Service Credit Purchase Process (2016)

REPORT DATE: 11/29/2016

CLOSED

Closed Observations: 1

OBSERVATION #1 - WORK IN PROCESS REPORTING

Process Owner:	MEMBER SERVICES	
Completion Date:	04/07/2021	MAP Status Unassigned
Action Plan:	OCERS' management agrees to initiate discussions with Vitech for best cost-benefit solutions to building work-in-process reporting to track the status of buybacks throughout its business processes to provide additional management oversight of staffing and resources; track compliance with business goals; and improve customer service response times to members.	
IA Follow-Up:	IA has verified that OCERS has implemented a work-in-process tracking database within SharePoint.	

Project: 26 - Audit of Orange County Fire Authority (2018)

REPORT DATE: 10/23/2018

CLOSED

Closed Observations: 1

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 8 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



OBSERVATION #6 - V3 CONTRIBUTION RATE CONFIGURATIONS SOD - THERE IS NOT A PROPER SEGREGATION OF DUTIES WITHIN OCERS' IT DIVISION IN REGARDS TO THE CONFIGURATION OF CONTRIBUTION RATES IN V3.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	01/11/2024	MAP Status Unassigned
Action Plan:	Management agreed to the following recommendation: OCERS' management should re-assign the duties of configuring updated rates in V3 from OCERS' Director of IT to the appropriate personnel for cross-training, process documentation, and backup purposes. The revised process will encompass multiple departments, and will segregate duties related to preparing the rate schedules, data input into V3 and verification/audit of contribution rates.	
IA Follow-Up:	IA confirmed the delegation of the configuration uploads to the IT Programming team and the review by Member Services of the updates to the pension administration system.	

Project: 22 - Audit of Orange County Superior Court Payroll Transmittal (2018)

REPORT DATE: 11/08/2018

CLOSED

Closed Observations: 1

OBSERVATION #4 - SUPERIOR COURT'S HR DEPARTMENT DOES NOT HAVE POLICIES AND PROCEDURES IN PLACE TO DETERMINE IF THE INDEPENDENT CONTRACTOR STATUS FOR ITS INDEPENDENT CONTRACTORS COMPLIES WITH IRS RULES

Process Owner:	EMPLOYER	
Completion Date:	01/05/2022	MAP Status Unassigned
Action Plan:	Superior Court to review independent contractors working for court reporting services, court language services and court technology to determine if their independent contractor status complies with IRS rules defined for independent contractors.	
IA Follow-Up:	Superior Court no longer use independent contractors as court reporters. New employee classification/class spec for "Assignment Court Reporter" was created.	

Project: 31 - Disability Payment Audit (2018)

REPORT DATE: 01/28/2019

CLOSED

Closed Observations: 1

OBSERVATION #1 - DISABILITY PAYMENT CALCULATION

Process Owner: MEMBER SERVICES

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."

Completion Date:	01/05/2022	MAP Status Unassigned
Action Plan:	Member Services will be continuing to review with increased diligence or newly implementing to ensure accuracy of Disability benefits that are setup: <ul style="list-style-type: none"> • Ensure that all disability benefits are peer audited (FAS calc) before benefit setup, including disability recalculations (from Service Retirement to SCD, Service Retirement to NSCD, NSCD to SCD) • Verify selected data points on the "New Benefit Setup Validation Report" (which will contain a subset of 16 reports – expected to be ready by Q3 2019) • Additional training will be provided to the RPS assigned to the disability department (this was a new position in 2018). These types of benefits are more specialized that regular retirement setups, and the Disability RPS will be trained to look for specific factors that affect the benefit, such as gaps in service, measuring period compression, manual calculations of FAS, recalculation issues. 	
IA Follow-Up:	IA confirmed action plan has been implemented. A new Disability Process has been implemented along with the appropriate training.	

Project:	6 - 1901 - Finance Contributions audit	
REPORT DATE:	05/16/2019	CLOSED
Closed Observations:	1	

OBSERVATION #1 - A FORMAL PERIODIC REVIEW OF PROPER USER ACCESS TO OCERS APPLICATIONS AND NETWORK IS NOT DOCUMENTED BY THE APPROPRIATE MEMBERS OF THE BUSINESS.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	08/07/2024	On Schedule
Action Plan:	Per IT Governance and Information Security action items to address Center for Internet Security (CIS) Control 16: Account Monitoring and Control, OCERS IT and the Executive management team are establishing the following: <ol style="list-style-type: none"> 1. Develop Account Management and Access Control Policies. 2. Create an annual User Account review process and supporting documentation. 3. Setup means for staff to review and enter data in SharePoint with associated workflow to complete and track reviews initiated with IT managed systems. 	
IA Follow-Up:	IT/InfoSec has: <ol style="list-style-type: none"> 1. Developed the Account Management and Access Control Policies. 2. Created an annual User Account review process and supporting documentation. 3. Established a means for staff to review data 	



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 36 - 1943 2019 BCDR Audit

REPORT DATE: 10/17/2019

CLOSED

Closed Observations: 2

OBSERVATION #3 - A FORMAL PROCESS INVOLVING CRITICAL OCERS STAKEHOLDERS IS NOT IN PLACE TO TEST THE RECOVERY OF DEPENDENT IT APPLICATIONS.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	04/10/2024	On Schedule
Action Plan:	OCERS IT will formalize and adopt a new Business Continuity and Disaster Recovery test plan that will include test activities, confirmation, and sign-off by the various business units within OCERS.	
IA Follow-Up:	IT developed a test plan that will require coordination with management to perform testing for IT managed systems. This includes an assessment form and a department validation forms to be completed by management participants.	

OBSERVATION #6 - 6. RECOVERY PROCEDURES FOR DEPENDENT IT APPLICATIONS ARE NOT DOCUMENTED IN THE RECOVERY PLANS.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	04/10/2024	On Schedule
Action Plan:	End User documents are being developed for the purpose of providing recovery instructions to the crisis management team, in the event IT staff are not available in the event of an emergency. The documents will provide simple easy to follow instructions on how to failover and/or recover sites or systems in the event of a technology failure. These documents will be included in OCERS IT Backup and Recovery test plan stored in Catalyst to ensure procedures are complete and can be followed by non- IT staff	
IA Follow-Up:	Documentation of the recovery process was provided. IT and InfoSec noted that IT staff with the appropriate level of access would be needed for the recovery process and that there are enough IT and InfoSec staff for BCDR situations. Management will still develop documented procedures for recovery but geared towards IT Staff.	

Project: 44 - 1944 - Finance Benefits Audit

REPORT DATE: 01/13/2020

CLOSED

Closed Observations: 1

OBSERVATION #2 - FINANCE DOES NOT SYSTEMATICALLY DELETE V3'S ACH FILES CONTAINING BENEFICIARIES' BANKING INFORMATION FROM LOCAL HARD DRIVES.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 11 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Process Owner:	FINANCE	
Completion Date:	03/14/2022	MAP Status Unassigned
Action Plan:	Management will establish procedures to delete copies of the ACH text files from local hard drives after a copy of the file has been uploaded to Wells Fargo. Finance will work with IT and Vitech to consider the cost/benefit of changing the ACH file process to directly upload an ACH file once it has been created in V3 and directly downloading the file to a secured network folder in the Finance directory.	
IA Follow-Up:	IA confirmed with the Finance team the deletion of the ACH file from the local hard drive is now being performed by management. IA reviewed the procedures updated to reflect this practice. Due to COVID, the cost/benefit analysis has been moved to 2021. 2/3/22 - OCERS IT was able to modify the PM Export file process. The PM Export is now going to be run as a batch export file and will automatically save into a new secured folder location in the Finance folder on the F drive. In addition, access to run the PM Export is restricted to the Finance Accountant Auditor, Senior Accountant Auditor and Supervisor roles 3/14/22 - IA was able to confirm the PM Export file automatically uploads to a secured folder with limited access. IA also confirmed a documented procedure exists.	

Project:	40 - 1945- FAS Pay Items Audit	
REPORT DATE:	06/04/2020	CLOSED
Closed Observations:	2	

OBSERVATION #1 - A FORMAL RECONCILIATION WAS NOT PERFORMED TO ENSURE THE PAY ITEMS REPORTED TO THE BOARD ACCURATELY AND COMPLETELY CORRESPONDED WITH THE CONFIGURATION IN V3.

Process Owner:	MEMBER SERVICES	
Completion Date:	09/16/2021	MAP Status Unassigned
Action Plan:	Member Services will address the variances noted in the audit, which includes making the appropriate configuration updates to the V3 system, communicating the updates to the Employers and following procedures in the OCERS' Overpaid and Underpaid Plan Contributions Policy in regards to the over and underpayment of contributions of the variances noted. At the next update to the Board, Member Services will include the corrections identified in this audit for pensionable attributes of relevant pay items. Going forward, Member Services will develop a process to perform a full reconciliation of the pay item file presented to the Board with the pay item configurations in the V3 system periodically, at least prior to the annual presentation to the Board to ensure accurate and complete reporting of pay items to the Board. Any discrepancies identified by the reconciliation will be addressed as needed.	
IA Follow-Up:	Internal Audit reviewed updated procedure document and annual reconciliation file.	

OBSERVATION #3 - A PROCESS DOES NOT EXIST TO IDENTIFY UPDATES TO EMPLOYER DOCUMENTATION THAT MAY IMPACT THE LIST OF PAY ITEMS.

Process Owner:	MEMBER SERVICES	
Completion Date:	03/14/2023	MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM	 On Schedule to complete MAP	Doc. No. 0080-0120-R0001 Page 12 of 46
Executed By: OCERS\plam	 Missed Due Date (1st Time), planned to complete by Revised Due Date	
	 Missed Due Date (2nd Time) since latest Revised Due Date	



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Member Services is in the process of documenting all current MOU's and will draft an update to the pay item review procedure to include a section on monitoring MOU's for adjustments made by Employers to ensure Employers have obtained OCERS approval prior to implementing a new pay item.

Currently, the Employer is required to submit a "pay item request form" to OCERS for approval in order to add a new or adjust an existing pay item. This is required to be done at least two pay periods prior to implementation of the pay item in the Employer payroll. If however an Employer attempts to pass a pay item that has not been added for that Employer, the system will produce an error for the Employer when they submit the payroll. This process assists Member Services in monitoring the implementation of pay items directly by the Employer.

IA Follow-Up: IA confirmed a process and supporting documentation was implemented.

Project: 39 - 1971-IT General Controls

REPORT DATE: 06/04/2020

CLOSED

Closed Observations: 3

OBSERVATION #1 - ADMINISTRATOR ACCESS GRANTED TO THE FINANCIAL REPORTING AND INTRANET PORTAL APPLICATIONS PRESENT A HIGHER THAN NORMAL RISK DUE TO SEGREGATION OF DUTIES CONCERNS.

Process Owner: INFORMATION TECHNOLOGY

Completion Date: 01/13/2022

MAP Status Unassigned

Action Plan: As OCERS is in the process of issuing an RFP for a new financial accounting system, we will defer changes to our current financial accounting system, and focus on building a secure segregated system with the appropriate controls and check and balances as part of the new system to be implemented in 2021.

Due to the size of the OCERS IT Programming group, team members share many administrative responsibilities and needs to be able to cover for other team member assignments and responsibilities when out of the office.

Both the intranet portal and the intranet portal source code repository provide account auditing features that track all changes are made, along with the user that made the change. This information is reported daily to the IT Programming Supervisor, so that he and the IT Management team have complete visibility into any administrative operations that are performed and by whom.

In addition to this audit trail, we have implemented a mandatory workflow process with each IT Programming Request that requires the review of a secondary team member when making changes to the intranet portal or source code in the intranet portal source code repository. This serves as an additional validation and backup to protect against segregation of duties concerns.

IA Follow-Up: New financial accounting system implementation was moved to 2021 with move to production in Jan 2022.
 IA confirmed that the Intranet Portal has restricted administrative access.
 IA also confirmed the new financial accounting system has restricted administrative access

OBSERVATION #2 - OCERS SHOULD FORMALIZE A PROCESS TO ANNUALLY OBTAIN AND REVIEW SOC REPORTS FOR RELEVANT IT VENDORS.

Process Owner: INFORMATION TECHNOLOGY

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Completion Date:	08/23/2023	MAP Status Unassigned
Action Plan:	OCERS has developed criteria to identify IT vendors and technology service providers' requiring SOC2 reports, and will enhance our systems to notify staff to request and review SOC2 reports annually. Process and review documentation is being developed along with updates to our procurement process to mandate SOC2 reports as a deliverable	
IA Follow-Up:	Enhancements have been made to the vendor management system. Processes and Procurement policy needs to be formally updated.	

OBSERVATION #3 - OCERS DOES NOT MAINTAIN DATA FLOW DIAGRAMS OR OTHER DOCUMENTATION OF INFORMATION FLOW BOTH INTERNALLY AND TO EXTERNAL PARTIES.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	12/11/2024	On Schedule
Action Plan:	Phase one of OCERS Data Classification project, will identify data elements in our V3 system and include the creation of data flow diagrams for data elements classified as "sensitive". In addition, OCERS IT Programming team will develop data flow diagrams of their internal datasets and reporting platform. Additional data flow diagrams may be developed along with process flow diagrams as part of future lean process improvements.	
IA Follow-Up:	IA obtained from IT data flow diagrams and other documentation to illustrate where sensitive data, such as SSNs, that reside and flow both within the PAS and to/from external parties.	

Project: 42 - 2032 - Actuarial Extract Audit

REPORT DATE: 10/13/2020

CLOSED

Closed Observations: 7

OBSERVATION #1 - 1. THE PENSION ADMINISTRATION SYSTEM'S ACTUARIAL EXTRACT REPORTING DOES NOT EXTRACT THE CORRECT STATUS (E.G. ACTIVE, DEFERRED, RETIRED, TERMINATED) OF A MEMBER UNDER CERTAIN SCENARIOS, RESULTING IN THE NEED TO MANUALLY CORRECT THE ACTUARIAL EXTRACT REPORT

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	09/22/2021	MAP Status Unassigned
Action Plan:	OCERS is working with pension administration vendor to correct issues associated with the member status logic used for the actuarial export and subsequent data cleanup.	
IA Follow-Up:	Member status logic recoding is complete and deployment launched.	

OBSERVATION #2 - 2. IT PROGRAMMING PERFORMS LOGICAL TESTING OF THE PROGRAMMING CODE BEHIND ITS ACTUARIAL EXTRACT VALIDATION PROCESS BUT DOES NOT KEEP FORMALIZED DOCUMENTATION EVIDENCING THE TESTING.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	03/11/2021	MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 14 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: The IT Programming team will formalize and document the process by which logical testing of our actuarial validation code will be performed.
IA Follow-Up: Formalized testing process has been documented and reviewed by IA

OBSERVATION #3 - 3. FORMAL DOCUMENTATION OF THE APPROVAL OF VALIDATION PROGRAMMING CODE CHANGES DOES NOT EXIST.

Process Owner: INFORMATION TECHNOLOGY
Completion Date: 03/11/2021 MAP Status Unassigned
Action Plan: The IT Programming team will formalize and document the process of how actuarial extract validation code changes will be approved, including how all approvals will be tracked and logged within our system.
IA Follow-Up: IT Programming has formalized the code change validations process.

OBSERVATION #4 - NUMERICAL THRESHOLDS UNDER WHICH FURTHER INVESTIGATION OF VALIDATION RESULTS ARE NO LONGER CONSIDERED NECESSARY ARE NOT FORMALLY DEFINED.

Process Owner: INFORMATION TECHNOLOGY
Completion Date: 01/11/2024 MAP Status Unassigned
Action Plan: The IT Programming team with work with OCERS Management to develop acceptable thresholds to use when reviewing the actuarial validation results.
IA Follow-Up: IT has developed threshold recommendations and updated the related procedures.

OBSERVATION #5 - 5. MEMBER SERVICES DOES NOT HAVE POLICIES AND PROCEDURES RELATED TO THE USE OF THE PENSION ADMINISTRATION SYSTEM MEMBER DATA VALIDATION QUERIES.

Process Owner: MEMBER SERVICES
Completion Date: 05/15/2023 MAP Status Unassigned
Action Plan: The Member Services team will document and formalize policies and procedures related to the pension administration system data queries created by the OCERS IT Department. We will also document the personnel structure responsible for the process as well as the timing and scheduling cycles for the annual review.
IA Follow-Up: Internal Audit confirmed a Member Services procedural document was created.

OBSERVATION #6 - 6. A MINOR VARIANCE NOTED AND ADDRESSED DURING THE VALIDATION PROCESS WAS NOT ACCURATELY UPDATED IN THE DATA EXTRACT FILE SENT TO THE ACTUARY.

Process Owner: INFORMATION TECHNOLOGY
Completion Date: 03/11/2021 MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 15 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: The IT Programming team will enhance its process to incorporate all validation review updates and related data cleanup changes to ensure all updates are included in the final export to OCERS Actuary.
IA Follow-Up: Data cleanup process has been updated and data validation has occurred.

OBSERVATION #7 - 7. OCERS ACTUARIAL EXTRACT PROCESSING GUIDE DOES NOT DESCRIBE INFORMATIONAL QUERIES WHICH DO NOT REQUIRE INVESTIGATION UNLESS REQUESTED BY SEGAL.

Process Owner: INFORMATION TECHNOLOGY
Completion Date: 03/11/2021 MAP Status Unassigned
Action Plan: The IT Programming team will add a section to the Actuarial Extract Processing guide that will describe the additional Informational queries available to OCERS staff to preview potential member datasets based on annual actuarial review question posed by OCERS actuary.
IA Follow-Up: IA confirmed the Actuarial Extract Processing guide has been updated with the informational queries description.

Project: 33 - 2090 - Vulnerability and Patch Management

REPORT DATE: 03/22/2021

CLOSED

Closed Observations: 2

OBSERVATION #1 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY
Completion Date: 08/07/2024 On Schedule
Action Plan: Details Removed - Discussed in Closed Session
IA Follow-Up: Information Security provided the related policies

OBSERVATION #2 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION TECHNOLOGY
Completion Date: 05/27/2021 MAP Status Unassigned
Action Plan: Details Removed - Discussed in Closed Session

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



IA Follow-Up: Closed

Project: 47 - 2020 - Continuous Audit of Final Average Salary Calculations (Q3/Q4 2020)

REPORT DATE: 03/22/2021

CLOSED

Closed Observations: 2

OBSERVATION #1 - 1. INTERNAL AUDIT NOTED AN 8% ERROR RATE (SIX ERRORS) WITH THE 75 FAS CALCULATIONS SAMPLED FROM THE 3RD AND 4TH QUARTERS OF 2020.

Process Owner: MEMBER SERVICES

Completion Date:

MAP Status Unassigned

Action Plan: Member Services has reviewed and is in the process of addressing the recalculations for members identified by Internal Audit during their review. Member Services Management has also taken the following steps which are further detailed in our "Member Services Management Quality Assurance Review Final Average Salary Q1-Q2 2020 Report.docx" document provided to the committee (Action Item A-5).

1. Reorganization of the Retirement Program Specialist (RPS) department.
2. Development of the OCERS Retirement Transaction Tool.
3. Development of detailed written procedures for the entire Retirement Transaction Process.
4. Retrained the RPS teams on the newly developed Retirement Transaction Tool.
5. Development of a fully focused Quality Assurance Review Team and Reporting process.
6. Random Sampling of Retirement Transactions by Member Services Management Team.

IA Follow-Up: As part of the continuous audit for the FAS calculation, Internal Audit noted the MAP was completed during the July 1 payroll review.

OBSERVATION #2 - 2. THE FAS SUPPORTING DOCUMENTATION FOR THREE MEMBERS NEEDED TO BE UPDATED IN THE PENSION ADMINISTRATION SYSTEM (NO FAS IMPACT).

Process Owner: MEMBER SERVICES

Completion Date: 04/02/2021

MAP Status Unassigned

Action Plan: Member Services has reviewed and updated the member files for the calculation documents for members identified by Internal Audit during their review. Member Services Management has also implemented a checklist within the new tool mentioned above.

IA Follow-Up: Internal Audit noted the checklist was included in the new FAS tool.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 17 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 48 - 2132 - Continuous Audit of Final Average Salary Calculations (Q2 2021)

REPORT DATE: 06/04/2021

CLOSED

Closed Observations: 2

OBSERVATION #1 - 1. INTERNAL AUDIT NOTED A 6.7% ERROR RATE (FOUR ERRORS) OUT OF THE 60 FAS CALCULATIONS SAMPLED FROM THE 2ND QUARTER OF 2021.

Process Owner:	MEMBER SERVICES	
Completion Date:	05/20/2021	MAP Status Unassigned
Action Plan:	<p>Member Services Management team takes all errors very seriously. As discussed before, we reorganized our team and implemented a full Quality Assurance process to review all payroll transactions and perform recalculations on any member's account where we found an error. We are reviewing the root cause of all errors and we are providing ongoing training on the errors found each month. We are providing direct feedback to the specific team members who processed the original calculations where errors occurred. We are also reporting up to senior management weekly on the results of our efforts.</p> <p>As to the fourth error, we are working with ViTech, our V3 pension administration system vendor to develop a solution to this issue. We are also working with our team to review any accounts with similar employment history to ensure this error does not occur in the future until we can have the systematic issue fixed in V3. Upon our initial review of all member retirements that have been processed since the implementation of V3 (2016 forward), it is believed to impact approximately 11 members, but the investigation is ongoing. We will provide an update on the final number of members affected at the time of the June Audit Committee Meeting.</p> <p>Member Services is also providing training to the team on how to identify members with this potential issue to ensure additional members are not impacted in the future until the fix in V3 is made</p>	
IA Follow-Up:	Internal Audit reviewed the ViTech submission and confirmed with Member Services of the additional training.	

OBSERVATION #2 - 2. THE FAS SUPPORTING DOCUMENTATION FOR TWO MEMBERS NEEDED TO BE UPDATED IN THE PENSION ADMINISTRATION SYSTEM (NO FAS IMPACT).

Process Owner:	MEMBER SERVICES	
Completion Date:	05/20/2021	MAP Status Unassigned
Action Plan:	<p>Member Services Management team is providing feedback to our team and the 2 specific team members who did not upload the fully completed supporting documentation to the V3 system. We will continue to reiterate the importance of maintaining the fully completed documentation in the members' files in V3 and will have the supervisor team monitor compliance.</p>	
IA Follow-Up:	Internal Audit confirmed the documents have been uploaded and the feedback to the team members have been provided.	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 18 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 55 - 2135 - Quarterly FAS Review (Q4 2021)

REPORT DATE: 10/04/2021

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. INTERNAL AUDIT NOTED AN 8% ERROR RATE (SIX ERRORS) WITH THE 75 FAS CALCULATIONS TESTED FROM THE 3RD QUARTER OF 2021.

Process Owner: MEMBER SERVICES

Completion Date: 10/01/2021

MAP Status Unassigned

Action Plan: Member Services has recalculated the 6 accounts and made corrective retroactive payments/adjustments to each of the members in accordance with OCERS Overpaid and Underpaid Plan Benefits Policy. The first 5 members were corrected with the 9/1/2021 payroll and the last account was corrected on the 10/1/2021 payroll. Member Services RPS management team formed a committee to assist in developing new controls. One specific solution that came from this committee was the need to have a consistent process for them to follow to sort through the pay data used in determining FAS pay items. Member Services management developed new controls within the FAS Calculation Tool that incorporate macros to help sort and organize the work history for pay items to ensure all team members are working in a consistent process and to make it easier to identify the pay items to include in the FAS. We implemented and trained the RPS team on the new process in September.

Member Services management has also enacted version control on the FAS Calculation tool to ensure it is easy to identify if calculations are performed on an outdated file. Member Services management will continue to find new ways to eliminate errors in this process and implement them quickly with appropriate training and documentation on the processes for the team.

IA Follow-Up: Member Services shared the updated version of the FAS excel tool.

Project: 56 - 2133 - Dependent Survivor Eligibility Audit

REPORT DATE: 10/04/2021

CLOSED

Closed Observations: 4

OBSERVATION #1 - 1. OCERS DOES NOT HAVE A FORMALIZED AND SYSTEMATIC PROCESS TO ADDRESS SURVIVOR BENEFITS UNCLAIMED OVER AN EXTENDED PERIOD OF TIME.

Process Owner: MEMBER SERVICES

Completion Date: 01/05/2022

MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 19 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan:	Member Services Management has worked with our IT partners to develop two reports that will alert us if we have a member that has a death date entered but does not have a survivorship processed. This will help us catch this type of oversight in the future. A process will be developed to monitor the reports/alerts and take appropriate action. Member Services will also research with ViTech to see if it would be possible to have an automated letter mailed out each month to a member's beneficiaries once a death date is entered and to conclude when a survivorship is processed to the beneficiaries. This will help ensure member beneficiaries are made aware of their possible benefit. 2 Reports are as follows: <ul style="list-style-type: none"> • Deceased Retirees with No Associated Burial Benefit nor Survivorship benefit established. • Deceased Retirees with an Associated Burial Benefit but no Survivorship benefit established.
IA Follow-Up:	Internal Audit confirmed the reports have been implemented

OBSERVATION #2 - 2. UPON REVIEWING A SURVIVOR'S BENEFIT PAYMENT, WE NOTED ERRORS WITH THE DECEASED MEMBER'S BENEFIT PAYMENT HISTORY FROM 2002 TO THE MEMBER'S DEATH IN 2018.

Process Owner:	MEMBER SERVICES	
Completion Date:	01/26/2023	MAP Status Unassigned
Action Plan:	1. Per the OCERS' Overpaid and Underpaid Plan Benefits Policy, OCERS will not recoup the overpaid funds from the surviving spouse's continuance. 2. Current procedures requires Member Services to perform a comparison of the benefit components on both member and survivor to identify any possible discrepancies at the time of the survivorship establishment. We will review our current procedures to see if there are any additional steps, we can take to ensure we do not miss this type of discrepancy moving forward. We will also update our team and provide training specific to this issue.	
IA Follow-Up:	Confirmed procedures were updated for Member Services to verify COLA and Pension amounts for survivor benefit payments.	

OBSERVATION #3 - A LUMP SUM BENEFICIARY PAYMENT TO A DECEASED DRO SURVIVOR PAYEE'S ESTATE WAS OVERPAID BY \$200.

Process Owner:	MEMBER SERVICES	
Completion Date:	04/25/2024	On Schedule
Action Plan:	Member Services Management will perform a root cause analysis and develop a QA process specific to the Manual Tertiary Applications. This type of application is very rare and is not fully developed and automated in V3. We will work to incorporate this in either a V3 upgrade or the new PAS system in the future.	
IA Follow-Up:	IA reviewed new QA Process document	

OBSERVATION #4 - 4. A MEMBER'S DISABILITY APPLICATION WAS NOT LOCATED IN THE MEMBER'S V3 RECORDS.

Process Owner:	MEMBER SERVICES	
Completion Date:	03/16/2022	MAP Status Unassigned
Action Plan:	Member Services/Disability team will ensure all the documents are uploaded before completing the Required Proof Doc Checklist. Member Services will validate at the time of disability recalculation that the required disability documentation is within the V3 member file.	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



IA Follow-Up: IA confirmed the disability documents have been uploaded to V3 and a process was implemented to validate documents have been uploaded.

Project: 57 - 2231 - SSA Employer Audit

REPORT DATE: 03/30/2022

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. THE JOB TITLE IN THE OCERS PENSION ADMINISTRATION SYSTEM (PAS) RECORDS FOR A SOCIAL SERVICES AGENCY RETIREE IN OUR SAMPLE DID NOT REFLECT THE RETIREE'S ACTUAL JOB TITLE.

Process Owner: MEMBER SERVICES

Completion Date: 01/30/2023

MAP Status Unassigned

Action Plan: Member Services Employer Payroll (EP) Management Team will perform a one-time audit of the records between OCERS and all employers supported through the County (Not Just SSA). Once Complete, updates will be sent to OCERS IT to make the necessary changes. After IT makes the changes to the system, a member of the EP Team will verify that the changes were successfully implemented. Ongoing, accuracy validation of the data at the time a member retires is currently performed and is also part of our updated Quality Assurance Process initiated in 2021. As a result of our updated quality assurance program and the fact that we rarely receive new or changed Bargaining Units and Job Class, Management is recommending we continue to review the quality for these records at the time of retirement. We will perform another global reconciliation at the time we perform a migration from the current pension administration system to our new pension administration system in the coming years.

IA Follow-Up: Internal Audit confirmed the reconciliation of job title and job codes between the County and OCERS PAS. The issue identified has been corrected.

Project: 58 - 2211 - Investment Manager Fee Report

REPORT DATE: 03/30/2022

CLOSED

Closed Observations: 1

OBSERVATION #1 - EVIDENCE OF MANAGEMENT REVIEW OVER THE PREPARATION OF THE FEE REPORT AND THE UNDERLYING EXCEL SCHEDULE USED TO HELP COMPILE THE REPORT IS NOT FORMALIZED AND RETAINED

Process Owner: INVESTMENTS

Completion Date: 09/12/2022

MAP Status Unassigned

Action Plan: We acknowledge and concur with the observation. We believe that documenting the process will strengthen Investment Division's procedures while also providing a strong audit trail.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 21 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



IA Follow-Up: Internal Audit reviewed the Fee Report Procedure and signoff for the 2021 Annual Fee Report presented at the August 2022 Investment Committee meeting.

Project: 59 - 2232 - Quarterly FAS Review (Q1 2022)

REPORT DATE: 03/30/2022

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. INTERNAL AUDIT NOTED A 4.0% ERROR RATE (TWO ERRORS) WITH THE 50 FAS CALCULATIONS SAMPLED FROM THE 1ST QUARTER OF 2022

Process Owner: MEMBER SERVICES

Completion Date: 01/26/2023

MAP Status Unassigned

Action Plan: Member Services (M.S.) Management team investigated the first error reported by Internal Audit for this quarter, and we determined that the original data came to OCERS from CalPERS in an Excel spreadsheet that contained improper formatting for the salary records. M.S. management has engaged the leadership team at CalPERS for the department that prepares this information to inform them of the formatting error. We have also reviewed additional member accounts for which we had received salary information from CalPERS to determine if any other accounts had a similar issue. All of the other accounts we reviewed contained spreadsheets that contained merged fields similar to this account, but they were formatted properly and correctly reported final average salary. We are also training our staff to be aware of the possibility of formatting errors from any outside agency using Excel to report data to OCERS.

Regarding the second account with an error, M.S. Management team is working with ViTech to determine the reason for the error and fix the PAS software to ensure it is following the configuration settings properly. We are also working to query the PAS software to see if there are any other accounts that may have been affected in a similar way to this account.

IA Follow-Up: Internal Audit confirmed the training was performed and a JIRA ticket was created to identify the proration issue.

Project: 60 - 2261 - Procurement Audit

REPORT DATE: 10/03/2022

CLOSED

Closed Observations: 8

OBSERVATION #1 - OCERS DID NOT COMPLY WITH OCERS PROCUREMENT AND CONTRACTING POLICY (POLICY) REGARDING CONTRACTS AWARDED TO TWO DIFFERENT VENDORS.

Process Owner: EXECUTIVE

Completion Date: 01/11/2024

MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 22 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan:
 A. Management will communicate with all Executives the requirements for issuing an RFP and will coordinate the RFP's per Policy requirements.
 B. Management will propose changes to the Procurement Policy to include a requirement of the Contracts Administrator to educate staff and confirm Policy compliance.
 C. Proof of bids and competitive price comparisons will be retained in the Contracts Management System ("CMS") for future reference

IA Follow-Up: IA confirmed management developed the training, updated the Policy and retained documents in the CMS.

OBSERVATION #2 - THE DUE DILIGENCE WAS NOT CONSISTENTLY PERFORMED OR DOCUMENTED BY THE CONTRACT ADMINISTRATOR, AS PER OCERS BUSINESS PRACTICES, FOR THREE VENDORS IN OUR SAMPLE:

Process Owner: EXECUTIVE

Completion Date: 01/30/2023

MAP Status Unassigned

Action Plan: A. Management will document and implement a process to ensure due diligence is performed prior to the execution of contracts and that will account for instances that might occur whereby a contract is signed before due diligence is completed.

IA Follow-Up: IA confirmed a new due diligence process was implemented. Additional samples were tested.

OBSERVATION #3 - AUTHORIZING SIGNATURES, AS REQUIRED BY THE POLICY, WERE NOT OBTAINED ON FIVE CONTRACTS WITHIN OUR SAMPLE.

Process Owner: EXECUTIVE

Completion Date: 04/20/2023

MAP Status Unassigned

Action Plan:
 A. Management will recommend changes to the Procurement and Contracting Policy to include a duty of the Contract Administer to ensure the appropriate signatures for contracts are obtained.
 B. In an instance where the Procurement and Contracting Policy is not followed, Management will address these non-compliance issues through the Employee Evaluation and Discipline practices as noted in the Employees Handbook.

IA Follow-Up: IA confirmed the Policy was updated with the provision for the Contract Administrator to ensure signatures comply with signature requirements.

OBSERVATION #4 - THE LEGAL DIVISION'S REVIEW WAS NOT OBTAINED FOR AN IT CONSULTANT'S CONTRACT AWARDED IN 2021. (CONTRACT VALUE OF \$126,000).

Process Owner: EXECUTIVE

Completion Date: 09/12/2022

MAP Status Unassigned

Action Plan: A. All contracts, including those that do not deviate from OCERS' form of contract, are now forwarded to the Legal Division for review. In addition, the Legal contract approval is being retained for future reference.

IA Follow-Up: Internal Audit reviewed sample of Legal approval of final contracts

OBSERVATION #5 - FOR TWO VENDORS IN OUR SAMPLE, THE CERTIFICATE OF INSURANCE (COI) PROVIDED BY THE VENDOR DID NOT MEET THE DOLLAR AMOUNT COVERAGE AS SPECIFICALLY STATED IN THE EXECUTED CONTRACT.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 23 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Process Owner:	EXECUTIVE	
Completion Date:	01/30/2023	MAP Status Unassigned
Action Plan:	A. Management will implement procedures to ensure Certificates of Insurance are in accordance with the vendor contracts. In those cases where the Insurance Certificate does not meet the contractual requirements, the contract stake holder and Legal Division will be consulted for additional action.	
IA Follow-Up:	Internal Audit confirmed COIs were obtained for an additional sample.	

OBSERVATION #6 - POLICY IS ABSENT GUIDANCE OF WHEN A CONTRACT IS NEEDED AND HOW TO MONITOR ROUTINE ITEMS THAT DO NOT WARRANT A CONTRACT.

Process Owner:	EXECUTIVE	
Completion Date:	04/20/2023	MAP Status Unassigned
Action Plan:	Policy Issue: Management will work with the Legal Division to identify circumstances where a contract is required and make recommendations to update the Procurement and Contracting Policy as deemed appropriate.	
IA Follow-Up:	IA confirmed the Policy was updated to define when a written contract was required.	

OBSERVATION #7 - UPON REVIEW OF OCERS' CONTRACT MANAGEMENT SYSTEM (CMS), WE NOTED DATA ENTRY ERRORS WITH SIX VENDORS IN OUR SAMPLE.

Process Owner:	EXECUTIVE	
Completion Date:	01/24/2023	MAP Status Unassigned
Action Plan:	Management has approval to hire an additional Team Member in this department. Review procedures will be created and implemented at that time.	
IA Follow-Up:	New Senior Manager hired. Internal Audit reviewed the Data Entry review schedule provided by management.	

OBSERVATION #8 - 8. WE NOTED POTENTIAL ROOM FOR IMPROVEMENT WITH EITHER THE POLICY OR WITH THE ADDITION OF NEW PROCEDURES.

Process Owner:	EXECUTIVE	
Completion Date:	04/20/2023	MAP Status Unassigned
Action Plan:	Policy Issue: A. Management will recommend changes to the Procurement and Contracting Policy regarding the approvals required for a contract whose value is unknown at the time of execution. B. Management will recommend changes to the Procurement and Contracting Policy to clarify proper approval of Named Service Providers C. Management will implement a process to track diverse and/or minority owned businesses in an RFP distribution sheet.	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."

IA Follow-Up: IA confirmed the Policy was updated to address instances when a contract value is not known at the time of execution, and to clarify the proper approval of Named Service Providers. Diverse Vendor tracking action plan is complete

Project: 62 - 2233 - Quarterly FAS Review (Q2 2022)

REPORT DATE: 10/03/2022

CLOSED

Closed Observations: 1

OBSERVATION #1 - INTERNAL AUDIT NOTED A 2.4% ERROR RATE (ONE ERROR) WITH THE 41 FAS CALCULATIONS SAMPLED FROM THE 2ND QUARTER OF 2022.

Process Owner: MEMBER SERVICES

Completion Date: 03/17/2023

MAP Status Unassigned

Action Plan: Provide additional training to the Team members when calculating a Sanitation District FAS and benefit. This would include reiterating that Quality Assurance will need to perform a completely separate reperformance of the FAS calculation. Work with the Employer, Sanitation District, to correct errors in the transmittal before OCERS can begin the process of calculating the FAS and benefit.

IA Follow-Up: IA confirmed Member Services provided the additional training and communicated the error with OC Sanitation District.

Project: 63 - 2235 - The Toll Roads Employer Audit

REPORT DATE: 02/14/2023

CLOSED

Closed Observations: 4

OBSERVATION #1 - 1. FOR ONE MEMBER IN OUR TEST SAMPLE, THE MEMBER AFFIDAVIT FORM WAS INCOMPLETE REGARDING THE MEMBER'S PREVIOUS PUBLIC SERVICE.

Process Owner: EMPLOYER

Completion Date: 03/22/2023

MAP Status Unassigned

Action Plan: TCA ensures all member affidavits are completed for previous public service. The instance identified was for the HR Director. He did not fill out the previous experience because he knew it would not be eligible for reciprocity. TCA reminded the HR Director to ensure all member affidavits have this section completed, regardless of the employee's service credit reciprocity eligibility.

IA Follow-Up: IA confirmed the HR Director was made aware to ensure all sections are completed in a member's affidavit.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 25 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



OBSERVATION #2 - FOR TWO MEMBERS IN OUR TEST SAMPLE, THE EMPLOYER INCORRECTLY REPORTED THE PAYROLL INFORMATION TO THE OCERS PENSION ADMINISTRATION SYSTEM (PAS).

Process Owner:	EMPLOYER	
Completion Date:	05/02/2023	MAP Status Unassigned
Action Plan:	TCA has adjusted the employee's reported hours for PP13 & PP14 to correctly reflect the hours worked. TCA noted our internal OCERS schedules properly reflected the number of hours worked, but they were incorrectly copied over to the OCERS transmittal. Additionally, TCA noted the internal schedule for the second employee properly reflected the hourly rate for the pay periods noted. TCA will adjust the employee's reported hourly rate for these periods. TCA reminded the staff and supervisor responsible for preparing and reviewing the transmittal to confirm all hours and information agree to our internal documentation prior to submission. TCA is also working to automate the process of updating the OCERS transmittals with the data from our payroll reports to limit the potential for manual data entry mistakes.	
IA Follow-Up:	IA confirmed transmittal adjustments were recorded in V3. TCA has been working with OCERS to find opportunities to automate the payroll transmittal.	

OBSERVATION #3 - 3. WE NOTED A SINGLE INSTANCE IN WHICH A TIMESHEET LACKED SUPERVISORY SIGNOFF.

Process Owner:	EMPLOYER	
Completion Date:	03/22/2023	MAP Status Unassigned
Action Plan:	The Sr. Accounting Clerk responsible for ensuring timesheets were properly approved for the selected pay period and the supervisor of the selected employee are no longer with TCA. TCA reminded the new payroll Sr. Accounting Clerk and Accounting Supervisor responsible for review to confirm all timecards (including partial timecards under a different supervisor) include supervisor approval prior to payroll submission.	
IA Follow-Up:	IA confirmed communication was made to the Sr. Accounting Clerk and Accounting Supervisor responsible for ensuring timesheets are approved.	

OBSERVATION #4 - TWO PROCESS AND REVIEW CONTROLS RELATED TO MEMBER ELIGIBILITY AND PREMIUM PAY ARE NOT FORMALLY DOCUMENTED.

Process Owner:	EMPLOYER	
Completion Date:	06/18/2024	On Schedule
Action Plan:	<ul style="list-style-type: none"> Quarterly review of total hours worked by Extra Help and temporary staff: TCA currently requires managers to monitor the hours of temporary project employees. The Controller reviews and signs off on each payroll register as evidence of review of payroll, which includes the hours of temporary project employees. The quarterly review is prepared as a visual aid to note the YTD hours of service for these employees. For additional documentation, TCA's Assistant Controller will begin signing off on her quarterly tracking spreadsheet. Auto allowance: TCA will add verbiage to the employee handbook describing the auto allowance program. This will be incorporated in the employee handbook revised draft for Board approval. 	
IA Follow-Up:	IA confirmed the quarterly review process is now performed and Employee Handbook was updated with Car Allowance documentation	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 66 - 2171 - IT Automated Controls

REPORT DATE: 02/14/2023

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. AN OPPORTUNITY EXISTS TO ENHANCE DOCUMENTATION OF THREE SPECIFIC AREAS DESCRIBED ACROSS SIX OF THE 19 PENSION ADMINISTRATION SYSTEM SPECIFICATION DOCUMENTS REVIEWED BY INTERNAL AUDIT.

Process Owner:	INFORMATION TECHNOLOGY	
Completion Date:	09/03/2024	On Schedule
Action Plan:	IT Management will work with our PAS vendor and Member Services to update the identified PAS Design Specification documents to include the detailed logic and calculations configured for our PAS.	
IA Follow-Up:	IT Ops received the information back from Vitech and updated the V3 Design Specs to include the information identified in the Observation.	

Project: 64 - 2331 - Children and Families Commission

REPORT DATE: 04/05/2023

CLOSED

Closed Observations: 3

OBSERVATION #1 - FOUR MEMBERS PREVIOUSLY SEPARATED FROM CFCOC WERE STILL CLASSIFIED WITH ACTIVE STATUS IN THE PENSION ADMINISTRATION SYSTEM (PAS).

Process Owner:	EMPLOYER	
Completion Date:	05/02/2023	MAP Status Unassigned
Action Plan:	The CFCOC Assistant to CEO will add the required termination form to the off-boarding process when an employee terminates. Once completed, the CFCOC Director of Finance will review for accuracy and submit to OCERS.	
IA Follow-Up:	IA confirmed the status was updated for the four members.	

OBSERVATION #2 - ONE MEMBER DID NOT HAVE A MEMBER AFFIDAVIT ON FILE IN THE PAS AND FIVE ADDITIONAL MEMBER AFFIDAVITS WERE SENT TO OCERS WITH MISSING INFORMATION.

Process Owner:	EMPLOYER	
Completion Date:	08/01/2023	MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 27 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: All future Member Affidavit forms will be reviewed for accuracy and completeness by the CFDOC Assistant to CEO at time of onboarding new staff. A final review of the form will be performed by CFDOC Director of Finance before being submitted to OCERS.

CFDOC will either amend or correct affidavits currently on file that are incomplete depending on direction from OCERS.

IA Follow-Up: IA confirmed updated member affidavit forms.

OBSERVATION #3 - THERE ARE NO FORMAL INTERNAL GUIDELINES HELPING TO MONITOR INDEPENDENT CONTRACTORS FOR COMPLIANCE WITH IRS REGULATIONS DEFINING INDEPENDENT CONTRACTORS.

Process Owner: EMPLOYER

Completion Date: 05/04/2023

MAP Status Unassigned

Action Plan: CFCOC staff will work with Commission Counsel and develop internal guidelines.

IA Follow-Up: IA confirmed internal guidelines were developed.

Project: 65 - 2332 - OC Superior Court

REPORT DATE: 04/05/2023

CLOSED

Closed Observations: 2

OBSERVATION #1 - THIRTEEN MEMBERS PREVIOUSLY SEPARATED FROM SUPERIOR COURT WERE STILL CLASSIFIED WITH ACTIVE STATUS IN THE PENSION ADMINISTRATION SYSTEM (PAS).

Process Owner: EMPLOYER

Completion Date: 08/01/2023

MAP Status Unassigned

Action Plan: OC Superior Court to send existing records of OCERS Termination Notices to eaa@ocers.org for all 13 members indicating the separation dates.

IA Follow-Up: IA confirmed status for all 13 members.

OBSERVATION #2 - 2. TWO MEMBERS DID NOT HAVE A MEMBER AFFIDAVIT ON FILE IN THE PAS AND FIVE ADDITIONAL MEMBER AFFIDAVITS WERE SENT TO OCERS WITH EITHER MISSING INFORMATION OR ON AN OUTDATED FORM.

Process Owner: EMPLOYER

Completion Date: 04/17/2023

MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 28 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: The Court will complete the following:
 • Send the two OCERS Member Affidavits that are missing from OCERS Records to employerpayroll@ocers.org
 • OCERS Member Services instructed the Court to obtain emails from the three members with missing information answering the following: "Are you a member of any other public retirement system in the state of California?
 If yes, please list other public retirement systems along with dates of service.
 If no please respond to confirm you do not have any other public service in California"
 Emails to be sent by the Court HR to the employees to obtain their responses
 • OCERS Member Services instructed the Court to obtain emails from the two members with outdated forms answering the following: "Are you a member of any other public retirement system in the state of California?
 If yes, please list other public retirement systems along with dates of service.
 If no please respond to confirm you do not have any other public service in California"
 Emails to be sent by the Court HR to the employees to obtain their responses

IA Follow-Up: IA Confirmed the necessary information was provided to OCERS

Project: 67 - 2202 - Alameda Audit

REPORT DATE: 04/05/2023

CLOSED

Closed Observations: 3

OBSERVATION #1 - 1. INTERNAL AUDIT NOTED A 6.7% ERROR RATE (TWO ERRORS OUT OF THE SAMPLE OF 30) WITH THE FAS CALCULATIONS SAMPLED.

Process Owner: MEMBER SERVICES

Completion Date: 05/15/2023

MAP Status Unassigned

Action Plan: These errors were associated to the first 30 transactions performed by external contractors. The prior 6 transactions (October and November 2022) where Member Services did not have any errors were performed by seasoned team members. From our review of these items, the contractors did not follow the documented processes and training they were provided; had the process been followed errors would not have occurred. The issue has been addressed with the contractors and they fully understand the need for following the documented process. The Member Services management team is also considering extending the payroll deadlines to allow for more time to perform the processing and QA. We believe rushing to get transactions processed before the deadline has contributed to the errors and think extending the timeline will help prevent future errors.

IA Follow-Up: Internal Audit confirmed the communication was made to the contractors to follow the documented procedure. The payroll deadline was also extended from 30 to 45 days.

OBSERVATION #2 - INTERNAL AUDIT NOTED A 13.3% ERROR RATE (FOUR ERRORS OUT OF THE SAMPLE OF 30) WITH THE MANUAL ALLOCATION OF THE TOTAL OVERPAID BENEFITS TO BE RECOVERED BETWEEN THE RETIREE AND THE EMPLOYER (NOT FAS IMPACTING).

Process Owner: MEMBER SERVICES

Completion Date: 05/15/2023

MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 29 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: These errors were on a new Excel tab specifically created for Alameda recalculations. With the Board direction to only collect overpayments from 10/1/2020 forward from the member, Member Services needed to create a manual calculation process. This tab was created so we could split the amount of the overpayment between the Member and the Employer. V3 automatically calculates the total overpayment, however V3 cannot automate the split between Member and Employer. The data in this tab is a direct extract from members' V3 accounts and the errors occurred when the contractors entered the data manually vs extracting it from V3. In addition, the QA team did not validate the numbers thinking they were a direct extract. Member Services management team will be modifying our controls to ensure this new data tab is calculated separately by our QA team to validate the numbers.

IA Follow-Up: Confirmed new control for overpayment allocation was implemented.

OBSERVATION #3 - FOR ONE RETIREE IN OUR SAMPLE, THREE PAY ITEMS IN ONE PARTIAL PAY PERIOD WERE NOT PRORATED IN A CONSISTENT MANNER.

Process Owner: MEMBER SERVICES

Completion Date: 01/19/2024

MAP Status Unassigned

Action Plan: Member Services followed a standing practice for this observation. OCERS current practice is to accept pay items that have already been prorated by the employer as reported in the transmittal. We will however ensure our current practice is documented in our procedure. We will also review our procedures to determine if it can be simplified even further to eliminate any manual proration of pay items passed to us from the employer.

IA Follow-Up: Member Services provided the updated procedure.

Project: 68 - 2334 - Member Data Maintenance_Bank Account Changes

REPORT DATE: 06/01/2023

CLOSED

Closed Observations: 5

OBSERVATION #1 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: MEMBER SERVICES

Completion Date: 06/01/2023

MAP Status Unassigned

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Internal Audit confirmed management action plan has been implemented.

OBSERVATION #2 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: MEMBER SERVICES

Completion Date: 12/18/2023

MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 30 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Details Removed - Discussed in Closed Session
IA Follow-Up: Member Services provided examples of reviewed confirmation letters.

OBSERVATION #3 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: MEMBER SERVICES
Completion Date: 12/18/2023
Action Plan: Details Removed - Discussed in Closed Session
IA Follow-Up: Member Services provided IT ticket to PAS vendor for letter generation.

MAP Status Unassigned

OBSERVATION #4 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: MEMBER SERVICES
Completion Date: 01/18/2024
Action Plan: Details Removed - Discussed in Closed Session
IA Follow-Up: Member Services confirmed direct deposit information, included reminders in meeting agendas and updated member facing information with reminders.

MAP Status Unassigned

OBSERVATION #5 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: MEMBER SERVICES
Completion Date: 01/18/2024
Action Plan: Details Removed - Discussed in Closed Session
IA Follow-Up: Member Services included reminders during team meetings and updated materials to verify information.

MAP Status Unassigned

Project: 72 - 2301 - Alameda 2nd audit

REPORT DATE: 10/11/2023

CLOSED

Closed Observations: 1

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



OBSERVATION #1 - INTERNAL AUDIT NOTED 13% OF THE ALAMEDA CONTRIBUTION REFUND RE-CALCULATIONS WERE INCORRECT DUE TO A RECENT CHANGE IN THE PENSION ATTRIBUTE FOR A SPECIFIC PAY ITEM. THIS DOES NOT IMPACT FAS.

Process Owner:	MEMBER SERVICES	
Completion Date:	12/18/2023	MAP Status Unassigned
Action Plan:	Member Services Management team reviewed the process for performing the recalculation of the Contribution Refunds as it pertains to the PHP pay item. As Internal Audit confirmed with the subsequent months' members affected by PHP, our process was corrected to include these amounts (reverse pickup rate) in our subsequent calculations. Member Services has also provided Internal Audit with the files containing the corrected contribution refund calculations for the five members noted. These revised contribution and interest amounts were used in total to offset the member's overpayment and thus did not get paid directly to the members as a refund.	
	We have also worked with the county to create a new pay item for PHP pay item in the PAS as a result to ensure future benefits automatically include the pay in the retirement benefits.	
IA Follow-Up:	Member Services adjusted the process to include the reverse pickup rate.	

Project: 73 - 2333 - Audit of OCFA employer audit

REPORT DATE: 10/11/2023

CLOSED

Closed Observations: 3

OBSERVATION #1 - FOR ONE MEMBER IN OUR TEST SAMPLE, THE MEMBER AFFIDAVIT FORM WAS INCOMPLETE REGARDING THE MEMBER'S PREVIOUS PUBLIC SERVICE.

Process Owner:	EMPLOYER	
Completion Date:	09/14/2023	MAP Status Unassigned
Action Plan:	The member has checked the appropriate box to indicate no prior public service. The amended form has been provided to OCERS Internal Audit team to provide to Member Services.	
IA Follow-Up:	IA confirmed the updated member affidavit.	

OBSERVATION #2 - TWO PERSONNEL ACTION FORM (PAF) APPROVALS DID NOT HAVE AN APPROVAL SIGNATURE FROM THE DEPARTMENT HEAD, ONLY APPROVAL FROM HUMAN RESOURCES.

Process Owner:	EMPLOYER	
Completion Date:	09/12/2023	MAP Status Unassigned

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 32 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: The PAF is designed to cover all of the personnel actions that occur within the agency. While the form has multiple signature lines, not every signature line is required to authorize a given action (e.g., a COLA increase, changing Org numbers (which occurs frequently based on reassignments to different stations). An Assistant Chief or Deputy Chief can be the single signatory in those instances. In the case of a COLA increase, a PAF, while not required, is done to simply document the increase and would not need multiple signatures. Multiple signatures are required for Merit Increases, Initial Hire, and Reductions. However, if it's a HR employee then a single signature from the Assistant Chief of Human Resources or Deputy Chief of Administration and Support would suffice, which is the case with one of the two sampled PAFs.

IA Follow-Up: OCFR noted the Assistant Chief of Human Resources has signed the PAF.

OBSERVATION #3 - MEMBERSHIP ELIGIBILITY REVIEW OCCURS BUT IS NOT FORMALLY DOCUMENTED.

Process Owner: EMPLOYER

Completion Date: 01/11/2024

MAP Status Unassigned

Action Plan: The Human Resources Manager over Benefits will review and sign the biweekly Extra-Help report submitted by Finance. HR Benefits and Payroll personnel have communicated regarding new process going forward.

IA Follow-Up: IA confirmed OCFR HR Manager is signing the biweekly Extra-Help report.

Project: 74 - 2337 - Employer audit of IHSS Public Authority

REPORT DATE: 10/11/2023

CLOSED

Closed Observations: 4

OBSERVATION #1 - IHSS PA IS INCORRECTLY ADDING NON-PENSIONABLE OVERTIME PAY TO PENSIONABLE SALARY IN ITS BI-WEEKLY PAYROLL TRANSMITTAL FILES.

Process Owner: EMPLOYER

Completion Date: 01/10/2024

MAP Status Unassigned

Action Plan: IHSS PA will work with OCERS Member Services to add non-pensionable overtime as a separately reported pay item in the transmittal files, as described in OCERS Board Pay Item Review policy.

IA Follow-Up: IHSS provided support for the implementation of a new pay item.

OBSERVATION #2 - FOR ONE ACTIVE MEMBER, IHSS PA INCORRECTLY REPORTED THE SERVICE HOURS IN THE TRANSMITTAL FILES FOR 12 CONSECUTIVE PAY PERIODS FROM AUGUST 2022 TO JANUARY 2023.

Process Owner: EMPLOYER

Completion Date: 07/29/2024

1st Missed Due Date

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 33 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Revised Due Date: 08/01/2024

Action Plan: IHSS PA will correct the member's transmittal records to reflect actual hours worked in the service hours column via payroll transmittal adjustment files.

IA Follow-Up: IHSS Public Authority provided the refund transmittals

OBSERVATION #3 - IHSS PA'S SALARY INCREASE AUTHORIZATION FORMS DO NOT HAVE THE EMPLOYEE'S TITLE CODE, TITLE DESCRIPTION, AND PAY GRADE.

Process Owner: EMPLOYER

Completion Date: 03/18/2024

On Schedule

Action Plan: IHSS PA will amend its Salary Increase Authorization forms to evidence the title code, title description and pay grade consistent with The County of Orange's pay schematics.

IA Follow-Up: IHSS PA updated the Salary Adjustment Authorization form

OBSERVATION #4 - FOR NINE MEMBERS IN OUR TEST SAMPLE, THE MEMBER AFFIDAVIT FORM WAS INCOMPLETE REGARDING THE MEMBER'S PREVIOUS PUBLIC SERVICE OR MISSING A WITNESS SIGNATURE.

Process Owner: EMPLOYER

Completion Date: 03/21/2024

On Schedule

Action Plan: IHSS PA will work with OCERS employer payroll team and determine if an amended Member Affidavit form should be sent to OCERS, or if another form of documentation should be sent to OCERS.
 IHSS PA will develop a process to confirm the forms are completed when onboarding a new employee.

IA Follow-Up: IHSS PA provided updated Member Affidavit forms and updated their process.

Project: 71 - 2361 - HR audit of hiring practices

REPORT DATE: 10/11/2023

CLOSED

Closed Observations: 4

OBSERVATION #1 - HUMAN RESOURCES (HR) DOES NOT HAVE FORMAL PROCEDURAL DOCUMENTATION FOR THE HIRING AND RECRUITING PROCESS.

Process Owner: HUMAN RESOURCES

Completion Date:

On Schedule

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 34 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: The Human Resources department will develop procedures for the hiring and recruitment practices.

IA Follow-Up: HR provided IA with documentation regarding the hiring and recruitment process.

OBSERVATION #2 - OCERS'S INTERNAL EMPLOYMENT OFFER WORKSHEET IS NOT FORMALLY DOCUMENTED WITH THE RATIONALE FOR HIRING A CANDIDATE.

Process Owner: HUMAN RESOURCES

Completion Date: 09/21/2023

MAP Status Unassigned

Action Plan: The HR department has added language that supports the CEO's approval criteria to the Employment Offer Worksheet. Hiring managers will now be required to acknowledge they have met the CEO's approval requirements.

Additionally, the CEO will acknowledge that he has met with the hiring manager and approve extending an offer of employment to the selected candidate.

IA Follow-Up: Internal Audit confirmed the Employment Offer Worksheet was updated with the CEO acknowledgement.

OBSERVATION #3 - OCERS IS USING THE STANDARD COUNTY BACKGROUND CHECK INSTEAD OF OCERS' MORE EXTENSIVE 3RD PARTY BACKGROUND CHECK FOR ALL NEW COUNTY EMPLOYEES WHO WILL GAIN ACCESS TO CONFIDENTIAL MEMBER DATA WITHIN THE PENSION ADMINISTRATION SYSTEM (PAS).

Process Owner: HUMAN RESOURCES

Completion Date: 09/20/2024

On Schedule

Action Plan: The HR department will schedule a meeting with the County to discuss next steps needed to institute more extensive background checks.

IA Follow-Up: IA has verified that the meeting will be held with County counsel and union representatives.

OBSERVATION #4 - HUMAN RESOURCES IS MAINTAINING TERMINATED EMPLOYEE PERSONNEL RECORDS BEYOND THAT ALLOWED PER OCERS BOARD RECORDS MANAGEMENT POLICY.

Process Owner: HUMAN RESOURCES

Completion Date: 11/14/2024

On Schedule

Action Plan: A request to increase the retention period for personnel files from 4 to 7 years will be made to the Governance Committee at their next review of the Records Management policy. All personnel files outside of the 7-year window were destroyed.

IA Follow-Up: We viewed the revised retention policy from the November 1st Governance meeting, we noted the retention period was changed from 4 years to 7 years.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 35 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 76 - 2391 - Azure Active Directory and Microsoft 365 Security Assessment

REPORT DATE: 01/19/2024

CLOSED

Closed Observations: 12

OBSERVATION #101 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	
Completion Date:	03/13/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item complete	

OBSERVATION #102 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	
Completion Date:	12/30/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item completed.	

OBSERVATION #103 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	
Completion Date:	03/13/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item Complete	

OBSERVATION #104 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	
-----------------------	----------------------	--

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."

Completion Date:	12/24/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item is closed.	
OBSERVATION #105 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION		
Process Owner:	INFORMATION SECURITY	
Completion Date:	04/01/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item completed.	
OBSERVATION #106 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION		
Process Owner:	INFORMATION SECURITY	
Completion Date:	03/13/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item complete	
OBSERVATION #201 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION		
Process Owner:	INFORMATION SECURITY	
Completion Date:	03/13/2024	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item complete	
OBSERVATION #202 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION		
Process Owner:	INFORMATION SECURITY	
Completion Date:	05/13/2024	On Schedule

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item completed

OBSERVATION #203 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 05/13/2024

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item completed

OBSERVATION #301 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/29/2023

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item completed

OBSERVATION #302 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/29/2023

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item closed

OBSERVATION #303 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/02/2024

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



IA Follow-Up: Item completed

Project: 79 - 2342 - Accounts Payable Audit

REPORT DATE: 03/28/2024

CLOSED

Closed Observations: 2

OBSERVATION #1 - FINANCE MANAGEMENT SHOULD FORMALIZE THE REVIEW OF (1) THE VENDOR MASTER FILE LIST IN THE ERP SYSTEM AND (2) THE QUARTERLY ACCOUNTS PAYABLE ACCRUAL.

Process Owner: FINANCE

Completion Date: 05/14/2024

On Schedule

Action Plan:

1. During the implementation of the ERP system, Finance purged inactive vendors from its previous accounting system, importing only active vendors into the new system that went live in 2022. Finance continues to review processes and procedures for improvement and starting in January 2024, as recommended by Internal Audit, we formally documented the annual review of the Vendor Maintenance List for the year ended December 2023 identifying vendors that could potentially be made inactive if they continue to have no activity during 2024.
2. Quarterly reconciliation of accrued payables is completed each quarter. The Accounts Payable Accountant prepares the accrual entries. The Finance Manager reviews the entries and the accrual balance for accuracy. Going forward, beginning with 4th quarter 2023, a sign-off will be noted within the file.

IA Follow-Up: IA confirmed the review of the Vendor Maintenance list and the Quarterly accrued payables reconciliation were performed

OBSERVATION #2 - A NETWORK FOLDER CONTAINING 2014 ACCOUNTS PAYABLE RELATED FILES HAD NOT BEEN DELETED.

Process Owner: FINANCE

Completion Date: 05/14/2024

On Schedule

Action Plan:

During 2022, the Finance Team reorganized the department's accounting folders and purged a large number of documents and folders in adherence with the Records Management Policy. The files in question were missed in the original purging of records and have since been deleted.

As part of the Legal Department's year-end request for an annual certification of compliance with the Records Management Policy for each department, the Finance Director emails all Finance Team Members to confirm that they are in compliance with the policy. As part of this compliance and to maintain records within the required retention period, all Finance Team members will purge files at the end of June each year, after the financial audit and other external reporting have been completed.

IA Follow-Up: IA confirmed the identified folders were deleted.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 39 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Project: 81 - 2336 - Payroll Transmittal Process

REPORT DATE: 03/28/2024

CLOSED

Closed Observations: 4

OBSERVATION #1 - OCERS DOES NOT HAVE A WRITTEN POLICY ESTABLISHING PURPOSE, SCOPE, AND ROLES REGARDING THE EMPLOYERS' RESPONSIBILITY TO ADDRESS EMPLOYER PAYROLL TRANSMITTAL EXCEPTIONS IN A TIMELY MANNER.

Process Owner:	MEMBER SERVICES	
Completion Date:	09/03/2024	On Schedule
Action Plan:	<p>The Employer Payroll Team will develop a written policy establishing purpose, scope, and roles regarding the employers' responsibility to address employer payroll transmittal exceptions in a timely manner.</p> <p>The Policy will incorporate the various reasons for exceptions, containing errors and False Positive errors, and how to differentiate between the two. The policy will also address the minimum acceptable levels of accuracy, based on the thorough review of what is a valid error.</p> <p>The development of the Policy will include an in-depth review of all aspects of the process, including current processes of reviewing and taking corrective actions, and recommending updates for the Transmittal Exceptions report (e.g., New info vs. reoccurring items). The Policy may generate a supplemental Procedure if necessary.</p> <p>While a policy is to be developed, employers were provided direction prior to V3 implementation, they have been provided guidance on a regular basis during the Annual Employer Workshop, as well as through regular channels of communication between the Employer Payroll Team and employers.</p>	
IA Follow-Up:	Draft policy has been presented to the Governance Committee on August 15, 2024 for its review. IA considers this MAP closed. See item A-9 on the agenda.	

OBSERVATION #2 - INTERNAL AUDIT IDENTIFIED TWO TYPES OF PAYROLL EXCEPTIONS TRACKED BY THE PAS THAT GENERATE NUMEROUS FALSE POSITIVES DUE TO EITHER PAS PROGRAMMING OR INSTANCES IN WHICH EMPLOYERS ARE REPORTING INCORRECT EMPLOYEE STATUS.

Process Owner:	MEMBER SERVICES	
Completion Date:		On Schedule
Action Plan:	<p>Review exceptions by importance/priority and determine if certain exceptions can be changed/deleted, especially looking at False Positives. Reach out to the PAS vendor to determine the cost to change in logic or turn off unnecessary exceptions (false positives) once exceptions are reviewed and further categorized (if needed).</p> <p>The Policy will recommend regular ongoing communication with employers, asking them to review and correct errors (that are not False Positives).</p>	
IA Follow-Up:	IA was informed by Member Services that a ticket resolution has been filed with the PAS vendor, Vitech.	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 40 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



OBSERVATION #3 - THE EMPLOYER PAYROLL TEAM'S PROCEDURE DOCUMENTATION DOES NOT PROVIDE GUIDANCE TO STAFF FOR HOW TO MONITOR IF THE EMPLOYERS ARE CORRECTING PAYROLL EXCEPTIONS.

Process Owner:	MEMBER SERVICES	
Completion Date:	09/23/2024	On Schedule
Action Plan:	Along with development of Policy, procedural guidance will be developed for processing exceptions.	
IA Follow-Up:	IA reviewed Member Services' new Employer Handbook and verified completion of the action plan.	

OBSERVATION #4 - THE EMPLOYER PAYROLL TEAM'S DOCUMENTATION DOES NOT PROVIDE STAFF GUIDANCE ON PROCEDURES FOR CHECKING NEW MEMBER AFFIDAVIT FORMS FOR COMPLETENESS AND ACCURACY OR DESCRIBE ESCALATION STEPS TO TAKE WHEN MEMBER AFFIDAVIT FORMS MISSING, INCOMPLETE, OR CONTA

Process Owner:	MEMBER SERVICES	
Completion Date:	09/23/2024	On Schedule
Action Plan:	<p>A New Member Affidavit has been developed and is in the final stage of review. This version gathers more and clearer information.</p> <p>We are also creating a Guidance Sheet for members and employers to assist them in completing the form.</p> <p>New Member Enrollment processes are due to be reviewed for Master Repository Project. We will also develop a Member Services Procedure for processing Affidavits based on current process. The procedure will provide guidance on reviewing and processing Affidavits including receiving and processing timing guidelines; following up for incomplete or missing Affidavits; and incorporate supervisory reviews (e.g., 1-5 % of total new Member Affidavits received).</p>	
IA Follow-Up:	IA reviewed Member Services' new Member Affidavit guidance sheet and new Member Affidavit form and verified completion of the action plan.	

Project: 82 - 2339 - Quarterly FAS Review (Q3 2023)

REPORT DATE: 03/28/2024

CLOSED

Closed Observations: 1

OBSERVATION #1 - INTERNAL AUDIT NOTED A 5.0% ERROR RATE (TWO ERRORS) WITH THE 40 FAS CALCULATIONS SAMPLED FROM THE 3RD QUARTER OF 2023.

Process Owner:	MEMBER SERVICES	
Completion Date:	12/02/2024	On Schedule

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 41 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Management takes all errors very seriously.

1(a) Response: In reviewing this specific transaction and the corresponding MOU section as shown below attached to this document, our Member Services team member had difficulty interpreting the language due to the many decision points within the vacation section of the document.

We will provide additional training to our team to address this risk. We are also in the process of creating a guidance sheet for the team members so they do not have to interpret the legal language in the individual MOU's.

In the future, our ongoing meetings with the employers in 2024 to address the missing data in the transmittals, will help eliminate the possibility of this type of error from happening.

1(b). Response: This error occurred post Quality Assurance (QA) when the representative was entering the approved calculation into the system.

Our new Member Services Robotic Process Automation robot (Bot), that performs a final check of a processed benefit after it has been processed in the system, will catch this type of error and prevent this from occurring in the future.

IA Follow-Up: IA verified implementation after reviewing MOU training class agenda regarding, MOU training guides, an employer meeting agenda from November 2024, and recent BOT report results.

Project: 84 - 2338 - OC Transportation Auth

REPORT DATE: 06/06/2024

CLOSED

Closed Observations: 2

OBSERVATION #1 - IN THREE OF OUR 60 SAMPLE TRANSACTIONS, OCTA OVER-COLLECTED CONTRIBUTIONS ON A NON-PENSIONABLE PAY ITEM (E.G., VAN PAY, OR VAN POOL INCENTIVE PAY).

Process Owner:	EMPLOYER	
Completion Date:	07/11/2024	On Schedule
Action Plan:	Information on over-collected amounts will be gathered and provided to OCTA from OCERS by mid-May. OCERS will handle refunds to retirees, deceased, terminated, and deferred retirees. Once information has been received from OCERS on amounts due to active OCTA employees, OCTA staff will process refunds within one month.	
IA Follow-Up:	OCTA processed refunds to active OCTA employees.	

OBSERVATION #2 - OCTA DOES NOT DETERMINE HOURS WORKED BY EXTRA-HELP AND REHIRED RETIREES BASED ON A FISCAL YEAR OR CALENDAR YEAR IN ACCORDANCE WITH OCERS MEMBERSHIP ELIGIBILITY REQUIREMENTS POLICY (POLICY) FOR DETERMINING MEMBERSHIP ELIGIBILITY.

Process Owner:	EMPLOYER	
Completion Date:	12/18/2024	1st Missed Due Date
Revised Due Date:	12/31/2024	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 42 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Human Resources will create a new report to monitor Extra-Help and rehired retirees on a calendar year basis. The new report will begin monitoring hours worked from January 1, 2024, for the 2024 calendar year. In addition, Human Resources will investigate creating a new status code for rehired retirees to ensure that their hours do not exceed 960.
IA Follow-Up: IA obtained updated Extra Help report and item is closed.

Project: 83 - 2491 - CIS Controls Assessment

REPORT DATE: 10/09/2024

CLOSED

Closed Observations: 4

OBSERVATION #1 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/09/2024

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item is closed.

OBSERVATION #2 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/18/2024

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item is closed.

OBSERVATION #3 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner: INFORMATION SECURITY

Completion Date: 12/02/2024

On Schedule

Action Plan: Details Removed - Discussed in Closed Session

IA Follow-Up: Item is closed.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

On Schedule to complete MAP
 Missed Due Date (1st Time), planned to complete by Revised Due Date
 Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 43 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



OBSERVATION #4 - DETAILS REMOVED - DISCUSSED IN CLOSED SESSION

Process Owner:	INFORMATION SECURITY	
Completion Date:	01/31/2025	On Schedule
Action Plan:	Details Removed - Discussed in Closed Session	
IA Follow-Up:	Item is closed.	

Project: 85 - 2431 - OC Public Law Library

REPORT DATE: 10/09/2024

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. FOR ONE MEMBER IN OUR TEST SAMPLE, THERE WAS A LACK OF SEPARATION OF DUTIES FOR TIMECARD APPROVAL.

Process Owner:	EMPLOYER	
Completion Date:		On Schedule
Action Plan:	Administrative Assistant Kelsey Chrisley will be added to the list of OCPLL staff with approval authority. She will review and approve a manager's timecard when no other manager is present.	
IA Follow-Up:		

Project: 90 - 2430 - HCA employer audit

REPORT DATE: 12/12/2024

CLOSED

Closed Observations: 5

OBSERVATION #1 - 1. RETROACTIVE PAY REPORTED FOR TWO EMPLOYEES WAS INCORRECT.

Process Owner:	EMPLOYER	
Completion Date:	09/12/2024	On Schedule

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

- On Schedule to complete MAP
- Missed Due Date (1st Time), planned to complete by Revised Due Date
- Missed Due Date (2nd Time) since latest Revised Due Date



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Both members whose retroactive pay was reported incorrectly have been corrected with the CAPS+ system and will be reflected in payroll transmittal adjustment files to be sent to OCERS.
IA Follow-Up: IA verified as closed during the course of the audit.

OBSERVATION #2 - 2. INTERNAL AUDIT IDENTIFIED 125 HCA MEMBERS WITH INCORRECT STATUS IN OCERS PENSION ADMINISTRATION SYSTEM (PAS).

Process Owner:	EMPLOYER	On Schedule
Completion Date:	08/01/2024	
Action Plan:	HCA has provided the requested documents to OCERS Member Services for the 112 members. OCERS has updated the PAS with the correct member status for the 13 active members.	
IA Follow-Up:	IA verified corrected status for all 125 members in the PAS.	

OBSERVATION #3 - 3. HCA HR DOES NOT USE EXTRA HELP POSITION REQUEST FORMS FOR CONTRACT EXTRA HELP EMPLOYEES, AS IT CONSISTENTLY DOES WITH NON-CONTRACT EXTRA HELP EMPLOYEES.

Process Owner:	EMPLOYER	On Schedule
Completion Date:	11/06/2024	
Action Plan:	The suggestion to amend the request form will be made to HCA leadership. The amendment would indicate that the employee has professional or highly technical skills (as per 5.c.i. of the OCERS Membership Eligibility Requirements policy).	
IA Follow-Up:	IA verified that the request was made.	

OBSERVATION #4 - 4. FOR 5 OF 10 EXTRA HELP EMPLOYEES SAMPLED, TOTAL HOURS REPORTED BY APPROVED TIMECARDS DID NOT MATCH THE TOTAL HOURS REPORTED ON THE HCA EXTRA HELP EMPLOYEES HOURS WORKED REPORT.

Process Owner:	EMPLOYER	On Schedule
Completion Date:	12/18/2024	
Action Plan:	For the five employees whose timecard hours do not match the reports, the differences were caused by missing data in our reporting system due to an archive error. This error is currently being corrected by IT.	
IA Follow-Up:	IA obtained documentation that the items is being addressed with HCA's IT Department.	

OBSERVATION #5 - 5. THE EXTRA HELP EMPLOYEES HOURS WORKED REPORTS HCA USES FOR MONITORING HOURS WORKED BY EXTRA HELP DOES NOT REPORT HOURS WORKED BY STAFF WHO HAVE BEEN HIRED AS REGULAR EMPLOYEES OR WERE SEPARATED.

Process Owner:	EMPLOYER	On Schedule
Completion Date:	10/18/2024	

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

	On Schedule to complete MAP
	Missed Due Date (1st Time), planned to complete by Revised Due Date
	Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 45 of 46



Management Action Plan Status Report

Project(s): ALL
 Mgmt. Status: OPEN, CLOSED - NO FURTHER ACTION REQUIRED
 Process Owner(s): ALL

"We provide secure retirement and disability benefits with the highest standards of excellence."



Action Plan: Reports only show active (current) extra help employees and do not include past or historical data, leading to the differences in employees reported on the Extra Help Employees Hours Worked reports. HRS Analytics also identified missing data in our reporting system due to an archive error. This error is currently being corrected by IT.

 Recommendations will be made for a future HR system to create reporting parameters to provide past or historical data to address the discrepancy. Also, a request has been made to HRS Analytics to address the archiving error.

IA Follow-Up: IA veified that the request was made with upper management.

Project: 89 - 2433- OCERS Employer Audit

REPORT DATE: 12/12/2025

CLOSED

Closed Observations: 1

OBSERVATION #1 - 1. IN ONE TEST SAMPLE, A PERSONNEL ACTION NOTICE (PAN) FORM WAS NOT COMPLETED TO DOCUMENT THE EMPLOYEE'S RETURN TO THEIR ORIGINAL POSITION AFTER A TEMPORARY PROMOTION ENDED.

Process Owner: HUMAN RESOURCES

Completion Date: 01/08/2025

On Schedule

Action Plan: The department will include in the payroll processing a process for using a PAN form to return employees to their regular pay.

IA Follow-Up: IA verified that PAN form is being used for return to work from temporary promotions.

Executed: 2/3/2025 10:14:26 AM
 Executed By: OCERS\plam

On Schedule to complete MAP
 Missed Due Date (1st Time), planned to complete by Revised Due Date
 Missed Due Date (2nd Time) since latest Revised Due Date

Doc. No. 0080-0120-R0001
 Page 46 of 46



Memorandum

DATE: February 11, 2025
TO: Members of the Audit Committee
FROM: Philip Lam, Director of Internal Audit
SUBJECT: **AUDIT COMMITTEE REVIEW OF ACTIVITIES**

Written Report

Background/Discussion

This report recaps the Audit Committee's previous activity to assist new Committee members with staying up to date.

Here's a summary of the key points and actions discussed during Audit Committee meetings in 2024:

Audit Committee Meeting held on January 19, 2024:

- **2024 Risk Assessment and Audit Plan:** Mr. Kim was praised for his work, especially on first-time audits and Employer Transmittal Audits. The Audit Committee gave directions to adjust the program, including performing fewer Final Average Salary (FAS) audits and revising the Alameda audit's scope. Ms. Freidenrich suggested quarterly quality review results from Member Services to determine FAS audit frequency.
- **External Quality Assessment (EQA):** The Internal Audit (IA) received the top rating of "Generally Conforms," with positive feedback on its governance, risk management, and effectiveness. The Audit Committee directed the General Counsel to report Compliance activities to them.
- **Key Performance Indicators (KPIs):** The Audit Committee provided feedback on audit report timelines and suggested including aging data in the Management Action Plan (MAP) report.

Audit Committee Meeting held on March 28, 2024:

- **Compliance Officer Charter:** Recognized Mr. Kim's work in strengthening the Internal Audit department.
- **Internal Audit Charter Review:** Ms. Freidenrich appreciated updates based on new Standards and led by OCERS Internal Audit.
- **Final Average Salary Audit:** First-time use of robotics in testing, with Ms. Freidenrich appreciating the technology's integration.
- **Investment Allocation Audit:** Suggested renaming the audit for clarity.
- **Other Audits:** Several audits were received and filed, including the OCERS Accounts Payable Audit and Payroll Transmittal Process.

Audit Committee Meeting held on June 6, 2024:

- **Employer Audit (OCTA):** Ms. Freidenrich provided direction to include dollar amounts in reports and categorize over/under-collected contributions as priority issues. Other directions included clarifying eligibility and Extra Help categorization under the OCERS Membership Eligibility Policy.
- **Compliance Program Report:** Mr. Addo acknowledged Mr. Kim's management of the Ethics Hotline and Management Action Plan.

Audit Committee Meeting held on October 9, 2024:

- Several audits, including the Public Law Library Employer Audit and Management Action Plan, were approved or filed without specific feedback.

Audit Committee Meeting held on December 12, 2024:

- **Employer Audit (OCERS):** Direction was given to bring the OCERS Direct Employee Handbook to the Personnel and Audit Committees.
- **Health Care Agency Employer Audit:** Mr. Prevatt recommended recategorizing observations and ensuring proper distribution of reports.
- **Internal Audit Transition:** Mr. Packard called for better communication with key decision-makers.
- **Compliance Program:** The Committee requested quarterly reports from the Compliance Department and annual training evaluations to ensure staff retains knowledge.

Overall, the meetings focused on strengthening internal audits, compliance reporting, and ensuring clarity and efficiency in audit processes.

Submitted by:



PL - Approved

Philip Lam
Director of Internal Audit