May 21, 2026

City of San Jose Office of Retirement Services

Risk Assessment and Proposed 5-Year Internal Audit Plan

Contents

Introduction

Overview

Background

The San Jose Office of Retirement Services (ORS) administers retirement benefits for eligible City of San Jose employees, retirees, and beneficiaries. As part of one of the largest municipal governments in California, ORS is responsible for safeguarding retirement assets, ensuring accurate and timely benefit payments, and complying with applicable legal and fiduciary requirements. These responsibilities are essential to supporting the financial security of plan members and maintaining public trust.

The ORS engaged Baker Tilly Advisory Group, LP (Baker Tilly) in 2026 to conduct an agency wide risk assessment and prepare a five-year internal audit plan to span the fiscal years of 2027 to 2031, with audits beginning at the start of July 2026. The purpose of the internal audit risk assessment is to develop an audit plan that assigns internal audit resources to the activities that add the most value to ORS.

Risk is defined as "the possibility of an event or condition occurring that will have an impact on the ability of an organization to achieve its objectives."[1] The risk assessment process involves identifying and measuring risks associated with the audit universe (a list of specific ORS divisions, functions, processes, programs, etc. that can be subject to an audit, i.e. auditable units).

Audit Planning

This report summarizes Baker Tilly's risk assessment methodology, analysis, and results. The 5-Year internal audit plan proposed in this report is based on the results of this risk assessment. The risk assessment involved collaboration with ORS leadership from the main departments across the organization.

In conducting this risk assessment, we performed the following:

- Obtained an understanding of the ORS' environment, businesses, and objectives
- Conducted interviews with leadership and staff representing the major operations and administrative functions of ORS, Audit Committee Members and the City of San Jose City Auditor
- Conducted risk assessment interviews to gain additional insight from ORS leadership
- Analyzed key documentation such as annual budget documents, financial statements, departmental strategic plans, and prior audit reports
- Evaluated the results of interviews and documentation reviews and considered industry factors to identify areas of risk to ORS

In developing the 5-Year Audit Plan, we considered the following:

- Risk assessment – Internal audit activities to target high risk areas based on the results of the risk assessment
- Adding value – Internal audit activities to add value through independent and objective analysis
- Coverage and other audits – Consideration of prior and other audits as well as pervasiveness of the process or control to ensure audit coverage and to avoid duplication of efforts
- Industry trends – Key risk and audit areas that have been a focus for other similar governmental organizations

[1] Rick A, Wright Jr., CIA, "The Internal Auditor's Guide to Risk Assessment" The Institute of Internal Auditors (IIA) Research Foundation (IIARF), 2018

Risk Assessment Process Considerations

The starting point of internal auditing is to conduct a risk assessment that is the basis for determining the internal audit activities. However, it is not a one-size-fits-all process. The scope and complexity of the risk assessment is affected by various factors such as the organization's risk profile, maturity level of the internal audit function and the organization's enterprise risk management (ERM) efforts, coordination with other monitoring and risk management functions, and the stakeholders' expectations. The best practice is to focus on risks related to the achievement of the organization's strategies and objectives. The internal audit risk assessment and audit plan is conducted formally every five years. However, internal audit monitors the environment for changes and emerging risks throughout the year and will review the audit plan annually, aligning and adjusting the annual audit plan accordingly.

In addition to the annual macro-level risk assessment, the internal audit function is required to perform an engagement-level risk assessment when starting each audit listed in the approved audit plan. The IIA Standard 2200 states, "Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement."

Risk assessment can also be conducted as part of risk management as one of the essential elements of organizational governance. ERM is defined as "the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value."[2] ERM is more than having a list of all the risks for an organization. The COSO's ERM principles covering governance to monitoring (including defining risk appetite and implementing risk responses), apply to all levels and functions of an organization although management has overall responsibility for managing risks and a governing body has an oversight role. The internal audit function may leverage ERM information, if available, for efficiency and quality of its risk assessment.

Fraud Considerations

While managing fraud risks is management's responsibility, internal auditors should consider probability of significant errors, fraud, or noncompliance. Consistent with the Global Internal Audit Standards, engagement objectives are based on engagement-level risk assessments (Standards *13.2 – Engagement Risk Assessment* and *13.3 – Engagement Objectives and Scope),* which include consideration of risks such as fraud, error, and noncompliance. Additionally, auditors apply due professional care in considering the likelihood of such risks (Standard 4.2).

[2] "COSO Enterprise Risk Management-Integrating with Strategy and Performance", The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017

Risk Assessment Approach

Baker Tilly's risk assessment approach consisted of four phases as illustrated in the graphic below.

2026 RISK ASSESSMENT PHASES	
Planning	• Performed risk assessment interviews with key stakeholders and leadership
Information Gathering	• Analyzed the key documents such as organizational charts, ORS' missions, visions, values, budget documents, strategic and past audit plans, audit reports, and information on the City's website and other relevant documents. • Interviewed ORS leadership, staff, Audit Committee and the City of San Jose's City Auditor to identify the events and conditions that may affect the achievement of ORS' objectives. • Determined the key activities and processes of each audit area. • Updated the risk assessment matrix with the information gathered.
Analysis	• Scored the auditable units (listed in **Appendix A**) in the risk matrix based on the likelihood and the impact[3] of potential adverse events ○ Each of the auditable units received scores for various risk factors related to the likelihood or impact (defined in **Appendix B**) ○ Risk factor scores were multiplied to create a single score for the auditable unit • Identified potential internal audit activities for the auditable units with high-risk scores
Reporting	• Summarized the approach and results of the risk assessment • Documented proposed internal audit plan

[3] Likelihood is the possibility that an event will occur. Impact is the extent to which an event might affect an organization.

City of San Jose's Office of Retirement Systems
FY 2027 - 2031 Risk Assessment
Listed in order of risk level, high to low

Division	Key Function	Risk Score	Previously Audited	Proposed Audit Plan Year
IT	1099-R Reporting	20	No	FY 2027
IT	Cybersecurity and Data Protection	15	No	FY 2028
Accounting	ACFR Requirements	12	No	TBD[4]
Accounting	Benefits Disbursements Process	12	FY2020	FY 2029
Accounting	Cash Disbursements Process	12	FY2020	TBD
Administration	Business Continuity Planning	12	No	FY 2029
Administration	Employee Training	12	No	FY 2031
Benefits	Disability Payments	12	No	FY 2031
Benefits	Return of Contributions	12	FY2021	TBD
Benefits	Service Purchase Contracts	12	No	FY 2028
Investments	Asset Allocation	12	No	FY2030
Investments	Due Diligence	12	No	FY2030
Investments	Investment Cash Outflows (Wires and Internal Transfers)	12	FY2020	TBD
Investments	Investment Compliance Monitoring	12	No	FY 2030
Investments	Investment Manager Reconciliation	12	No	FY 2027
Investments	Investment Process	12	No	FY 2030
IT	Compliance and Regulatory Requirements	12	No	FY 2030
IT	IT Operations and System Administration	12	No	FY 2028
IT	Physical Security	12	No	FY 2028
Accounting	COLA Posting	9	No	TBD
Accounting	Contribution Reconciliation	9	FY2021	TBD
Accounting	Custodian Bank Reconciliation	9	No	TBD
Accounting	Interest Posting	9	No	TBD
Benefits	Member Enrollment Set-up	9	FY2020	TBD
Benefits	Member Termination	9	FY2020	TBD

[4] TBD = "To Be Determined" items did not fit into the current, budgeted 5-year audit plan. Only items that were rated as "high" were selected for the audit plan with the exception of some IT areas that naturally fit with auditing IT Operations and Systems Controls. Each year the audit plan will be evaluated and project changes may be suggested to the audit committee based on the prior year's work, organizational changes, or new/emerging risks.

Division	Key Function	Risk Score	Previously Audited	Proposed Audit Plan Year
Benefits	Military Time Purchase	9	No	TBD
Benefits	Rehired Retirees	9	No	TBD
IT	Application Controls	9	No	TBD
IT	Change Management	9	No	FY 2028
IT	Data Management and Data Integrity	9	No	FY 2028
IT	Identity and Access Management (IAM)	9	No	FY 2028
IT	IT Governance and Management	9	No	FY 2028
IT	Logging, Monitoring, and Audit Trails	9	No	FY 2028
IT	Third-Party Vendor Management	9	No	TBD
IT	Access to Programs and Data	8	No	TBD
Administration	Communication Audit	6	No	TBD
Benefits	Deferred Vested	6	No	TBD
Benefits	Disability Retirement Application	6	No	TBD
Benefits	Reciprocity	6	No	TBD
Benefits	Service Retirement Application	6	FY2020	TBD
Investments	Cash Projection Process	6	No	TBD
Investments	Investment Manager Fees	6	No	TBD
Investments	Sweep Vehicle Process	6	No	TBD
IT	Systems Development, Acquisitions, and Implementation	6	No	TBD
IT	New Accounts Opening	4	No	TBD
Benefits	Member Death Verification	3	FY2020	TBD

Proposed FY 2027-2031 Audit Plan

Summary

The proposed FY 2027-2031 audit plan outlines a diverse portfolio of projects spanning a five-year period, offering flexibility in scheduling audits across various departments and functions. The execution of this plan is contingent upon budget availability and will undergo annual revisions to reflect audit progress and address emerging risks. Amendments to the approved audit plan may be introduced during the year to adapt to changes in ORS's operational environment, including organizational structure, operations, risk profiles, systems, and controls.

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

Proposed Audit Plan for FY 2027 – 2031

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2027	IT	1099-R Reporting	Inaccurate information Unreconciled variances Delays in processing and communication to members Incorrect reporting to IRS Failure to comply with IRS filing deadlines/ requirements Inadequate validation between source systems and reported amounts Lack of audit trail supporting adjustments or corrections	**1099-R Reporting Advisory Project:** Assess the design and operating effectiveness of controls related to the organization's transition from the IRS FIRE system to the IRIS platform, including the integration between LRS (PensionGold) and Yearli. Evaluate whether risks associated with increased filing complexity, reliance on a new third-party vendor, data accuracy, and regulatory compliance are being appropriately identified, mitigated, and monitored.	180
FY 2027	Investments	Investment Manager Reconciliation	Inaccurate Net Asset Valuation (NAV) reported Late closing of books No resolution for variances Performance and compliance reporting delays Incomplete or inaccurate data received from investment managers Pricing discrepancies (e.g., stale or incorrect valuations for illiquid assets) Failure to reconcile capital calls, distributions, and expenses Lack of independent review and approval of reconciliations	**Investment Management Process:** Assess the design and effectiveness of controls over investment valuation and financial reporting, including accuracy of NAV, completeness and accuracy of data from investment managers, and timeliness of the close process. Evaluate controls over pricing and valuation, as well as reconciliations of capital calls, distributions, and expenses, including independent review and the timely identification and resolution of variances to ensure accurate and timely reporting.	250

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2028	Benefits	Service Purchase Contracts	Over/underestimated contract cost Eligibility requirements issues Improper set-up in Pension Gold & People Soft Untimely development/ processing of contracts Inadequate review of contracts Contract breach Incorrect calculation of interest or actuarial assumptions Failure to monitor payment schedules for contracts Unauthorized modifications to contract terms Lack of reconciliation between contract balances and payments received	**Service Purchase Contracts Audit:** Assess whether contracts administered by the retirement system are developed, approved, recorded, and monitored accurately and in a timely manner to ensure contract costs, interest calculations, eligibility requirements, actuarial assumptions, payment schedules, and system configurations (Pension Gold and PeopleSoft) are correct, authorized, and reconciled.	260
FY 2028	IT	IT Operations and System Administration	System downtime or availability issues Misconfigured systems or infrastructure Inadequate capacity planning or performance monitoring Lack of standard operating procedures Overreliance on key personnel (key person risk) Ineffective job scheduling and batch processing controls	**IT Cybersecurity & General Controls Audit:** Assess the design and effectiveness of IT general controls across the technology environment, including IT governance and compliance; identity and access management; logging and monitoring; physical security; change management; and system development and implementation. Evaluate controls over IT operations, cybersecurity and data protection, third-party vendor management, and application controls to ensure data is accurate, complete, and authorized. Assess controls over data access and management, as well as supporting controls such as security awareness and training and device and inventory management.	290
FY 2028	IT	Cybersecurity and Data Protection	Malware, ransomware, or phishing attacks Unpatched vulnerabilities and outdated systems Weak network security controls (e.g., firewalls, segmentation) Data breaches or unauthorized data exfiltration Lack of encryption for sensitive data Ineffective incident detection and response	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2028	IT	Logging, Monitoring, and Audit Trails	Insufficient logging of critical activities Logs not reviewed or monitored regularly Tampering or deletion of logs Lack of centralized logging or SIEM capabilities Inability to detect or investigate incidents Poor retention policies for audit logs	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A
FY 2028	IT	Physical Security	Unauthorized physical access to data centers or offices Theft or damage of hardware and devices Environmental threats (fire, flood, power failure) Inadequate surveillance or access controls (badges, biometrics) Poor asset management and tracking Lack of secure disposal of hardware/media	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A
FY 2028	IT	IT Governance and Management	Lack of alignment between IT strategy and business objectives Undefined roles, responsibilities, and accountability Inadequate IT policies, standards, or oversight Poor risk management framework or risk awareness Insufficient resource allocation or prioritization Weak decision-making and escalation processes	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A
FY 2028	IT	Identity and Access Management (IAM)	Excessive or inappropriate user access (violations of least privilege) Weak authentication mechanisms (e.g., no MFA) Orphaned or inactive accounts not deprovisioned Poor segregation of duties (SoD) conflicts Ineffective user provisioning/deprovisioning processes Credential theft or misuse	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2028	IT	Change Management	Unauthorized or unapproved system changes Inadequate testing leading to system failures or defects Lack of rollback procedures Poor documentation of changes Changes implemented directly in production Segregation of duties conflicts in change approval/deployment	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A
FY 2028	IT	Data Management and Data Integrity	Inaccurate, incomplete, or inconsistent data Unauthorized data modification or deletion Lack of data validation and reconciliation controls Poor data governance and ownership Inadequate backup and recovery processes Data corruption during processing or transmission	**Assessed as part of IT Cybersecurity & General Controls Audit**	N/A
FY 2029	Accounting	Benefit Disbursements Process	Lost checks Mailing checks to the wrong member Unreconciled differences Out-of-date bank information Improper recording of journal entries Inaccurate GL and trial balance Payments made to ineligible, deceased, or terminated members Failure to stop or adjust payments timely Incorrect tax withholding or reporting on benefit payments Lack of audit trail supporting benefit calculations and changes	**Benefits Disbursement Process:** Assess the design and effectiveness of controls over benefit payment processing and reporting, including payment execution, accuracy of benefit calculations, validation of member eligibility, and maintenance of member banking information. Evaluate controls to prevent unauthorized or misdirected payments, ensure accurate tax withholding and reporting, and maintain an adequate audit trail. Assess controls over financial recording and reconciliation, including journal entries, general ledger accuracy, and timely resolution of discrepancies.	300

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2029	Administration	Business Continuity	Operations shutdown Inadequate disaster recovery testing or outdated recovery plans Lack of staff awareness or training on BCP procedures Insufficient backup systems or data recovery capabilities Dependency on key vendors or systems without contingency arrangements	**Business Continuity & Disaster Recovery:** Assess whether the retirement system has adequately designed and operating business continuity and disaster recovery controls to ensure continuity of critical operations, timely recovery from disruptions, protection and recoverability of data, staff readiness to execute BCP/DR procedures, and resilience against vendor or system dependencies.	250
FY 2030	Investments	Investment Compliance Monitoring	Non-compliance with investment policies Failure to detect breaches of investment guidelines or restrictions Inadequate tracking of regulatory or policy changes Delayed remediation of compliance violations Lack of independent oversight or reporting of compliance activities	**Investment Management & Operations Audit:** Assess the design and effectiveness of controls over investment management and operations, including governance, portfolio construction and rebalancing, manager selection and oversight, and trade execution, with a focus on alignment with investment objectives and policies, risk management (including liquidity, solvency, and conflicts of interest), performance monitoring, and the accuracy and completeness of investment transactions and records.	400
FY 2030	Investments	Investment Process	Investment performance risk Investment opportunity cost Liquidity and solvency of plans Non-compliance with investment policies Unauthorized investment transactions or trades Execution errors (e.g., incorrect securities, quantities, or pricing) Lack of documentation supporting investment decisions Inadequate monitoring of manager performance and benchmarks	**Assessed as part of the Investment Management & Operations Audit**	N/A

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2030	Investments	Due Diligence	Investment performance risk Investment opportunity cost Liquidity and solvency of plans Inadequate assessment of manager risks (operational, financial, compliance) Failure to identify conflicts of interest Reliance on outdated or incomplete due diligence information Lack of documentation supporting due diligence conclusions	**Assessed as part of the Investment Management & Operations Audit**	N/A
FY 2030	Investments	Asset Allocation	Non-compliance with investment policies Investment diversification risk Investment opportunity cost Failure to rebalance portfolio in accordance with policy targets Overconcentration in specific asset classes, sectors, or managers Misalignment with long-term investment strategy or actuarial assumptions Inadequate monitoring of asset allocation drift	**Assessed as part of the Investment Management & Operations Audit**	N/A
FY 2030	IT	Compliance and Regulatory Requirements	Non-compliance with laws, regulations, or standards (e.g., GDPR, HIPAA) Inadequate documentation to support compliance Failure to implement required controls Regulatory penalties, fines, or reputational damage Lack of awareness of changing regulatory requirements Ineffective compliance monitoring	**Regulatory Compliance Audit:** Assess the design and effectiveness of the organization's compliance framework and related controls, including processes to identify and stay current with applicable laws and regulations, adequacy of policies and documentation, and implementation of required controls. Evaluate controls to monitor and enforce compliance, including ongoing monitoring activities, identification and remediation of non-compliance issues, and mitigation of regulatory and reputational risks.	150

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
FY 2031	Administration	Employee Training	Poor performance Higher chance of turnover Poor customer service and damage to reputation Slow productivity Operational errors Lack of role-specific or compliance-required training Inadequate tracking of training completion Training content not updated for regulatory or policy changes Ineffective knowledge transfer = control gaps	**Employee Training & Workforce Effectiveness:** Assess the design and effectiveness of controls over employee training and workforce effectiveness, including role-based and compliance-required training, tracking of completion, and timely updates to training content. Evaluate processes supporting knowledge transfer and whether gaps in training or staffing contribute to operational errors, reduced productivity, or customer service issues.	260
FY 2031	Benefits	Disability Payments	Inaccurate calculation of benefits Over/underpayment of disability retirement allowance Failure to adjust payments based on status changes (e.g., recovery, earnings limits) Incorrect tax treatment of disability payments Lack of periodic review of continued eligibility Inadequate reconciliation of disability payroll to approved benefits	**Disability Retirement Benefits Operational Audit:** Assess whether controls over disability retirement benefits are adequately designed and operating effectively to ensure benefits are calculated accurately, payments are made in the correct amounts and tax treatment, eligibility is periodically reviewed, status changes are appropriately reflected, and disability payroll is reconciled to approved benefit determinations	290
Audits of Remaining Functional Areas and Associated Risks To Be Determined (TBD) in Subsequent Audit Planning Cycles					
TBD	Accounting	ACFR Preparation	Improper presentation of financial statements Non-compliance with GAAP and other regulatory standards Inaccurate financial figures Lack of required disclosures Lack of review/approval controls over financial statements and disclosures Inconsistent application of accounting policies year over year Failure to incorporate actuarial data accurately (e.g., pension liabilities) Inadequate documentation supporting reported balances and disclosures	• Assess the design and effectiveness of controls over financial statement preparation and reporting, including compliance with applicable accounting standards and regulatory requirements, accuracy and completeness of financial data and disclosures, consistent application of accounting policies, management review and approval processes, incorporation of actuarial data, and adequacy of supporting documentation for reported balances and disclosures.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Accounting	Cash Disbursements Process	Delayed processing of payments Inaccurate payments Lack of internal controls Payments to wrong vendors Improper recording of journal entries Inaccurate GL and trial balance Duplicate or fraudulent payments (e.g., duplicate invoices, ghost vendors) Unauthorized disbursements due to weak approval controls Failure to detect or prevent payment fraud (e.g., vendor banking changes not validated) Inadequate segregation of duties between initiation, approval, and payment processing	• Assess the design, effectiveness, and efficiency of controls over payment processes, including timeliness and accuracy of payments, vendor validation (e.g., banking changes), and controls to prevent and detect fraudulent, unauthorized, or duplicate payments. Evaluate controls over approval processes and segregation of duties across payment initiation, approval, and processing, as well as the completeness and accuracy of related journal entries, general ledger activity, and financial reporting, including timely identification and correction of errors.	TBD
TBD	Accounting	Contribution Reconciliation	Incorrect contribution amounts Inaccurate amounts wired to custodian bank Improper recording of entries in GL Untimely correction of errors Uncorrected errors and exceptions Missing contributions (e.g., employers fail to remit but not detected) Misallocation of contributions to incorrect member accounts Failure to identify late contributions and assess penalties/interest Inadequate reconciliation between payroll reports and contributions received	• Assess the effectiveness of controls over contribution processing and financial recording, including calculation accuracy, amounts remitted to the custodian bank, general ledger entries, and timely identification and correction of errors or exceptions. (150)	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Accounting	Custodian Bank Reconciliation	Inaccurate Net Asset Valuation (NAV) reported Late closing of books Unreconciled variances Incomplete or inaccurate data feeds from custodian or internal systems Timing differences not properly tracked or resolved (cutoff errors) Unauthorized or unrecorded transactions at custodian level Lack of independent review of reconciliation and sign-off	• Assess the design and effectiveness of controls over financial reporting, including accuracy of NAV, timeliness of the close process, and proper recording of transactions. Evaluate controls over reconciliations and data integrity, including completeness and accuracy of data from custodians and internal systems, identification and resolution of variances and timing differences, and independent review and approval of reconciliations to ensure financial data is complete, accurate, and supported. (240)	TBD
TBD	Accounting	COLA Posting	Inaccurate calculation of benefits Over/underpayment of benefits Failure to apply COLA updates timely per policy or statute Application of incorrect COLA rates or eligibility criteria System configuration errors impacting bulk COLA updates Lack of review or validation of COLA adjustment outputs	• Assess the design and effectiveness of controls over benefit calculation processes, including accuracy and completeness of calculations, prevention of overpayments and underpayments, validation of calculation logic and outputs, and controls over periodic adjustments such as COLA, including timely application, accuracy of rates and eligibility criteria, system configuration for bulk updates, and review and validation of adjustment outputs.	TBD
TBD	Accounting	Interest Posting	Inaccurate interest amounts Over/underpayment for return of contributions Incorrect interest rate applied (e.g., statutory vs. system-configured rates) Failure to post interest for all eligible accounts or periods Timing errors in interest calculations (cutoff or compounding issues) Lack of reconciliation between calculated and posted interest amount	• Assess the design and effectiveness of controls over interest calculations for return of contributions, including accuracy of interest amounts, correct application of rates (e.g., statutory vs. system-configured), and prevention of overpayments or underpayments.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Administration	Communications Audit	Communication delays Compromised member's confidence Inaccurate or inconsistent information communicated to stakeholders Lack of documentation or audit trail of communications Failure to comply with public disclosure or transparency requirements Ineffective communication channels during critical events	• Assess the design and effectiveness of controls over stakeholder communication processes, including the timeliness, accuracy, and consistency of information communicated to members and other stakeholders, as well as compliance with applicable disclosure and transparency requirements.	TBD
TBD	Benefits	Deferred Vested	Processing ineligible member application Inaccurate records for deferred vested member's contributions and interest Over/underestimated monthly benefit Failure to track or notify members of eligibility for benefits Incorrect application of vesting rules or service credit Lack of periodic reconciliation of deferred member accounts Missing or incomplete member records impacting future benefits	• Assess whether controls over deferred vested member administration are adequately designed and operating effectively to ensure member applications are processed only when eligibility requirements are met, vesting rules and service credit are applied correctly, member records are complete and accurate, benefits are calculated appropriately, and deferred member accounts are periodically reconciled and monitored.	TBD
TBD	Benefits	Disability Retirement Application	Delayed processing of benefit payments Incorrect benefits set-up Insufficient medical documentation or review Failure to validate eligibility criteria for disability status Delays due to incomplete coordination with medical evaluators Lack of independent approval or oversight of disability determinations	• Assess the design and effectiveness of controls over the setup and processing of benefit payments, including timeliness of processing and accuracy of benefit configurations. • Assess the design and effectiveness of controls over disability determinations, including completeness and review of medical documentation, validation of eligibility criteria, coordination with medical evaluators, and independent approval or oversight of disability decisions.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Benefits	Member Death Verification	Untimely detection of member death Benefit overpayment Reliance on incomplete or inaccurate death data sources Failure to stop ancillary benefits (e.g., health benefits) timely Incorrect beneficiary identification or payment distribution Lack of periodic death match (e.g., SSA DMF) controls	• Assess the design and effectiveness of controls over member death identification and related benefit processing, including the use of reliable data sources (e.g., periodic death matches such as SSA DMF) to ensure timely and accurate detection. Evaluate controls to ensure prompt cessation of benefit and ancillary payments, accurate identification of beneficiaries and payment distribution, and prevention of overpayments, supported by adequate documentation and monitoring processes.	TBD
TBD	Benefits	Member Enrollment and Set-up	Ineligible employees enrolled in the retirement plans Members are enrolled in the incorrect tier and plan Incorrect information are established for new members. Duplicate member records created in the system Failure to collect or validate required supporting documentation Incorrect service credit or hire date established Lack of proper authorization or review of enrollment data	• Assess the design and effectiveness of controls over member enrollment data to ensure accuracy and completeness, including prevention of duplicate records, correct setup of member information (e.g., hire date, service credit), and appropriate plan/tier assignment. (140)	TBD
TBD	Benefits	Membership Termination	Untimely removal of terminated members in the system Members are inappropriately removed from the system (e.g., deferred vested) Continued accrual of benefits after termination date Failure to notify downstream systems (payroll, benefits) of termination Incorrect classification of termination status (e.g., vested vs. non-vested) Lack of review/approval for termination processing	• Assess whether terminated members are accurately, timely, and appropriately processed within the retirement system to ensure benefits cease as of the correct termination date, member status is properly classified, required reviews and approvals are performed, and termination information is communicated to all relevant downstream systems (e.g., payroll and benefits). (160)	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Benefits	Military Time Purchase	Over/underestimated contract cost Eligibility requirements issues Improper set-up in Pension Gold and People Soft Untimely development and processing of contracts Inadequate review of contracts Contract breach Inadequate verification of military service documentation Incorrect application of purchase rules or caps Failure to track installment payments and outstanding balances Lack of reconciliation between purchased service credit and system records	• Assess whether controls over service credit purchase contracts (including military service) are adequately designed and operating effectively to ensure member eligibility requirements are met, supporting documentation is properly verified, contract costs are calculated accurately, purchase rules and caps are correctly applied, contracts are developed and processed timely, and contracts are reviewed and approved to prevent errors or contract breach.	TBD
TBD	Benefits	Rehired Retirees	Non-compliance with laws and regulations Breach of tax status of the benefit plans Failure to monitor post-retirement employment limits (hours/earnings) Continued benefit payments when suspension is required Inadequate tracking of rehire status across departments Lack of timely reporting to regulatory or oversight bodies	• Assess whether controls are adequately designed and operating effectively to ensure compliance with applicable laws and regulations governing retirement benefits, including monitoring post-retirement employment limits (hours and earnings), tracking rehire status across departments, and identifying situations requiring suspension or adjustment of benefit payments.	TBD
TBD	Benefits	Return of Contributions	Delayed processing of refunds Inaccurate returned contribution, interest, and any tax withheld amounts Unauthorized or fraudulent refund requests Failure to obtain required approvals before processing refunds Incorrect tax reporting (e.g., 1099-R) Lack of reconciliation between refunded amounts and member balances	• Assess the design and effectiveness of controls over member refund processing and reporting, including validation and authorization of refund requests, accuracy of calculated amounts (e.g., contributions, interest, and withholding), and timeliness of processing. Evaluate controls to prevent unauthorized or fraudulent refunds, ensure correct tax treatment and reporting (e.g., Forms 1099-R), and support the completeness and accuracy of accounting and reconciliations, including timely identification and resolution of discrepancies.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Benefits	Service Retirement Application	Delayed processing of benefit payments Incorrect benefits set-up Incomplete or missing application documentation Failure to verify eligibility (age, service credit) prior to approval Incorrect selection of benefit options (e.g., survivorship options) Lack of independent review of retirement calculations	• Assess the design and effectiveness of controls over benefit setup and payment processing, including timeliness of processing, accuracy of benefit configurations, and completeness of required documentation. Evaluate controls to ensure proper verification of member eligibility (e.g., age and service credit), accurate selection of benefit options, and independent review and approval of retirement calculations prior to payment. (260)	TBD
TBD	Benefits	Reciprocity	Eligible employees not granted reciprocity Ineligible members granted reciprocity Untimely processing of reciprocity elections Incorrect calculation of service credit across systems Failure to obtain or validate data from reciprocal systems Miscommunication between agencies impacting benefit determinations Lack of documentation supporting reciprocity decisions	• Assess whether controls over reciprocity administration are adequately designed and operating effectively to ensure reciprocity elections are processed timely, eligibility determinations are accurate and supported, ineligible members are not granted reciprocity, and sufficient documentation is maintained to support reciprocity decisions.	TBD
TBD	IT	Access to Programs and Data	Unauthorized access Unauthorized changes Incorrect member profile leading to inaccurate contributions, benefits, etc. Excessive user access rights (violation of least privilege) Failure to timely remove access for terminated or transferred employees Lack of segregation of duties (e.g., users with conflicting access) Inadequate monitoring/logging of user access and activities	• Assess whether logical access controls over retirement system applications are adequately designed and operating effectively to ensure only authorized users have appropriate access, changes to member data are authorized and accurate, access is removed timely upon employee termination or role changes, segregation of duties is enforced, and user activities are appropriately monitored and logged.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	IT	Application Controls	Inadequate input validation (leading to erroneous data entry) Incorrect processing logic or calculation errors Lack of automated controls or overreliance on manual processes Unauthorized changes to application logic Weak interface and integration controls Insufficient error handling and exception reporting	• Assess whether application controls within key retirement system applications are adequately designed and operating effectively to ensure data is complete, accurate, authorized, and processed correctly, including controls over input validation, processing logic, system integrations, change management, and error handling	TBD
TBD	IT	Third-Party Vendor Management	Overreliance on vendors without proper oversight Inadequate due diligence or risk assessments Lack of clear contracts or SLAs Third-party security weaknesses impacting your environment Data sharing risks and privacy concerns Limited visibility into vendor controls and operations	• Assess whether third-party vendor risk management controls are adequately designed and operating effectively to ensure appropriate oversight, due diligence, contractual protections, security and privacy safeguards, and visibility into vendor controls and operations.	TBD
TBD	IT	Systems Development, Acquisitions, and Implementation	Changes are not implemented Unverified modifications System incompatibility and malfunction Inadequate user acceptance testing (UAT) Lack of formal change management & approval processes Data migration errors or loss during system implementation Insufficient training & documentation for end users	• Assess whether change management and system implementation controls are adequately designed and operating effectively to ensure changes are properly implemented, authorized, tested (including user acceptance testing), and approved; modifications are verified and documented; system compatibility and functionality are maintained; and data migration processes preserve data integrity, completeness, and accuracy.	TBD
TBD	Investments	Cash Projection Process	Cash overdrafts Idle cash balance Inaccurate forecasting assumptions (e.g., contributions, benefit payments, capital calls) Failure to incorporate upcoming liquidity needs (e.g., capital calls, redemptions) Lack of coordination between finance, investments, and operations Insufficient monitoring and updating of projections	• Assess the design and effectiveness of controls over cash flow forecasting and liquidity management, including the accuracy of forecasting assumptions (e.g., contributions, benefit payments, and capital calls), incorporation of upcoming liquidity needs (e.g., redemptions), and coordination across finance, investments, and operations, as well as timely monitoring and updating of projections, optimization of cash balances to minimize idle cash, and prevention of cash overdrafts.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Investments	Investment Cash Outflows (Wires and Internal Transfers)	Delayed processing of cash outflows Wires and internal transfers are sent to wrong Investment Managers Wires and internal transfers are not authorized and reviewed Incorrect amounts are sent Cash overdrafts Fraudulent wire requests or social engineering (e.g., spoofed instructions) Inadequate verification of banking instructions (e.g., changes not independently confirmed) Lack of segregation of duties between initiation and approval of transfers Failure to reconcile cash movements to custodian or bank records timely	• Assess whether controls over cash outflows, including wires and internal transfers to investment managers, are adequately designed and operating effectively to ensure transfers are authorized, reviewed, accurate, and timely; banking instructions are independently verified; segregation of duties is enforced; and the risk of fraudulent or socially engineered wire requests is mitigated.	TBD
TBD	Investments & Accounting	Investment Manager Fees	Over/underpayment of investment fees Inaccurate Net Asset Valuation (NAV) reported* Misinterpretation of fee agreements (e.g., tiered or performance-based fees) Failure to validate fee calculations against contracts Fees charged on incorrect asset values or periods Lack of transparency or supporting documentation from managers	• Assess the design and effectiveness of controls over investment fee calculation and validation, including interpretation of fee agreements (e.g., tiered and performance-based structures), accuracy of fee calculations, and alignment with applicable asset values and periods. Evaluate controls to ensure fees are validated against contractual terms, supported by adequate documentation from investment managers, and appropriately reflected in Net Asset Valuation (NAV) and financial reporting.	TBD
TBD	Investments	New Accounts Opening	Delays in account opening Investment opportunity cost Incomplete or incorrect account documentation (e.g., legal, tax forms) Unauthorized account openings or changes Failure to comply with KYC/AML requirements Incorrect account setup (e.g., ownership, authorized signers)	• Assess the design and effectiveness of controls over investment account setup and maintenance, including timeliness of account opening, completeness and accuracy of required documentation (e.g., legal and tax forms), and compliance with KYC/AML requirements. Evaluate controls to ensure accounts are established and modified only with appropriate authorization, account details (e.g., ownership and authorized signers) are accurate, and processes minimize delays and associated investment opportunity costs.	TBD

Planned Year	Division	Functional Areas	Potential Risks	Planned Audit & Scope	Planned Hours
TBD	Investments	Sweep Vehicle Process	Lost interest Cash overdrafts Incorrect sweep thresholds or parameters configured Failure to execute sweeps timely or completely Counterparty risk related to sweep vehicles (e.g., money market funds) Lack of monitoring of sweep activity and balances	• Assess the design and effectiveness of controls over cash sweep processes, including configuration of sweep thresholds and parameters, timely and complete execution of sweeps, and monitoring of sweep activity and balances. Evaluate controls to ensure optimization of interest earnings, prevention of cash overdrafts, and management of counterparty risk associated with sweep vehicles (e.g., money market funds).	TBD

Appendices

Appendix A: Audit Universe

Department
- **Key Function**

Accounting
- ACFR Preparation
- Benefits Disbursement
- Cash Disbursement
- COLA Posting
- Contribution Reconciliation
- Custodian Bank Reconciliation
- Interest Posting

Administration
- BCP
- Business Continuity
- Communications
- Employee Training

Benefits
- Deferred Vested
- Disability Payments
- Disability Retirement Application
- Member Death Verification
- Member Enrollment Set-up
- Member Termination
- Military Time Purchase
- Reciprocity
- Rehired Retirees
- Return of Contributions
- Service Purchase Contracts
- Service Retirement Application

Investments
- Asset Allocation
- Cash Projection Process
- Due Diligence
- Investment Cash Outflows (Wires and Internal Transfers)
- Investment Compliance Monitoring
- Investment Manager Fees
- Investment Manager Reconciliation
- Investment Process
- New Accounts Opening
- Sweep Vehicle Process

Information Technology (IT)
- 1099-R Reporting
- Access to Programs and Data
- Application Controls
- Compliance and Regulatory Requirements
- Change Management
- Cybersecurity and Data Protection
- Data Management and Data Integrity
- Identity and Access Management (IAM)
- IT Governance and Management
- IT Operations and System Administration
- Logging, Monitoring and Audit Trails
- Physical Security
- Third-Party Vendor Management
- Systems Development, Acquisitions, and Implementation

Appendix B: Risk Scoring Rubric

Impact

Score	Description	Service Delivery & Operational Impact	Financial & Resource Impact (Illustrative)	Public Trust & Reputational Impact	Legal, Regulatory & Political Impact
1 - Negligible	No discernible impact or very minor, easily absorbed.	Minor inconvenience; no disruption to core services.	Minimal financial waste (e.g., < $10,000); no impact on budget.	No public notice; minimal internal concern.	No breach of law/policy; minor administrative error.
2 - Low	Minor impact, manageable with existing resources, minimal disruption.	Minor disruption to non-critical services; easily rectified.	Low financial impact (e.g., $10,000 - $100,000); minor budget reallocation.	Limited negative perception internally or among immediate stakeholders.	Minor non-compliance with internal policies or less significant regulations.
3 - Medium	Moderate impact, requiring additional resources to manage, some disruption.	Moderate disruption to some core services; short-term delays or reduced quality.	Moderate financial impact (e.g., $100,001 - $1,000,000); potential for budget shortfall requiring minor adjustments.	Potential for negative local media attention or stakeholder concern; moderate erosion of trust.	Non-compliance with significant policies or minor statutory requirements; potential for low-level public inquiry.
4 - High	Significant impact, major disruption, significant resources required to manage.	Significant disruption or failure of critical services; inability to meet key mandates.	High financial impact (e.g., $1,000,001 - $10,000,000); significant budget deficit, requiring major financial intervention.	Widespread negative media attention; significant loss of public trust; political scrutiny.	Breach of significant laws, regulations, or constitutional mandates; potential for large fines, sanctions, or widespread public outcry.
5 - Critical	Catastrophic impact, existential threat to an agency/program, severe and long-lasting consequences.	Complete failure or sustained inability to deliver essential services; poses a threat to public safety or welfare.	Catastrophic financial impact (e.g., > $10,000,000); severe budget crisis, jeopardizing long-term financial stability.	Widespread public outrage, severe reputational damage, potential for loss of mandates, political fallout, loss of public confidence in government function.	Major legal action, criminal charges, legislative intervention, loss of delegated authority, impeachment proceedings.

Likelihood

Score	Description	Probability/Frequency	Qualitative Description (Public Sector Context)
1 - Rare	May occur only in exceptional circumstances.	< 5%	Has never happened in this or similar public entities; highly unlikely given current environment.
2 - Unlikely	Could occur at some time.	5% - 20%	Has occurred in other public sector entities, or there are very limited indicators it could happen here.
3 - Possible	Might occur or is likely to occur at some time.	21% - 50%	Has occurred infrequently within this entity, or there are known, albeit manageable, conditions that could lead to it (e.g., pending legislative changes).
4 - Likely	Will probably occur in most circumstances.	51% - 80%	Has occurred multiple times within this entity or sector; strong indicators or trends suggest it will occur (e.g., identified recurring audit findings, persistent capacity issues).
5 - Almost Certain	Is expected to occur in most circumstances.	> 80%	Is a recurring event or a known systemic issue within the entity; current conditions make it highly probable or inevitable (e.g., critical staffing shortages, outdated systems, consistent public complaints).