bakertilly

Internal Audit

City of San Jose Office of Retirement Services (ORS)

Audit Committee Meeting:

Risk Assessment and Proposed 5-Year Internal Audit Plan

Presenter: Kate Murdock, Senior Manager

May 21, 2026

Agenda

- Background
- Risk Assessment approach
- Risk Assessment Results
- Proposed Audit Plan

Background

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.

- The risk assessment process evaluates key risks across the organization's operations and functions
- Results of the assessment are used to prioritize audit areas based on risk level and impact

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." 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).
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 Approach

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

Planning
- Performed risk assessment interviews with key stakeholders and leadership

Information Gathering
- Reviewed key documents (strategic plans, audit, budgets, organizational materials)

Analysis
- Scored auditable units based on likelihood and impact of risks
- Prioritized high-risk areas to inform audit focus

Reporting
- Developed and documented the proposed internal audit plan

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*
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

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.

FY 2027 – 2031 Risk Assessment (Continued)

Listed in order of risk level, high to low

Division	Key Function	Risk Score	Previously Audited	Proposed Audit Plan Year
Benefits	Member Termination	9	FY2020	TBD
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

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.

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

Proposed Audit Plan for FY 2027 – 2031(p.2)

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

Proposed Audit Plan for FY 2027 – 2031 (p.3)

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

Proposed Audit Plan for FY 2027 – 2031(p.4)

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

Proposed Audit Plan for FY 2027 – 2031 (p.5)

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

Proposed Audit Plan for FY 2027 – 2031(p.6)

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

Proposed Audit Plan for FY 2027 – 2031(p.7)

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

Questions?

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.

Risk Scoring Rubric (continued)

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).