SERS Retirement Board Audit Committee
Regular Meeting Agenda
June 17, 2026
2:30 P.M.

1. Roll call (R)
2. Approval of March 18, 2026 minutes (R)
3. External Audit Update: Plante Moran
4. Internal Audit Update: Chief Audit Officer's Report
    - Q4 Update on the FY2026 Audit Plan
    - Status of Audit Recommendations
    - Recently Completed Audits and Other Activities
    - FY2027 Audit Plan
5. Review and Approve FY2027 Audit Plan (R)
6. Executive session pursuant to R.C. 121.22 (G) (1) to consider the employment and compensation of a public employee (R)
7. Approval of FY2027 Chief Audit Officer Goals (R)
8. Audit committee requests and follow-up items
9. Adjournment

SCHOOL EMPLOYEES RETIREMENT SYSTEM

AUDIT COMMITTEE

June 17, 2026

_____ P.M.

Roll Call:

Catherine Moss	_____
James Rossler	_____
Aimee Russell	_____

Guests in Attendance:

_____

_____

_____

_____

_____

SCHOOL EMPLOYEES RETIREMENT SYSTEM

APPROVAL OF MINUTES OF THE AUDIT COMMITTEE MEETING HELD ON March 18, 2026

_____moved and _____seconded , the motion to approve the minutes of the Audit Committee meeting held on March 18, 2026.

Upon roll call, the vote was as follows:

ROLL CALL:	YEA	NAY	ABSTAIN
Catherine Moss	_____	_____	_____
James Rossler	_____	_____	_____
Aimee Russell	_____	_____	_____

School Employees Retirement System	AUDIT COMMITTEE MINUTES		
Preparer	Megan Robertson	**Meeting Date**:	March 18, 2026
Committee Chair	Aimee Russell		
Agenda	1. Roll call (R) 2. Approval of December 17, 2025, minutes (R) 3. Executive session pursuant to R.C. 121.22 (G) (6) to discuss security matters (R) 4. Internal Audit Update: Chief Audit Officer's Report o Q3 Update on the FY2026 Audit Plan o Status of Outstanding Audit Recommendations o Recently Completed Audits and Other Activities i. ORSC Annual Audit Committee Report ii. Audit Committee Charter and Internal Audit charter o Internal Audit's Strategic Plan (FY2026 – FY2029) o GAP Assessment Results to the IIA Global Internal Audit Standards 5. Executive session pursuant to R.C. 121.22 (G) (1) to consider the employment of a public employee (R) 6. Audit committee requests and follow-up items 7. Adjournment		
Discussion	The meeting began in open session at 2:30 p.m. **Roll Call** The SERS Regular Audit Committee began with a roll call. The committee roll call was as follows: Catherine Moss, James Rossler, and Aimee Russell. Also in attendance was Maggie O'Shea, Representative of the Ohio Attorney General, along with members of the public who joined via Zoom. Staff Members: Steve Ritzer, Joe Marotta, Marni Hall, Richard Stensrud, Karen Roggenkamp, Vatina Gray, Nicole Whitacre, Olivia Hill, Jennifer Chao, and Megan Robertson. **Approval of Minutes (R)** Catherine Moss moved, and Jamie Rossler seconded the motion to approve the minutes of the Audit Committee meeting held on December 17, 2025. Upon roll call, the vote was as follows: Yea: Catherine Moss, James Rossler, Aimee Russell. The motion carried. **Executive session pursuant to R.C. 121.22 (G) (6) to discuss security matters (R)** Catherine Moss moved, and Jamie Rossler seconded the motion that the Audit Committee convene into Executive Session pursuant to R.C. 121.22 (G) (6) to discuss security matters. Upon roll call, the vote was as follows: Yea: Catherine Moss, James Rossler, Aimee Russell. The motion carried. The committee convened in executive session at 2:31 p.m. The committee returned to open session at 2:45 p.m.		

	Chief Audit Officer's Report Next, Mr. Ritzer provided a presentation on the status of his FY2026 Internal Audit Plan for the third quarter, reporting steady progress, with the portal audit completed, the purchasing and identity access audits underway, and HIPAA compliance efforts advancing without concerns from the committee. Continuous auditing reviews and audit recommendations show positive movement, with outstanding items decreasing and most scheduled for completion by end of FY2026. The Audit Committee and Internal Audit charters were discussed with no recommended changes at this time. The committee reviewed the new long-term internal audit strategic plan and GAP assessment to the updated IIA standards and had no questions or comments on any items. Recently completed audits and other activities were also briefly discussed. There were no comments or questions from the Committee. **Executive session pursuant to R.C. 121.22 (G) (1) to discuss the employment of a public employee (R)** Catherine Moss moved, and Jamie Rossler seconded the motion that the Audit Committee convene into Executive Session pursuant to R.C. 121.22 (G) (1) to discuss the employment of a public employee. Upon roll call, the vote was as follows: Yea: Catherine Moss, James Rossler, Aimee Russell. The motion carried. The committee convened in executive session at 3:10 p.m. The committee returned to open session at 3:29 p.m. **Committee Requests and Follow Up Items** The next audit committee meeting will be on June 17, 2026. There were no requests or follow-up items discussed. The meeting adjourned at 3:29 p.m.

	Action Items	**Assigned Person**	**Due Date**
Action Items	n/a		
Agenda for Next Meeting			

_____ _____

Aimee Russell, Committee Chair Richard Stensrud, Secretary

School Employees Retirement System of Ohio Audit Committee Pre-Audit Communication

Representing Plante Moran:
Ashley Raden

Your Team

Kristin Hunt, CPA
Engagement Partner

- 30 years of experience
- A leader in the firm's public employee retirement system audit practice with 20 years of experience serving as a specialist in this area

Ashley Raden, CPA
Senior Manager

- 10+ years of experience serving governmental clients with a specialty in public employee retirement systems
- Experience auditing pension plans and governmental organizations and serves as a benefit plan audit specialist

Agenda

- Pre-Audit Communication
  - Audits to Perform
  - Auditor Responsibilities
  - Identification of Significant Risks
  - Plante Moran's Approach to Internal Control
  - Materiality Concept
  - Audit Committee Member Views
- Expected Audit Timeline
- Accounting Standard Changes for FY 2026
- Questions

Pre-Audit Communication

Pre-Audit Communication

Plante Moran will perform an audit and express an opinion on the following statements:

- SERS Annual Comprehensive Financial Report as of and for the year ended June 30, 2026
- Audit in accordance with GASB 68 of the Schedule of Employer Allocations and Schedule of Collective Pension Amounts by Employer for the measurement year ended June 30, 2026
- Audit in accordance with GASB 75 of the Schedule of Employer Allocations and Healthcare Amounts by Employer for the measurement year ended June 30, 2026

Pre-Audit Communication

Auditor Responsibilities

- Express an opinion about whether the financial statements prepared by management are fairly presented, in all material respects, in accordance with GAAP
- Communicate noncompliance with provisions of laws, regulations, contracts or grants that have a material effect on the financial statements that come to our attention
- In accordance with Generally Accepted Government Auditing Standards (GAO Standards), we are required to communicate all noncompliance with provisions of laws, regulations, contracts, or grants that have a material effect on the financial statements that comes to our attention.

Pre-Audit Communication

Identification of Significant Risks

- Accuracy of participant census data and the assumptions underlying the determination of both the total pension liability and total OPEB liability under GASB 67 and GASB 74, respectively
- Management override of controls
- Income recognition related to alternative investment income, along with gains and losses

Additional Significant Focus Areas

- Appropriate valuation of investments, particularly the alternative investments that do not have readily established market values
- Related to both Schedules of Employer Allocations, the calculation of the Collective Pension/OPEB amounts as well as the allocation methodology
- Accuracy of benefit calculations and related payments
- Changes made during the year related to controls surrounding cash reconciliations

Pre-Audit Communication

Plante Moran's Approach to Internal Control

- Narratives/Questionnaires
- Observation and inspection of procedures
- Effectiveness of controls over investments
- No opinion on effectiveness of internal controls

Materiality Concept

We place greater emphasis on those items that have, on a relative basis, more importance to the financial statements and greater possibilities of material error than with those items of lesser importance or those in which the possibility of material error is remote.

Expected Audit Timeline

Our anticipated timeline is as follows:

- Interim testing/understanding of controls – June 2026
- Fieldwork testing – Mid-September – Mid-October 2026
- Review ACFR – November 2026
- Audit opinion – by November 30, 2026
- Audit committee presentation – December 2026
- GASB 68 and 75 reports – February 2027

Accounting Standards Changes

GASB Statement No. 103, *Financial Reporting Model Improvements*

- What is the scope and potential impact?
  - Enhancements to the MD&A, proprietary fund statement presentation, budgetary comparison information, unusual or infrequent items, major component unit presentation, and financial trends in the statistical section.
  - For SERS, the most significant impact is likely on the MD&A enhancements, which under the standard will focus on five specific sections and placing emphasis on explaining why significant changes occurred.
  - SERS will need to consider how current MD&A aligns with this new standard and implement any changes to ensure compliance with the new standard.
  - Management is working on evaluation of the impact of this new standard.
- When is this effective?
  - SERS's Fiscal Year Ending June 30, 2026

Accounting Standards Changes

GASB Statement No. 104, *Disclosure of Certain Capital Assets*

- What is the scope and potential impact?
  - Requires certain types of capital assets (lease assets, intangible right-to-use assets, subscription assets, and other intangible assets) to be disclosed separately and introduces new disclosure requirements for capital assets identified as held for sale.
  - Management is working on evaluation of the impact of this new standard.
- When is this effective?
  - SERS's Fiscal Year Ending June 30, 2026

Questions?

We greatly appreciate the opportunity to serve you!

Contact Information:

Kristin Hunt, CPA

Engagement Partner

Kristin.Hunt@plantemoran.com

419.842.6110

Ashley Raden, CPA

Senior Manager

Ashley.Raden@plantemoran.com

586.416.4931

Internal Audit Update

June 2026

Agenda

- **Q4 Update on the FY2026 Audit Plan**
- **Status of Outstanding Audit Recommendations**
- **Recently Completed Audits and Other Activities**
  - FY27 Internal Audit Budget
  - Internal Audit Mandate
  - Audit Committee Calendar
- **FY27 Audit Plan**

Q4 Update on FY2026 Audit Plan

FY2026 Audit Plan Status

Audit	Type	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Progress	Notes
Undue Influence (issued 8.8.25)	compliance													100%	issued
Conflicts of Interest (issued 10.31.25)	compliance													100%	issued
Investment Incentive Compensation (issued 10.2.25)	compliance													100%	issued
Required Minimum Distribution (issued 11.24.25)	audit													100%	issued
Member Self-Service Portal (issued 3.6.26)	audit													100%	issued
Purchasing/Contracts (issued 5.13.26)	audit													100%	issued
Identity and Access Management (Finance)	audit													80%	
Continuous Auditing	audit														
Audit Committee Annual Report	administrative													100%	submitted
Fiscal Year 2027 Internal Audit Plan	administrative													100%	
Internal Audit Strategic Plan - FY26 - FY29	administrative													100%	
Internal Audit Recommendations Follow-up	administrative														
Other Consulting/Special Projects	consulting														
IT Consulting	consulting														
Health Care Medical/Pharmacy Claims	consulting														

Continuous Auditing

Area	Frequency	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Notes
Accounts payable	bi-monthly		■		■		■		■		■		☐	
Credit card transactions	bi-monthly		■		■		■		■		■		☐	
Member refund testing	quarterly					■			■			■		
Bank account changes	quarterly					■			■			■		
Address changes	quarterly					■			■			■		
Data fix changes	quarterly					■			■				☐	
Duplicate transactions	quarterly				■				■				☐	
Disability	quarterly					■			■				☐	
Vendor/SERS employee comparison	annually						■							
Badge access	annually									■				
Review of service credit	annually									■				
Active employees vs. Active Directory users	annually						■							
Merit increases	annually												☐	June/July

FY2026 Audit Plan Status

Engagement	Qtr.	Type	Status	Comments
FY25: Audit				
IT Infrastructure (issued 8/29/25)	Q4 2025	Audit	Completed	Outsourced Audit
FY26: Compliance				
Undue Influence (issued 8/8/25)	Q1	Audit	Completed	
Conflicts of Interest (issued 10/31/25)	Q2	Audit	Completed	
Investment Incentive Compensation (issued 10/2/25)	Q2	Audit	Completed	
FY26: Audit				
Required Minimum Distribution (issued 11/24/25)	Q2	Audit	Completed	

FY2026 Audit Plan Status

Engagement	Qtr.	Type	Status	Comments
FY26: Audit				
Member Self-Service Portal (issued 3/6/26)	Q2 – Q3	Audit	Completed	
HIPAA Compliance	Q3 – Q4	Audit	Deemed not necessary	Deemed not necessary based on SERS hiring a HIPAA Compliance Officer, additional training, and a new HIPAA Compliance Manual.
Identity and Access Management (Finance)	Q4	Audit	Pending	Fieldwork in process
Purchasing/Contracts (issued 5/13/26)	Q3-Q4	Audit	Completed	
Continuous Auditing	Q1- Q4	Audit	Ongoing	

FY2026 Audit Plan Status

Engagement	Qtr.	Type	Status	Comments
FY26: Consulting				
Other Consulting/Special Projects	Q1- Q4	Consulting	Ongoing	
IT Consulting	Q1- Q4	Consulting	Ongoing	
Health Care Medical/Pharmacy Claims	Q1- Q4	Consulting	Ongoing	
FY26: Internal Audit Activities				
Annual Audit Committee Report	Q2 - Q3	Administrative	Completed	Annual Activities for Ohio Retirement Study Council
Internal Audit Strategic Plan	Q3	Administrative	Completed	
Fiscal Year 2027 Internal Audit Plan	Q3 - Q4	Administrative	Completed	
Internal Audit Recommendations Follow-up	Q1- Q4	Administrative	Ongoing	

Status of Outstanding Audit Recommendations

Status of Audit Recommendations - Overall

Audit	Deficiency	Moderate	Total
External auditor			
Segregation of duties in change mgmt.	1		1
Management requested audits (outsourced) *			
Identity & Access Management		3	3
IT Infrastructure		1	1
Internal audit			
Purchasing/Contracts		1	1
Member Self-Service Portal		1	1
Total	**1**	**6**	**7**

* These were audits requested by management and performed by third-parties.

Audit Recommendations Q3 to Q4

Audit	Q3 FY26	Change	Q4 FY26
External audit			
Segregation of duties in change mgmt.	1	0	1
Internal audit			
Purchasing/Contracts	0	2	1
Purchasing/Contracts		(1)	
Member Self-Service Portal	1	0	1
Management requested audit (outsourced)*			
Identity & Access Management (note 1)	3	0	3
IT Infrastructure *	4	(3)	1
Total	**9**	**(2)**	**7**

Note 1: Management is actively addressing these recommendations through process improvements and software solutions. Evaluation and procurement of tools can cause revised implementation dates.

Status of Audit Recommendations – MSS Portal

Internal Audit

An internal audit of the Member Self-Service Portal was performed in 3rd QTR FY26.

Recommendations

There were two moderate risk recommendations.

Audit details

The details of the audit were discussed in executive session at the March 2026 Audit Committee meeting.

Corrective Action Plan

One recommendation has been corrected.

One recommendation has an implementation date through 1st QTR FY27.

Status of Audit Recommendations – Identity and Access Management

Outsourced Audit

An outsourced audit of Identity and Access Management was completed in 4th QTR FY24.

Audit details

The details of the audit were discussed in executive session at the June 2024 Audit Committee meeting.

Recommendations

There were six moderate risk recommendations.

Corrective Action Plan

Three recommendations corrected to date.

Two recommendations have revised implementation dates through 4th QTR FY26 and one revised through 1st QTR FY27.

Status of Audit Recommendations – IT Infrastructure

Outsourced Audit

An outsourced audit of IT Infrastructure was performed in 4th QTR FY25.

Audit details

The details of the audit were discussed in executive session at the September 2025 Audit Committee meeting.

Recommendations

There were two high and five moderate risk recommendations.

Corrective Action Plan

Six recommendations have been corrected.

One recommendation has a revised implementation date through 1st QTR FY27.

Recently Completed Audits and Other Activities

Recently Completed Audits and Other Activities

Recently Completed Audits

- One audit completed since the last committee meeting:

  Purchasing/Contracts (Attachment A). This audit was to review documentation and approvals for purchase orders and new vendors.

Other Activities

- FY27 Audit Committee Calendar (Attachment B)
- Optional Audit Committee Training (Attachment C)
- Internal Audit Operations Manual
  - Updated to reflect current practices
- Internal Audit FY27 Draft Budget
- Internal Audit Mandate

Internal Audit Advisory/Consulting Services

Risk

- Weekly team meetings
- Risk register review meetings
- Fiduciary self-assessment meetings
- Risk maturity model assessment

Executive

- Weekly Senior Leadership meetings
- Monthly Director meetings
- Information Governance committee
- Strategic Leadership panel for Emerging Leader group

Internal Audit FY27 Draft Budget

- **Responsibility under the Internal Audit Charter:**
  - The CAO will report periodically to the Audit Committee and senior management regarding:
    - Internal audit budget

Budgeted item	FY27	FY26	Change
Audit Services	$50,000	$40,000	$10,000
Training	2,750	2,000	750
Transportation and travel	1,800	1,500	300
Membership subscriptions	1,255	1,135	120
Total	**$55,805**	**$44,635**	**$11,170**

Note: The increase relates to the actual FY26 outsourced audit service of $44,999 vs the budget of $40,000. Due to inflation, the budgeted outsourced audit service was increased to $50,000.

Internal Audit Mandate

What is an internal audit mandate? This outlines the authority of the internal audit function in an organization.

Required by the IIA's Global Internal Audit Standards (2024):

- **Standard 6.1 – Internal Audit Mandate requires:**
  - The chief audit executive must provide the board and senior management with the information necessary to establish the internal audit mandate. In those jurisdictions and industries where the internal audit function's mandate is prescribed wholly or partially in laws or regulations, the internal audit charter must include the legal requirements of the mandate. The chief audit executive must document or reference the mandate in the internal audit charter, which is approved by the board.

Below excerpt from the Internal Audit Charter

AUTHORITY

SERS internal audit function mandate is found in ORC 3309.044, which states "The school employees retirement board shall appoint a committee to oversee the selection of an internal auditor. The committee shall select one or more persons for employment as an internal auditor. The board shall employ the person or persons elected by the committee." The internal audit function's authority is created by its direct reporting relationship to the Audit Committee. Such authority allows for unrestricted access to the Audit Committee.

Proposed FY27 Audit Plan

Proposed FY27 Audit Plan

Purpose:

The purpose of the audit plan is to define the work that will be completed in FY2027.

Objective:

Fulfill the requirements of the SERS Internal Audit Charter by conducting a risk assessment and the completion of the audit plan for the upcoming fiscal year.

The audit plan focuses on high and medium risk areas, provides assurance over key pension operations, maintains flexibility for emerging risks, while staying aligned with the Enterprise Risk Management (ERM) risks.

Present the audit plan to the Audit Committee for review and approval.

Proposed FY27 Audit Plan

Why perform a Risk Assessment?

Required by the IIA's Global Internal Audit Standards (2024):

- **Standard 9.4 – Internal Audit Plan requires:**
  - The chief audit executive (CAE) must create an internal audit plan that supports achievement of the organization's objectives.
  - The CAE must base the internal audit plan on a **documented assessment of the organization's strategies, objectives, and risks.** This assessment must be **informed by input from the board and senior management** as well as the CAE's understanding of the organization's governance, risk management, and control processes.
  - The assessment must be **performed at least annually,** be dynamic and updated timely in responses to changes in the organization's business, risk operations, programs, systems, controls, and organizational culture.

Proposed FY27 Audit Plan

Why perform a Risk Assessment? *(continued)*

- **Responsibility under the Audit Committee Charter:**
  - **3.1** Review and approve the Internal Audit Charter, **plans,** activities, staffing, and organizational structure of the internal audit activity, including succession planning.

- **Responsibility under the IA Charter:**
  - The CAO has the responsibility to at least annually, develop a **risk-based internal audit plan** that considers the input of the Audit Committee and senior management. Discuss the plan with the Audit Committee and senior management and submit the plan to the Audit Committee for review and approval.

FY27 Audit Plan Process

Information Gathering and Scoping

- Reviewed historical audit coverage
- Gained understanding of industry trends and business sector risks
- Reviewed SERS' Strategic Plan objectives for alignment
- Reviewed ERM's risk register for alignment
- Updated the Audit Universe, including documentation of organization's processes, risks, and controls

Risk Assessment

- Surveyed Members of the Board
- Meetings with SERS' Leadership
- Assessed significant changes throughout the organization
- Reviewed management's risk assessment of key processes

Developing and Vetting Proposed Audit Plan

- Developed draft audit plan based on information gathering and risk analysis
- Shared draft risk assessment and audit plan with senior management
- Shared draft risk assessment and audit plan with Audit Committee members
- Incorporated feedback

Obtain Audit Committee Approval

- Present to Audit Committee the results of the risk assessment and audit plan development process
- Discuss draft FY27 Audit Plan with Audit Committee
- Request Audit Committee approval of the FY27 Audit Plan

Risk Assessments and Cycle

Risks consider numerous factors and undergo a standard evaluation process.

FY27 Audit Plan Overview

The risk assessment and audit plan process included the following:

- ❑ Nine department/senior leadership meetings with approximately 40 leaders that involved discussions to risk score each audit unit which then produced a risk ranked list of audit units.
- ❑ In addition, a meeting was held with the external auditors to avoid duplication of audit coverage.
- ❑ The risk ranked units were aligned with the risk categories identified by ERM.
- ❑ This was then used to build the FY27 Internal Audit Plan. See “Attachment D”

Risk Assessment: Factors

Factors considered in selecting projects to include in the IA plan:

- ❑ Input from management and the Audit Committee
- ❑ Significant changes in systems or processes; recently completed or expected to be completed soon
- ❑ The time since the entity was last audited and the results
- ❑ Anticipated coverage through other monitoring/compliance functions and external audit
- ❑ Overall risk rating
- ❑ Available resources

Risk Assessment: Collaboration

IA, along with ERM, met with the below areas to discuss the current risk environment including any major changes that have occurred, assign risk factors to the various audit units, and to provide input on audit units to include in the FY27 Audit Plan.

.

- Information Technology
- Enterprise Risk Management
- Legal, Communications, & Government Relations
- Health Care
- Building & Tenant Services
- Member Services
- Investments
- Administrative Services
- Finance
- Plante (external auditors)

Developing and Vetting Proposed Audit Plan

The risk assessment process, along with ongoing communications with ERM, resulted in specific projects intended to be performed in the upcoming fiscal year. These are defined as:

- FY27 Audit Plan Detail by Category
  - Includes each project and an estimated time to complete per category

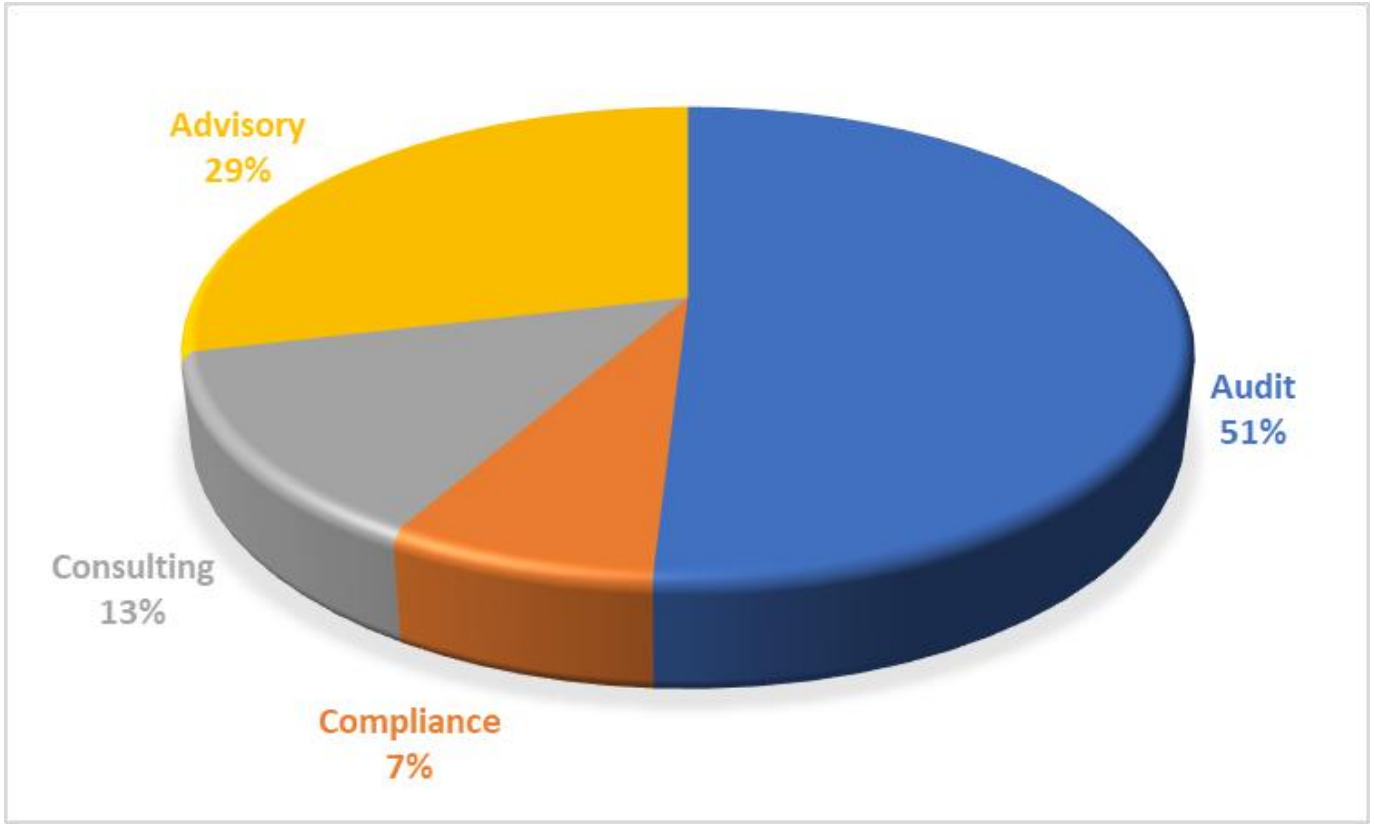
- FY27 Audit Plan and ERM Alignment
  - Ensures FY27 Audit Plan and ERM are in alignment on risks

FY27 Audit Plan Detail by Category

The below reflects the detail within each project type.

 Audit	 Compliance	 Consulting	 Advisory Services
Assess evidence available to provide assurance on an audit objective	Determine specific steps to test with management's agreement and report on results	Departmental consulting and special projects related to various processes.	Participate in activities in a non-voting capacity
• Continuous Auditing • Health Care Audits (pharmacy/medical) • Health Care Premiums • Experience Study • Member Service Team • Qualified Excess Benefit Arrangement (QEBA) • ETF Investments • IT Change Management • Investment Compliance with Clearwater	• Undue Influence • Investment Incentive Compensation • Conflict of Interest	• Fiduciary Audit • Health Care Documentation	• Disaster Recovery Plan • ORSC Annual Audit Plan • FY28 Audit Plan • Open audit recommendations • Audit Committee meeting preparation • Senior Leadership Team/Director/Other Meetings
Total: 9	Total: 3	Total: 2	Total: 6
~940 hours	~140 hours	~240 hours	~530 hours

FY2027 Audit Plan Coverage by Project Type



Category	Hours
Audit	940
Compliance	140
Consulting	240
Advisory	530
Total	1,850

FY27 Audit Plan and ERM Alignment

Internal Audit has ongoing communications with ERM as it relates to their evaluation of risk. This involved including ERM in the risk assessment meetings with management and weekly IA/ERM meetings to discuss ongoing and emerging risks at SERS. This resulted in the following alignment:

- ❑ Major Risk Categories identified by ERM aligned with audit coverage
- ❑ Major Risk Categories identified by ERM aligned with individual activities in the FY27 Audit Plan
- ❑ Emerging Risks identified by ERM aligned audit coverage

ERM Alignment: Major Risk Categories vs. Audit Coverage

The below reflects the link between the major risk categories identified by ERM and how that aligns with the audit coverage.

Risk Categories (ERM)	FY27 Audit Plan	External Auditor	Fiduciary Audit
Sustainability Risk			✓
Investment Risk	✓	✓	✓
Operational Risk	✓		✓
Cyber & Technology Risk	✓		✓
Reputational Risk	✓		✓
Compliance & Regulatory Risks	✓	✓	✓
Vendor Risk			✓

Note: The FY27 Audit Plan is risk based and constrained by limited resources. As a result, the plan does not include low risk rated areas or areas covered by the external auditors.

ERM Alignment: Major Risk Categories vs. FY27 Audit Plan

The below reflects the link between the major risk categories identified by ERM and the individual activities included in the FY27 Audit Plan.

Risk Categories (ERM)	FY27 Audit Plan
Investment Risk	• ETF Investments • Investment Compliance with Clearwater
Operational Risk	• Member Services Team • QEBA • Healthcare Premiums
Cyber & Technology Risk	• Participate in Disaster Recovery Plan exercise
Reputational Risk	• Conflicts of Interest • Undue Influence
Compliance & Regulatory Risks	• Conflicts of Interest • Undue Influence • Information Governance Requirements

ERM Alignment: Emerging Risks vs. Audit Coverage

The below reflects the link between the emerging risks identified by ERM and how that aligns with the audit coverage.

Emerging Risks (ERM)	Audit Coverage/Advisory Support
Fraud	• Continuous auditing
Artificial Intelligence	• Become member of AIOC
Vendor cyber hygiene	• Weekly meetings with ERM
Regulatory/Political Environment (legislative changes)	• Participate in Senior Leadership and Director meetings

Risk Rating Summary by Department

The Internal Audit risk assessment resulted in 100 auditable units among the respective departments.

Department	Low	Medium	High	# of Auditable Areas	Included in FY27 Audit Plan
Building & Tenant Services	0	3	0	3	0
Health Care	0	6	0	6	2
Finance	1	17	1	19	1
Legal, Communications, & Government Relations	0	14	0	14	0
Administrative Services	3	5	0	8	0
Investments	2	11	1	14	4
Member Services	0	12	4	16	2
Information Technology	0	10	2	12	1
ERM	0	6	2	8	1
Total	**6**	**84**	**10**	**100**	**11**

Q & A

SERS AUDIT COMMITTEE – APPROVAL OF FY 2027 INTERNAL AUDIT PLAN

_____ moved and _____ seconded the motion that the FY2027 Internal Audit Plan, as discussed at the June 2026 Audit Committee meeting, be approved.

Upon roll call, the vote was as follows:

ROLL CALL:	YEA	NAY	ABSTAIN
Catherine Moss	_____	_____	_____
James Rossler	_____	_____	_____
Aimee Russell	_____	_____	_____

EXECUTIVE SESSION

_____ moved and _____ seconded the motion that the Audit Committee convene in Executive Session pursuant to R.C. 121.22 (G)(1) to consider the employment and compensation of a public employee.

Upon roll call, the vote was as follows:

ROLL CALL:	**YEA**	**NAY**	**ABSTAIN**
Catherine Moss	_____	_____	_____
James Rossler	_____	_____	_____
Aimee Russell	_____	_____	_____

IN EXECUTIVE SESSION AT _____ A.M./P.M.

RETURN TO OPEN SESSION _____ A.M. / P.M.

SERS AUDIT COMMITTEE – APPROVAL OF CHIEF AUDIT OFFICER GOALS FOR FY 2027

_____moved and _____seconded the motion to approve the Chief Audit Officer's goals for FY 2027.

Upon roll call, the vote was as follows:

ROLL CALL:	YEA	NAY	ABSTAIN
Catherine Moss	_____	_____	_____
James Rossler	_____	_____	_____
Aimee Russell	_____	_____	_____

AUDIT COMMITTEE REQUESTS AND FOLLOW-UP ITEMS

ADJOURNMENT

_____moved that the Audit Committee adjourn to meet at its next regularly scheduled audit committee meeting.

The meeting adjourned at _____ p.m.

_____
Aimee Russell, Audit Committee Chair

Internal Audit Department

To: SERS Audit Committee, Board of Trustees

cc: Richard Stensrud, Executive Director
Karen Roggenkamp, Deputy Executive Director
Marni Hall, Chief Financial Officer
Joe Marotta, General Counsel
Colette Barricks, Chief Risk Officer

From: Steve Ritzer, Chief Audit Officer

Date: May 13, 2026

Re: Purchasing/Contracts Audit

EXECUTIVE SUMMARY

Internal Audit has completed the Purchasing/Contracts audit, as included in the *Fiscal Year 2026 Audit Plan.* The audit objective was to evaluate whether purchases and contracts were authorized, processed, and properly recorded in accordance with SERS' procurement process.

Based on the audit results, Internal Audit determined that overall management controls for the Purchasing/Contracts were operating effectively to achieve the business objective. Internal Audit did not identify any high-risk audit observations but did identify two moderate risk and one low risk audit observations.

The overall audit conclusion was determined to be well-controlled with improvement needed for the Purchasing/Contracts process during the audit period January 1, 2025, through December 31, 2025.

The audit objective, scope, methodology and conclusion are described later in the report.

POSITIVE RESULTS

Personnel responsible for purchasing are very knowledgeable of the purchasing workflow process.

Proper supporting evidence and controls were in place and operating effectively during the audit period (January 1, 2025, through December 31, 2025). Audit results were validated through inquiry, observation, and sample testing of transactions.

Internal Audit was grateful for the assistance and time provided in support of this audit by personnel in the Finance department. Internal Audit conducted interviews and would especially like to thank the following individuals for their cooperation, courtesy and professionalism provided on this engagement:

- Marni Hall, Chief Financial Officer
- Maria Robinson, Assistant Director - Finance
- Donita Thomas, Purchasing Coordinator

Steve Ritzer, CIA, CPA, CFE
Chief Audit Officer

BACKGROUND

SERS' management procures goods and services on behalf of the system and maintains a fiduciary role in exercising their discretionary authority. As a result, SERS has adopted policies and procedures below to obtain the best price, quality, and service for all goods and services.

POLICY, PROCEDURE, AND COMPLIANCE REQUIREMENTS (EXCERPTS from the respective policies)

Purchasing Policy

Purchasing Responsibilities

The Finance department is responsible for the administration of purchasing policies and procedures, and the purchasing of all goods and services. No other SERS department may have any policies, procedures, or forms that conflict with this policy or its related procedures or forms. Each Department Director shall authorize one or more employees to make purchasing decisions and to implement such decisions as required or permitted by SERS policies and procedures.

Purchasing Authority

A Department Director or their designee may approve and sign agreements for the purchase of goods and/or services included in their approved budget for amounts up to $20,000 per agreement. SERS' General Counsel shall have purchasing authority comparable to that of a Department Director. The Executive Director or Deputy Executive Director shall approve the purchase of goods and/or services in any amount above $20,000. If the purchase of goods and/or services will exceed the agreement limits noted above, an employee shall not divide such purchases in order to circumvent the authority to approve such purchases.

Solicitation and Selection of Vendors

Except as otherwise provided in SERS policies or procedures, all purchases of goods and/or services shall be obtained through competitive selection. Competitive selection requires the use of a Price Quote (PQ), Request for Quotation (RFQ), or Request for Proposal (RFP).

Purchases shall not be divided into multiple purchases or across fiscal years in order to circumvent the requirements above.

If a purchase is over $50,000, the vendor must complete a Standards of Conduct form (PUR-7005) prior to the execution of an agreement.

Contract Review and Execution Policy

Contract Review and Approval

All contracts and agreements must be reviewed by the Legal Department prior to execution. When applicable, SERS' contract templates should be used. Templates can be found in the Forms library. If using an external party's template agreement, SERS' standard terms and conditions should be included to the extent possible. If applicable, SERS' business associate agreement should be included.

Vendor Risk Management Policy

Assessment of Risk Posed by Third Party Relationships

Request for Proposal (RFP), Request for Quotation (RFQ), operational due diligence summary memos, and contract renewal assessments help SERS better understand the risk and control environment associated with a proposed vendor, product, or service. These evaluations help evaluate security practices, processes and policies, financial stability, and reputation.

BUSINESS OBJECTIVES, RISKS, AND CONTROLS

Internal Audit obtained information about the following business objective, as well as the related risks and controls management established to mitigate these risks:

Business Objective	Ensure purchases and contracts are authorized and processed in accordance with SERS' procurement process.
Business Risks	• Noncompliance with policy/procedures • Bid procedures not properly followed • Ineffective monitoring • Unapproved purchases • Vendor fraud or conflicts-of-interest • Split purchases to bypass bidding requirements
Management Controls **(Bold = Tested)**	• **Written policies/procedures** • **Authorizations and audit trails (including ERM and legal's review prior to final sign-off)** • **Required documentation per policy** • **Segregation of duties** • Reconciliations • Cross training & succession planning • Restricted files and access • Fraud and ethics training • Business continuity and recovery plans • System edits and access controls in NetSuite

AUDIT OBJECTIVE, SCOPE, METHODOLOGY, AND CONCLUSION

Internal Audit aligns its audit practices with the Institute of Internal Auditors' *Global Internal Audit Standards (the Standards)*.

These *Standards* require IA to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the conclusions based on the audit objective. Internal Audit believes the evidence obtained provides a reasonable basis for Internal Audit's findings and conclusions based on the audit objective.

Audit Objective	The audit objective was to evaluate whether purchases and contracts were authorized, processed, and properly recorded in accordance with SERS' procurement process.
Audit Scope	The scope was to verify whether all necessary documentation and approvals were obtained for purchase orders and new vendors (>$50,000) during 2025. Audit Period: January 1, 2025 – December 31, 2025 Populations and sample sizes included during the audit period: <u>Purchase Order Test</u> • Population: 327 purchase orders in 2025 • Sample size: 20 largest purchase orders based on dollar amount. This sample covered 68% of the total amount of all 2025 purchase orders. Note: The Purchase Order test excluded the onboarding process (i.e. RFPs and RFQs), as most of these vendors were existing vendors with a multi-year relationship with SERS. <u>New Vendor Test</u> • Population of new vendors in 2025 with purchases over $50,000: 3 • Sample size: 100% tested Note: The New Vendor test included the onboarding process (i.e. RFPs and RFQs) <u>Vendor Account Number Test</u> • Population: 414 vendors, 327 associate account numbers (checking, savings, etc.) • Sample size: 100% tested Note: No matches identified between associate and vendor account numbers. <u>Vendor Email Test</u> • Population: 414 vendors, 184 associates • Sample size: 100% tested Note: No matches identified between associate and vendor emails. <u>Terminated Employee Test</u> Population: 15 terminated associates • Sample size: 100% tested Note: No activity identified after associate's termination date.

	Note: Scope did not include credit card purchases, health care payments, investment transactions, employee reimbursements, memberships, tuition, seminars/training, travel, other compensation, or application testing.
Audit Methodology	IA's methodology included obtaining information on management's business objective and risks and focused on key processes and monitoring controls management has established to address significant risks. To meet the audit objectives, IA specifically performed the following procedures: • Conducted interviews/walkthroughs with management and key staff members • Reviewed compliance requirements, policies, and procedures • Documented understanding, key risks and controls • Performed tests of controls during the audit period as defined in the above Scope section.
Audit Conclusion	Internal Audit determined overall management controls for SERS' purchasing and contracts process were **operating effectively** to achieve the business objective. Internal Audit did not identify any high-risk audit observations but did identify two moderate and one low-risk audit observations. The overall conclusion was determined to be **well-controlled with improvement needed**.

OBSERVATIONS AND RECOMMENDATIONS

Required Documentation

Rating: Moderate

Criteria

Per the Purchasing Policy, “If a purchase is over $50,000, the vendor must complete a Standards of Conduct form (PUR-7005) prior to the execution of the agreement.”

The Standards of Conduct form is completed by the vendor and includes questions relating to:

- the vendor’s knowledge of any potential conflicts of interest,
- any known personal or business relationship with a SERS Retirement Board member, officer or employee within the last 12 months,
- and has the vendor or any officer or employee of the vendor given money or any other thing of value directly or indirectly to SERS Retirement Board member, officer or employees.

Condition

Of the 20 vendors reviewed with purchase orders over $50,000, 18 lacked a Standards of Conduct form.

Cause

Although the Finance department manages the purchase order process, each department is responsible for collecting vendor information. Due to an oversight at the department level, the completed Standards of Conduct form was not obtained from the vendor.

Effect / Risk

The lack of defined conflicts can result in legal liability, reputational damage, biased selections, or unfair contract awards.

Recommendation

Review the current process to ensure that all necessary forms are collected. Consider the implementation of a checklist or workflow tailored to specific dollar threshold or policy requirements. Ensure the checklist or workflow not only include requirements from the Purchasing Policy, but also requirements from the Vendor Risk Management Policy and Contract Review and Execution Policy. The checklist or workflow ensures the minimum level of documentation is maintained to promote quality control checkpoints.

Management Response

We identified that the Purchase Authorization form used with contracting documents no longer includes the requirement for a Standards of Conduct form when purchases exceed $50,000. We will partner with Communications to ensure that this requirement is reinstated on the Purchase Authorization form and incorporated into the Price Quote form as well. During the May meeting with department purchasing liaisons, we will reinforce this requirement and clarify where the completed form should be retained. Our goal is to finalize updates to both the Purchase Authorization and Price Quote forms by the end of the fiscal year.

In the meantime, the Standards of Conduct form will be included for all applicable purchases effective immediately, and we will work to obtain the form for applicable purchases made earlier in the fiscal year.

Centralized Document Repository

Rating: Moderate

Criteria

A centralized repository of required vendor documents allows associates to quickly locate documents and reduce the risk of errors by misplaced or outdated documents. Required vendor documents include documents as defined in the SERS' policies.

Condition

A centralized repository of all required vendor documents currently does not exist. Certain vendor documents are stored on the Boulevard, such as contracts, but other documents, such as the request for proposals (RFPs) and request for quotes (RFQs), are maintained within each department. Some of these documents are in hard-copy format, in emails, or on personal drives.

Cause

Although the Finance department manages the purchase order process, each department is responsible for collecting vendor information. The designated department associate may have this information either in hard copy or on their personal drive. If the associate leaves SERS, locating the required vendor documents can be difficult.

Effect / Risk

Inconsistent documentation approaches lead to variations in practice, ineffective documentation retention, noncompliance with policies, and the inability to use data for future decisions.

Recommendation

Establish a centralized location, such as the Boulevard, for storing required vendor related documents. In addition, implement a review process to ensure all required documentation is being provided, and at least annually, schedule regular management reviews to ensure the documents are up to date.

Management Response

Before this audit began, a team had already been convened to address the gap in maintaining a centralized location for vendor support documents such as RFPs and RFQs. A SharePoint site was created for this purpose, and we are currently testing the configurations designed to establish a consistent and structured repository. We will provide department purchasing liaisons with a preview of the SharePoint site and its processes during the May meeting, and we plan to conduct formal training in June. Our goal is to have departments fully aligned with this repository framework as implementation progresses.

Vendor Master File Review

Rating: Low

NetSuite is a cloud-based enterprise resource planning (ERP) system used to manage financials, procurement, vendor data, workflows, reporting, and other core business operations. In July 2024, NetSuite replaced Great Plains, and all vendor records, including ACH details, were migrated from Great Plains into the new system. Currently, the vendor master file includes vendors with one-time transactions and those who have not had any purchase activity since the system conversion. Although management has this as a future to-do item slated for 2026; no specific actions have been taken yet.

Management should implement an annual review of the vendor master file. This review should verify the accuracy and completeness of vendor information and remove inactive or duplicate vendors. Without periodic reviews, SERS may face increased exposure to fraud, payment errors, or unauthorized transactions due to inaccurate or outdated vendor data.

---

* Refer to Appendix A for classification of audit observations.

OTHER REPORTABLE RESULTS

There were no other reportable results identified.

APPENDIX A

CLASSIFICATION OF AUDIT OBSERVATIONS AND CONCLUSIONS

Classification of Audit Observations

Observations will be judgmentally risk ranked based on the below rating factors:

Rating	Description of Factors
Low	Observation poses relatively minor exposure to SERS. Represents a process improvement opportunity.
Moderate	Observation has significant impact to department or business objective but not to SERS as a whole. Compensating controls may exist but are not operating as designed. Requires near-term attention.
High	Observation has broad (SERS organization) impact and possible or existing material business objective exposure requiring immediate attention and remediation.

Classification of Audit Conclusions

Each conclusion will be identified with one of the four categories utilizing the following description of factors:

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present and could compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

FY2027 AUDIT CALENDAR

MONTH	TOPIC	PRESENTER	CAO	AUDIT COMMITTEE	SENIOR MANAGEMENT	EVERY YEAR	EVERY 5 YEARS
July	NO MEETING						
August	NO MEETING						
September	Internal Audit Update Update on Audit Plan Status of Outstanding Audit Recommendations Recently Completed Audits and Other Activities Essentional conditions	CAO	✓				
	Confirmation of Internal Audit Independence	CAO	✓				
	External Audit Update	Plante Moran		✓			
	Executive Session to consider the employment of a public employee. This includes reviewing the CAO goals.	CAO	✓	✓			
October	NO MEETING						
November	NO MEETING						
December	Internal Audit Update Update on Audit Plan Status of Outstanding Audit Recommendations Recently Completed Audits and Other Activities	CAO	✓				
	External Audit Update Review external auditor's financial statement opinion letter, internal control letter, and required communications	Plante Moran		✓			
	Status of ORSC Annual Audit Committee Report	CAO	✓				
	Executive Session to consider the employment of a public employee. This includes reviewing the CAO goals.	CAO	✓	✓			

6/2026

MONTH	TOPIC	PRESENTER	CAO	AUDIT COMMITTEE	SENIOR MANAGEMENT	EVERY YEAR	EVERY 5 YEARS
January	NO MEETING						
February	NO MEETING						
March	Internal Audit Update Update on Audit Plan Status of Outstanding Audit Recommendations Recently Completed Audits and Other Activities	CAO	✓				
	Review Audit Committee and Internal Audit Charters	CAO	✓	✓	✓		
	Executive Session to consider the employment of a public employee. This includes reviewing the CAO goals.	CAO	✓	✓			
April	NO MEETING						
May	NO MEETING						
June	Internal Audit Update Update on Audit Plan Status of Outstanding Audit Recommendations Recently Completed Audits and Other Activities	CAO	✓				
	External Audit Update	Plante Moran		✓			
	Approval of FY28 Chief Audit Officer Goals	CAO		✓			
	Discuss Internal Audit Mandate	CAO	✓				
	Discuss FY28 Internal Audit Budget	CAO	✓				
	Approval of FY28 Audit Plan	CAO		✓			
	Discuss IA Strategic Plan progress (FY26 - FY29)	CAO	✓				
	(Chief Audit Officer Evaluation) Executive Session to consider the employment and compensation of a public employee	CAO	✓	✓			
Other	Quality Assurance Improvement Plan					✓	
	Quality Assurance Review						✓

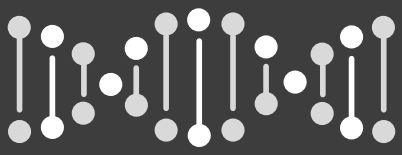
Corporate Governance: Guiding Principles for Board Oversight

The is a new publication that came out in March 2026 and provides boards with a clear, board-level set of guiding principles and practical illustrations to help them assess whether their governance model remains fit for purpose as organizations confront accelerating change, heightened stakeholder scrutiny, and increasingly complex risk environments.

Note: Page nine is a nice summary which outlines the 12 guiding principles.

The Role of the Audit Committee

This is a BoardSmart slide deck that outlines the oversight responsibilities of the Audit Committee. It's 22 slides but easy to read.



Corporate Governance: Guiding Principles for Board Oversight

About the authors and contributors

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a globally recognized organization dedicated to providing thought leadership that enhances governance, risk management, internal control, and fraud detection, primarily through the development of comprehensive frameworks and guidance to help entities reduce fraud and improve performance and oversight. COSO is a private-sector initiative, jointly sponsored and funded by:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- The Institute of Internal Auditors (IIA)

Committee of Sponsoring Organizations of the Treadway Commission

Board members

Lucia Wind
COSO Board Chair and Executive Director

Douglas F. Prawitt
COSO Board Lead Director
American Accounting Association

Larry R. White
Institute of Management Accountants

Jennifer Burns
American Institute of Certified Public Accountants

Lisa Halper
Financial Executives International

Benito Ybarra
The Institute of Internal Auditors

PwC

Principal authors

Lillian M. Borsa
Co-Engagement Leader and Principal, Governance Insights Center

Brian M. Schwartz
Co-Engagement Leader and Principal, Governance Insights Center

Paul DeNicola
Managing Editor and Principal, Governance Insights Center

Carin Robinson
Senior Director and Lead Writer

Matt DiGuiseppe
Managing Director and Lead Writer

Lauren Cohen
Manager

PwC

Additional contributors

Claudia Montgomery
Managing Director

Ashley Burgstahler
Director

Catherine Hall
Director

Katee Puterbaugh
Director

Nicholas Bochna
Manager

Project advisors

Project advisors were selected by the COSO Board. Consideration was given to each member's corporate governance knowledge and expertise to provide advice and feedback in connection with the development of this publication.

Patricia K. Miller
Project Advisory Chair
Deloitte & Touche LLP (*Retired*)

Lucia Wind
COSO Board Chair & Executive Director

William Gipson
Independent Director

Dawnella Johnson
Crowe LLP

Lindsay Jordan
Ernst & Young LLP

Aeisha Mastagni
CalSTRS

Karen Narwold
Independent Director

Kris Pederson
Independent Governance Professional

Paul Perry
Warren Averett (AICPA)*

Laura Phillips
Independent Governance Professional (FEI)*

Michael Phillips
South Georgia Banking Company (IMA)*

Andrew Struthers-Kennedy
Protiviti (IIA)*

Mark H. Taylor, Ph.D
University of South Florida (AAA)*

**COSO sponsoring organization representative*

Contents

Message from COSO's Board of Directors

This publication articulates a clear, board-level set of governance guiding principles, grounded in COSO's longstanding work on risk, internal control, and oversight, and is intended to serve as a common reference point where governance expectations can be fragmented. This focus reflects COSO's view that effective risk management and internal control operate within, and are strengthened by, a broader governance environment shaped by board oversight, accountability, information flow, and culture.

The guiding principles are designed to be read together. They are not intended to function as a checklist, and boards can determine how and to what extent to draw on them in light of the entity's circumstances. Taken together, they offer boards a structured way to reflect on whether governance practices remain coherent, balanced, and aligned with the entity's purpose, mission, values, and long-term direction. Rather than prescribing actions, the principles provide a practical lens for board dialogue on how oversight responsibilities fit together and are carried out in the entity's circumstances.

COSO offers this publication to support boards and those charged with governance in strengthening effective oversight over time, recognizing that durable governance is shaped by how responsibility and accountability are exercised in pursuit of long-term value.

COSO's perspective on corporate governance

Corporate governance is the oversight structures and processes by which an informed board steers an entity toward executing its strategy and objectives while maximizing long-term value in an ethical manner and within the relevant legal and regulatory environment.

About this publication

COSO, in collaboration with PwC US Consulting LLP, developed this corporate governance publication to provide guiding principles and practical illustrations that support effective board oversight in a changing governance environment. The guiding principles are intended to be broadly applicable across entity types, including public, private, and not-for-profit entities, and globally applicable across geographies and jurisdictions.

The publication helps boards determine whether their governance model remains fit for purpose by clarifying roles, sharpening governance discussions, and highlighting practices that support disciplined decision-making, accountability, and constructive challenge. It draws on extensive research, a review of widely recognized governance guidance, and input from directors, executives, governance professionals, and COSO's sponsoring organizations.

The guidance is directional and illustrative. It does not set requirements, prescribe a single governance model, or provide a comprehensive inventory of governance expectations. Nor does it address every board responsibility or area of oversight through a separate guiding principle. Instead, it brings together interrelated principles that commonly inform effective board oversight. It is intended to complement, not replace, applicable law, regulation, governance standards, and other widely recognized governance guidance. Boards can apply the guiding principles in light of the entity's purpose, mission, and values; strategy and objectives; risk profile; ownership structure; and applicable law, regulation, and governance standards.

The guiding principles focus on the board's oversight role. Management enablement considerations are included to illustrate how executive management and other key functions can support board oversight through information, analysis, and implementation, while day-to-day operations remain with management.

How to use this publication

Boards are the primary audience for this publication. It reflects both widely established board expectations and context-dependent practices. Qualifying language signals when application depends on circumstances and the applicable legal and regulatory environment. Boards can determine the practices and examples that are most relevant and apply them proportionately.

This publication can also support broader governance professionals, including corporate secretaries, chief audit executives, risk and compliance professionals, institutional investors, and others who interact with the governance process. It provides a shared language for board oversight discussions and for the information and analysis executive management can provide to support those discussions.

Throughout this publication, terms are used contextually, including references to shareholders, beneficiaries, and other stakeholders. Boards are accountable to shareholders or other beneficiaries under their governance model and legal structure. Other key stakeholders, such as employees, customers, suppliers, regulators, and communities, frequently impact an entity's ability to deliver long-term value. How these interests relate varies by jurisdiction and ownership model, and readers should interpret these terms accordingly.

Corporate governance supports constructive challenge and clear accountability, but outcomes remain subject to inherent limitations, including human judgment, unintended error, external events, and the potential for misconduct or override of established processes. Sound governance can strengthen resilience and confidence, but it cannot guarantee outcomes.

Boards and those that support them can use this publication to:

- Frame board and committee discussions around priority oversight topics
- Support board and committee assessments, governance reviews, and refreshment efforts
- Inform director onboarding and continuing education through a shared governance vocabulary
- Identify where information flows, decision processes, or accountability benefit from clarification
- Align oversight practices with the entity's strategy, risk appetite, culture, and operating context

This publication presents 12 interrelated guiding principles that reflect common areas of board responsibility. Boards and governance professionals can emphasize the principles most relevant to their circumstances and governance model.

How the guiding principles are organized

Each guiding principle follows a consistent structure:

Guiding principle

A concise title and one sentence description defining the core governance concept

Why this principle matters

Context on how the principle contributes to oversight, alignment with strategy, and long-term value

This principle in the boardroom

Illustrative examples of how the principle may be reflected in board oversight behaviors, processes, and considerations

Management enablement considerations

Examples of how management, including executive management or other key functions, may support the board with enabling structures and information flows, without prescribing specific actions or operating models

This structure is intended to support meaningful governance conversations, while allowing entities to draw on the concepts in ways that fit their needs and context. Not every illustrative example or management enablement consideration will be relevant in every entity, and boards can draw on them in ways that fit their circumstances and governance model.

Guiding principles at a glance

1 Board Governance Structure

The board establishes and oversees a governance structure that supports the board's fiduciary duties, clarifies roles and delegations of authority, and aligns oversight responsibilities with the entity's purpose and mission, strategy and objectives, risk appetite, and applicable law, regulation, and governance standards.

2 Board Accountability

The board fulfills its fiduciary duties in accordance with applicable law, regulation, and governance standards, honors shareholder or other beneficiary rights, and oversees governance and controls to promote accountability and maintain stakeholder confidence through complete, accurate, and timely disclosures.

3 Board Composition and Leadership

The board comprises a mix of skills, experience, and perspectives to operate with integrity and objectivity, demonstrates appropriate independence, and periodically reviews its composition, leadership roles, and succession plans to sustain effectiveness over time.

4 Board Effectiveness

The board regularly evaluates and improves its effectiveness, monitors internal and external changes, and refines its governance practices to strengthen oversight, support informed decision-making, and sustain long-term value creation.

5 Purpose, Mission, and Values

The board periodically reviews the entity's purpose, mission, and values, and oversees their alignment with strategy, culture, incentive structures, and workforce practices to confirm they are reflected throughout the entity and guide decision-making and strategic consistency.

6 Culture, Conduct, and Tone at the Top

The board sets clear expectations for integrity and ethical conduct, models them in its actions and decisions, expects executive management to uphold those standards, and oversees whether these expectations reflect the entity's purpose, mission, and values.

7 Strategy, Objectives, and Performance

The board provides independent perspective on strategy and objectives, approves material plans and actions, and oversees execution by monitoring performance against agreed objectives and measures and confirming incentives align with the entity's purpose, mission, values, risk appetite, and long-term value creation.

8 Technology and Data

The board oversees technology and data practices and opportunities to confirm they are managed in line with the entity's strategy and risk appetite and used to enhance performance and resilience.

9 Stakeholder Engagement

The board oversees management's approach to stakeholder identification and engagement, promotes credible, balanced communication, engages directly when appropriate, and incorporates relevant stakeholder interests and feedback into strategic discussions to strengthen trust and long-term value creation.

10 Executive Leadership and Succession

The board appoints the CEO and, as appropriate, other key members of executive management, oversees leadership development and succession plans, and periodically reviews management's talent strategy, leadership pipeline, and capability needs for executing strategy to support leadership continuity and organizational resilience.

11 Executive Performance and Compensation

The board evaluates the performance of the CEO and, as appropriate, other key members of executive management, approves executive compensation plans, and oversees compensation and incentive structures to drive long-term performance and reinforce accountability for long-term value creation.

12 Risk Management and Internal Control

The board oversees the entity's approach to managing risk and internal control, including management's monitoring and assurance activities, to support strategy and objectives and strengthen resilience.

Board foundations | Purpose and culture | Strategy and enablement | Leadership and resilience

Guiding principle 1

Board Governance Structure

The board establishes and oversees a governance structure that supports the board's fiduciary duties, clarifies roles and delegations of authority, and aligns oversight responsibilities with the entity's purpose and mission, strategy and objectives, risk appetite, and applicable law, regulation, and governance standards.

Why this principle matters

A well-defined governance structure is essential to the board's ability to fulfill its responsibilities effectively. Clear delineation of roles, responsibilities, and decision rights enables the board to focus on oversight and strategic guidance, while management operates within boundaries defined by the board. This clarity supports board independence, reduces duplication or gaps in oversight, and promotes efficient use of time and expertise. A fit-for-purpose governance structure also facilitates productive interaction among directors, committees, and management, reinforcing the board's ability to govern in line with its fiduciary duties.

Governance structures typically adapt over time as the entity's strategy, size, and risk profile evolve. A static or outdated structure can hinder effective oversight, obscure accountability, or result in fragmented decision-making. Regular reviews of the structure help the board confirm that its committee mandates, delegations, and reporting lines remain aligned with the entity's strategy, objectives, and regulatory context. Sound structures also support transparency with shareholders and other stakeholders by demonstrating how the board organizes itself to oversee critical areas such as strategy, risk, compliance, financial reporting, and executive performance.

This principle in the boardroom

The board adopts a governance structure that defines its roles, responsibilities, and decision-making authority. This includes reviewing and endorsing committee structures, typically audit, compensation, and nominating and/or governance committees, with clearly defined charters aligned to the board's core oversight duties. Boards periodically assess whether additional or specialized committees (such as strategy, risk, or technology) are warranted

Management enablement considerations

Management, particularly the corporate secretary, and general counsel as applicable, may support the governance structure by maintaining the formal governance documents that define the board's roles and authorities. This includes activities such as keeping board and committee charters current, documenting delegations (including approval thresholds), and coordinating how responsibilities are allocated among the board, its committees, and management. In some entities, the corporate secretary periodically reviews evolving governance structures and practices, including peer or similar committee structures and mandates, and highlights trends the board may wish to consider as needs and expectations change. Management then typically implements structural changes approved by the board and communicates these changes (e.g., new committees, revised mandates, or updated reporting

based on the entity's strategy, complexity, and regulatory environment. Charters and governance policies are reviewed at regular intervals to confirm that they remain current and effective.

Boards typically delegate authority through a resolution or approved policy that delineates which decisions are reserved for the board and which are delegated to executive management, often with specific thresholds. This allows executive management to act with agility within approved parameters while preserving the board's oversight of significant matters. The board generally considers whether committee mandates and information flows work together, for example whether audit committee insights on reporting and risk inform compensation committee decisions and full-board strategy discussions.

The board periodically reviews whether its governance structure remains fit for purpose. This often includes assessing whether the mandates of committees align with the entity's strategy, risk profile, and regulatory environment; considering whether responsibilities should shift between the board and its committees; and confirming that each committee's composition and expertise match its remit. In many entities, the nominating and/or governance committee leads this review as part of its annual workplan, drawing on internal input, external benchmarking, and developments in relevant governance codes or listing standards.

When the entity operates across multiple jurisdictions, business units, or subsidiaries, the board also considers how governance responsibilities are cascaded and coordinated across the group. The board may approve a governance structure that distinguishes the responsibilities of the parent board from those of subsidiary boards and any advisory bodies, clarifies reporting and escalation pathways between executive management committees and board committees, and defines how assurance providers and risk and control functions engage with the board and its committees. Clearly documenting these relationships helps avoid gaps or overlaps in oversight and supports timely escalation of matters that require board attention.

lines) across the entity and to relevant stakeholders where appropriate, so that the governance structure functions as intended.

Guiding principle 2

Board Accountability

The board fulfills its fiduciary duties in accordance with applicable law, regulation, and governance standards, honors shareholder or other beneficiary rights, and oversees governance and controls to promote accountability and maintain stakeholder confidence through complete, accurate, and timely disclosures.

Why this principle matters

Fiduciary duties anchor the board's role as a steward of the entity. These duties, commonly expressed in many jurisdictions as duties of care and loyalty, guide how directors act with diligence, good faith, and undivided commitment to the entity when making decisions. Acting in this way fosters trust in the board's decision-making and in the broader governance system. When boards adhere to these obligations, they strengthen the legitimacy of their oversight and the credibility of the entity's strategy and performance.

Accountability reflects the board's commitment to exercising fiduciary duties transparently and responsibly. Effective boards demonstrate this through high-quality disclosures, fair and responsive governance processes, and mechanisms that provide shareholders or other beneficiaries with a voice, such as elections, engagement, and voting rights. These practices allow shareholders to assess board performance, signal concerns, and influence governance outcomes.

This principle in the boardroom

The board applies its fiduciary duties as defined by applicable law, regulation, and governance standards, and periodically reflects on how those duties are carried out in board decisions. Directors act with care by preparing for meetings, challenging assumptions, and making decisions based on adequate information and deliberation. The duty of loyalty is often reflected in the board's adoption and monitoring of policies on conflicts of interest and related-party transactions, which are designed to prevent self-dealing and preserve objectivity in oversight. Boards also typically receive periodic reporting from management on conflicts of interest involving directors and executive management and on how those conflicts are addressed under the entity's policies. Boards may

Management enablement considerations

Management can facilitate the board's execution of its fiduciary duties by maintaining a strong governance infrastructure and information flows that support the board's oversight and accountability responsibilities. For example, the corporate secretary, and general counsel as applicable, advise the board on evolving legal and governance standards, help maintain conflict-of-interest and related-party policies, and coordinate processes that support disclosure obligations. Finance and investor relations teams typically support transparent and timely shareholder communications and engagement and may summarize voting results or investor concerns for board consideration. Management also operates compliance programs, internal control, and reporting mechanisms that provide the board with visibility into the effectiveness of those mechanisms. Together, these functions can support the board's ability to discharge its fiduciary responsibilities credibly and consistently.

request briefings from executive management and relevant third-party advisers on how legal duties apply in specific contexts, such as mergers, related-party transactions, or significant capital allocation decisions, and on how policies and practices for managing conflicts of interest and related-party transactions are being implemented.

Boards typically approve or review public disclosures, including financial statements, governance reports, and material non-financial information. In many entities, the board, through the audit committee, works with management and external auditors to oversee the process for evaluating whether financial and regulatory disclosures are complete, accurate, and timely. Boards may also review narrative sections of annual or sustainability reports, such as operating reviews, risk disclosures, governance descriptions, and executive compensation discussions, to confirm that significant matters are presented clearly and consistently. Some boards receive attestation from executive management and/or draw on assurance from internal audit, compliance, risk management, or external auditors regarding the effectiveness of controls and processes that support external reporting, reinforcing accountability.

When an external audit is conducted, the board, often through the audit committee, oversees the appointment or recommendation of the external auditor (as applicable), the ongoing evaluation of performance, and how independence is maintained. Most boards schedule executive sessions with the external auditor to support candid dialogue and provide an additional escalation channel when issues warrant board attention.

The board also oversees mechanisms that support shareholder or other beneficiary rights and governance transparency. In many entities, this includes monitoring shareholder meeting processes, board elections, and voting mechanics to confirm they are accessible, fair, and consistent with regulatory requirements. When applicable, the board reviews the outcomes of say-on-pay votes or director elections and considers engagement with shareholders if results indicate concerns. In some cases, boards support structured shareholder engagement programs and review aggregated investor feedback to inform governance or disclosure enhancements.

Other accountability mechanisms, such as ethics codes, whistleblower or speak-up systems, or board assessments, are important elements of the governance structure. Boards confirm that the mechanisms selected extend across the entity, including to the board itself, and that they are functioning as intended, often relying on designated committees (e.g., audit, governance) or specific processes (e.g., annual assessments) for more detailed review and improvement planning. Accountability is not only about compliance; it reflects a commitment to transparency and responsiveness that sustains trust in the board and its oversight.

Guiding principle 3

Board Composition and Leadership

The board comprises a mix of skills, experience, and perspectives to operate with integrity and objectivity, demonstrates appropriate independence, and periodically reviews its composition, leadership roles, and succession plans to sustain effectiveness over time.

Why this principle matters

Board composition directly affects the quality of oversight. A group of directors with complementary skills, varied experience, and diverse perspectives is more likely to make better decisions by challenging assumptions and surfacing blind spots. When aligned to the entity's strategy, risk appetite, and risk profile, a well-constructed board enhances credibility with shareholders, regulators, and other stakeholders. Independence within the board, both formal and behavioral, supports objective judgment, while well-designed leadership roles can facilitate robust dialogue, clear accountability, and effective board functioning.

Over time, a board's effectiveness depends on its ability to refresh itself. Regular reviews of composition and succession planning help keep the board's collective capabilities aligned with the entity's evolving needs. Boards that manage tenure, turnover, and leadership development intentionally are better equipped to sustain performance, adapt to change, and maintain stakeholder confidence.

This principle in the boardroom

The board approves its own composition policies and reviews them regularly to confirm alignment with the entity's strategy, risk profile, legal and regulatory requirements, and stakeholder expectations. Many boards use a skills and experience matrix to assess their current mix of capabilities and identify gaps or emerging needs, for example, digital expertise, geopolitical insight, or sector-specific knowledge. The nominating and/or governance committee typically leads director recruitment, using independent search support when appropriate and evaluating candidates against agreed criteria that include integrity, sound judgment, fit with the board's culture and working style, and diversity of background and perspective. Boards often consider how their composition and refreshment decisions are

Management enablement considerations

Management can support the board's composition and leadership planning by providing information, logistics, and relevant context. The corporate secretary typically maintains the board's skills matrix, tracks tenure and independence status, and facilitates director onboarding and education. Executive management may offer perspectives on strategic or operational areas where additional board expertise could add value, while respecting the board's independent authority over nominations. Human resources and legal teams support candidate due diligence and interface with search firms as needed. Management also supports independent board judgment by reinforcing role expectations for key stewardship and control functions, including the corporate secretary, chief financial officer, general counsel, chief human resources officer, the internal audit leader, or equivalent roles, to act in the interests of the

communicated externally, including disclosure of the board's skills, experience, and broader diversity profile and the rationale for director appointments, so stakeholders can understand who serves on the board and why.

Board independence is considered in light of both external standards and individual director behavior. Boards often define independence in governance policies aligned to applicable regulations. They typically assess each director's independence status annually. They also reflect on behavioral independence: whether directors are prepared to offer dissenting views, avoid groupthink, and act without undue influence. Formal mechanisms, such as executive sessions, committee leadership arrangements, and, where relevant, lead independent director roles, support these dynamics.

Leadership roles are generally reviewed periodically to confirm that they support effective oversight, board dynamics, and succession planning. Consistent with applicable requirements and local practice, boards decide whether to combine or separate the chair and CEO roles, whether to appoint an independent chair or lead independent director, and how committee chair responsibilities are allocated, considering the entity's ownership structure and culture, among other factors. Boards may rotate committee chairs on a planned cadence and establish succession plans for key board leadership roles. In some entities, the board maintains a multi-year roadmap for leadership transitions to support continuity and build readiness. When appropriate, directors are encouraged to gain leadership experience on committees before stepping into broader roles.

Tenure and refreshment practices vary, but many boards use term limits, a mandatory retirement age, or explicit planning discussions to balance continuity and thoughtful turnover. Boards may integrate insights from board or director peer assessments into succession planning decisions, considering not just individual contribution but also overall board dynamics. Composition and leadership discussions often draw on input from multiple sources, including self-assessments, stakeholder perspectives, and governance benchmarking, to support an informed and forward-looking approach.

entity and raise matters directly with the board and its committees when appropriate. Together, these functions can help the board maintain a composition and leadership structure that reflects both external expectations and internal priorities.

Guiding principle 4

Board Effectiveness

The board regularly evaluates and improves its effectiveness, monitors internal and external changes, and refines its governance practices to strengthen oversight, support informed decision-making, and sustain long-term value creation.

Why this principle matters

Board effectiveness does not occur by default; it requires ongoing attention and deliberate improvement. An effective board sets clear expectations, makes informed decisions, and promotes productive engagement with executive management. Regular assessment, whether self-led or independently facilitated, allows the board to reflect on what is working well and identify opportunities to improve its composition, processes, and dynamics. These assessments help keep the board capable of overseeing executive management as it navigates increasingly complex risks and strategic choices in a changing environment.

By rigorously evaluating its own effectiveness, the board demonstrates accountability at the highest level. It reinforces expectations for integrity and ethical conduct, transparency, and responsiveness throughout the entity. Assessments that result in concrete actions, such as changes to meeting structures, agenda planning, or onboarding, demonstrate that the board is committed to its own development. This continuous improvement mindset strengthens the board's ability to oversee long-term value creation and maintain stakeholder trust.

This principle in the boardroom

The board approves a regular cadence and scope for assessing its effectiveness and uses the process to identify practical improvements. Most boards conduct an annual assessment at the board and committee levels, using a combination of questionnaires, interviews, and facilitated discussions. Some boards seek feedback from the CEO or other executives to help identify blind spots in how the board supports strategy, oversight, and culture, and to strengthen dialogue and overall board effectiveness. Many boards also conduct individual director or peer assessments to strengthen

Management enablement considerations

Management can support board effectiveness by facilitating and participating in the assessment process and providing high-quality information. The corporate secretary typically coordinates assessment logistics, summarizes findings, and tracks follow-up actions. Management often works with the board to design meeting agendas, calibrate the frequency and format of materials, provide directors with the information they need to make informed decisions, and appropriately document meeting minutes. Management typically participates in onboarding and education, offering briefings and access to internal and external experts. By engaging transparently with the board and responding to feedback, management can contribute to a governance environment that supports continuous improvement and oversight quality.

accountability, surface development needs, and support thoughtful decisions about board composition and succession over time. To encourage candor and avoid repetitive or formulaic results, boards may periodically vary assessment methods and engage an external advisor. Whether led internally or supported periodically by an external advisor, assessments can surface actionable insights and allow for benchmarking against evolving practices.

Assessment processes are most useful when results translate into changes in board behaviors and working norms, as appropriate. Board effectiveness is shaped by how directors engage with management and with one another, including tone, preparedness, listening, and constructive challenge. These behaviors can materially influence decision quality. Boards often reflect on whether discussions encourage candid debate while maintaining collegiality, whether all voices are heard, and whether directors operate at the appropriate level. Many boards also use assessment output and board leadership's ongoing observations to address underperformance constructively, reinforce expectations for respectful challenge, and build trust over time. Boards that can engage in difficult conversations and maintain confidence in how they work together are better positioned to operate as an effective, integrated decision-making body.

Boards also use assessment results to inform improvements to their board practices and operations. Actions might include refining meeting agendas to prioritize forward-looking topics, updating board materials for clarity and relevance, or adjusting committee roles to reduce overlap. Some boards incorporate findings into succession planning, for example, identifying emerging skill needs or considering changes in leadership roles. Boards often track action items from prior assessments to monitor progress and reinforce a culture of follow-through.

The way board time is structured and discussions are sequenced throughout the year play an important role in enabling effective oversight. Boards typically approve an annual workplan that maps key oversight responsibilities, such as strategy, risk, talent, and culture, across the year and leaves room for emerging issues. Agendas are often designed to allocate sufficient time for forward-looking and high-impact discussions while meeting core compliance obligations. Executive sessions, held without management present, are often scheduled to support candid dialogue about board dynamics and leadership. In entities with combined chair-CEO roles, a lead independent director may facilitate these sessions and serve as a counterweight to executive leadership.

Within this structure, directors generally expect concise, decision-relevant materials prepared and distributed on a timely basis. Directors may also provide feedback to executive management on how board materials can better support informed oversight, for example by adding clear executive summaries, highlighting key risks, or including trend data aligned to the annual workplan. Directors may also request direct access to senior management outside the CEO to inform their oversight, with appropriate protocols in place to maintain clarity of roles.

The board, often through the nominating and/or governance committee, periodically reviews the approach to director onboarding and continuing education as part of its oversight of board effectiveness. To support director readiness, directors are typically provided with site visits, in-depth briefings, exposure to key executives, and opportunities for external education. By setting expectations for robust onboarding and ongoing development, the board helps build a shared knowledge base and strengthens the quality of board discussions and decisions over time.

Guiding principle 5

Purpose, Mission, and Values

The board periodically reviews the entity's purpose, mission, and values, and oversees their alignment with strategy, culture, incentive structures, and workforce practices to confirm they are reflected throughout the entity and guide decision-making and strategic consistency.

Why this principle matters

An entity's purpose, mission, and values provide a foundation for its strategic direction, operational choices, and stakeholder relationships. Purpose defines why the entity exists; mission articulates what it seeks to achieve; and values express the commitments that guide behavior and decision-making. Values connect purpose and mission to the culture and conduct experienced in practice. When these elements are clear, aligned, and consistently applied, they can guide behavior, build trust, and support long-term resilience. Misalignment between stated values and actual practices, or between purpose and performance incentives, can erode credibility and impair execution.

Boards have a critical role in confirming that the entity's purpose, mission, and values remain relevant and are integrated into decision-making. These elements shape culture, influence risk behaviors, and frame how the entity defines success. In a rapidly changing environment, clarity of purpose and values helps entities navigate trade-offs and maintain stakeholder confidence. By overseeing these foundational concepts, boards reinforce the conditions for sustainable performance and ethical conduct.

This principle in the boardroom

The board periodically reviews the entity's purpose, mission, and values, typically in connection with strategic planning or major business model changes. Directors may challenge whether the purpose is specific and credible, whether the mission remains relevant to evolving priorities, and whether the values are observable in leadership behavior and workforce norms. When necessary, the board works with executive management to refine or reaffirm these statements so they are meaningful guides for action.

Management enablement considerations

Management can support board oversight by translating the entity's purpose, mission, and values into policies, processes, and reporting. Management incorporates these elements into strategic plans, internal communications, and leadership messaging. Human resources typically integrates values into onboarding, performance management, training, and employee engagement programs. Human resources, risk management, internal audit, and other monitoring or assurance providers may assess patterns and themes across the entity such as conduct trends, recurring issues, or control breakdowns that signal whether purpose and mission are understood and whether values are being lived in practice. Management can also provide the board with qualitative and quantitative indicators of alignment, such as employee feedback, purpose-linked key performance indicators (KPIs), or

Boards often ask executive management to demonstrate how the entity's purpose, mission, and values influence strategy and decision-making. For example, directors may probe how the entity handled a recent trade-off, such as declining a lucrative opportunity that conflicted with its stated values, or how their values informed their response to a reputational or operational crisis. Discussions often explore how these foundational concepts shape capital allocation, risk appetite, and stakeholder engagement. Directors also consider whether incentive structures and performance metrics support the behaviors and outcomes that reflect the entity's values.

Boards typically review inputs from management that assess how well the entity's purpose and values are embedded in practice. These may include culture survey results, qualitative feedback from employees and customers, or external indicators such as reputation rankings and stakeholder trust scores. In some cases, boards receive reporting that links purpose or values to performance outcomes, for instance, improved employee retention or customer loyalty associated with mission alignment. Directors use these insights to assess the authenticity and effectiveness of how the entity lives its stated commitments.

Incentives, workforce policies, and leadership expectations are often areas of focus. Boards may ask how hiring, promotion, and recognition programs reinforce the entity's values. They consider whether incentive structures and executive management objectives reinforce values-aligned choices as well as results. Directors may also encourage transparency in communicating purpose and values internally and externally, particularly when these shape decisions that affect stakeholders. Through these actions, the board reinforces that purpose and values are not abstract ideals but strategic and operational anchors.

feedback, conduct trends, or purpose-linked key performance indicators (KPIs), and, where helpful, prepare illustrative case studies or incident reviews to bring these concepts to life. These practices can support the board in evaluating whether foundational commitments are credible, consistently applied, and integrated into the entity's policies, incentive structures, and decision-making.

Guiding principle 6

Culture, Conduct, and Tone at the Top

The board sets clear expectations for integrity and ethical conduct, models them in its actions and decisions, expects executive management to uphold those standards, and oversees whether these expectations reflect the entity's purpose, mission, and values.

Why this principle matters

Culture reflects the shared behaviors and norms that express the entity's values in practice. It affects how employees make decisions, respond to pressure, and raise concerns. A strong culture aligned with the entity's purpose, mission, and values supports ethical conduct, risk awareness, and long-term performance. Conversely, a misaligned or unhealthy culture can enable misconduct, distort information, or undermine strategic execution, often without clear early warning signs.

Boards play a critical role in overseeing culture because leadership behavior, incentives, and everyday practices reinforce what is truly valued. The tone set at the top, by both the board and executive management, shapes expectations and influences conduct throughout the entity. Cultural insights help the board assess the reliability of information, the credibility of leadership, and the likelihood that strategy will be executed in a manner consistent with the entity's values and risk appetite.

This principle in the boardroom

The board sets expectations for ethical behavior and oversees whether executive management's actions reinforce those expectations. This begins with adopting or approving a code of conduct and monitoring the practices that guide behavior, including ethics and compliance programs. The board also exemplifies those same behaviors in how it operates, through respectful deliberation, transparency in decision-making, and holding itself to the same standards it expects from management. It typically reflects upon its own conduct and incentives, recognizing that its tone, behaviors, and assessment practices influence culture across the entity.

Management enablement considerations

Management can provide structured insights and timely reporting to support board oversight of culture. Examples include presenting data from engagement surveys, turnover trends, ethics hotline or speak-up metrics, and culture-related assessments or audits. Management also shares qualitative signals, such as employee feedback themes or outcomes from internal reviews, in a manner that protects confidentiality while allowing the board to understand patterns and implications. Compliance, ethics, investigations, human resources, and internal audit functions may provide aggregated or thematic information on speak-up activity and the handling of significant matters, supporting the board's ability to assess whether concerns are raised, addressed, and resolved in line with the entity's values and anti-retaliation

Boards regularly review indicators of culture and conduct, including how executive management's tone at the top is understood and reinforced across the entity. These indicators may include employee engagement results, speak-up systems or hotline usage, retention and turnover in key roles, incident trends, and signals that incentives or performance pressures are shaping behavior in unintended ways. Directors may request direct exposure to cultural signals, such as attending site visits, holding workforce listening sessions, or reviewing summaries of exit interviews or internal investigations. These touchpoints help boards assess whether the desired behaviors are reflected in the day-to-day experience of employees and whether any pockets of risk or erosion of culture or trust are emerging.

The board also oversees the design and function of speak-up systems and anti-retaliation protections. While operational details reside with management, the board confirms that there are accessible, trusted channels for employees to raise concerns and that retaliation is actively discouraged and addressed consistently. The board may review high-level information on speak-up activity to assess whether issues are surfaced and resolved in a manner consistent with the entity's values and expected conduct. In some cases, directors also receive targeted summaries or briefings on how significant matters were raised and resolved to evaluate responsiveness.

Incentives that support appropriate leadership behaviors are core to sustaining a healthy culture. Through periodic reporting, the board considers how executive compensation structures, recognition programs, and promotion decisions support or undercut cultural priorities. For example, if collaboration is a stated value, boards may examine how collaborative behaviors are reinforced in performance evaluations. Culture is also linked to risk: a culture that tolerates excessive pressure, ignores dissent, or conceals problems can magnify risk. Boards can probe how leadership actions align with the desired tone, particularly during periods of stress, change, or underperformance.

expectations. Executive management reinforces these systems by modeling expected behaviors and communicating the importance of raising concerns. Taken together, these inputs give the board a multi-dimensional view of culture and help directors assess whether the tone at the top is consistently reinforced across the entity.

Guiding principle 7

Strategy, Objectives, and Performance

The board provides independent perspective on strategy and objectives, approves material plans and actions, and oversees execution by monitoring performance against agreed objectives and measures and confirming incentives align with the entity's purpose, mission, values, risk appetite, and long-term value creation.

Why this principle matters

Strategy is the primary way an entity translates its purpose and mission into concrete choices about where to compete, how to win, and how to deploy scarce resources. When the board is closely involved in shaping and challenging strategy and major objectives, it brings an independent perspective on assumptions, trade-offs, and the balance between risk and opportunity. This perspective can strengthen the quality of decisions about capital allocation, portfolio focus, and strategic priorities. Board oversight also connects high-level objectives to the outcomes that matter to shareholders, beneficiaries, and other key stakeholders. By testing whether proposed strategies are coherent, realistic, and aligned with the entity's purpose, mission, values, and risk appetite, boards help position the entity for long-term value creation and resilience.

Effective oversight continues after agreement is reached on strategy and objectives. Execution unfolds in an environment shaped by technological change, macroeconomic shifts, competition, and evolving stakeholder expectations, so performance rarely follows a straight line. Boards that monitor performance through a balanced set of financial and non-financial indicators are better able to identify early signals of shifting conditions, spot inflection points, learn from outcomes, and support timely course corrections. Linking strategic objectives, risk appetite, and incentive plans allows the board to assess whether management is rewarded for decisions that advance long-term value instead of only short-term results. A disciplined, forward-looking approach to strategy, objectives, and performance oversight helps the board view strategy as a continuous cycle of learning and adaptation rather than a periodic discussion.

This principle in the boardroom

The board provides independent perspective as executive management develops the enterprise strategy, and evaluates and

Management enablement considerations

Management can design structured strategic planning processes and provide clear, decision-ready information to support board oversight of strategy, objectives, and performance. Examples include preparing complete and concise materials that frame the strategic context, options, assumptions, and expected outcomes, along with scenario and sensitivity analyses. Management typically translates approved strategies into coherent plans, budgets, and KPIs and develops dashboards or scorecards that link these metrics to strategic priorities. Throughout execution, executive management reports candidly on progress, emerging risks, and new opportunities, highlighting where adjustments or additional board decisions may be needed. Executive management may also conduct retrospective reviews of major initiatives and share insights with the board so that lessons learned can inform future strategic planning and performance expectations.

agrees to final plans, including major initiatives and high-level performance objectives, with formal approvals when required. Directors participate in structured strategy discussions, which may include annual or multi-year strategy meetings, periodic deep dives on key businesses or themes, and reviews of the competitive landscape and external trends. In these sessions, they assess the clarity of strategic choices, question critical assumptions, and explore alternative pathways, including different pacing or sequencing of initiatives. The board considers whether proposed strategies and objectives are aligned with the entity's purpose, mission, values, and risk appetite and whether they reflect the entity's capabilities and constraints. Directors may also discuss how stakeholders such as shareholders or other beneficiaries, employees, customers, and regulators are likely to respond to major strategic moves.

Boards commonly review how strategy is translated into objectives, plans, and metrics. They may ask executive management to show how strategic priorities connect to capital allocation, major investments, divestitures, and resource deployment across businesses or geographies. Directors often seek visibility into how technology, digital initiatives, talent priorities, and data capabilities support the strategy. They may request that materials describe expected milestones and leading indicators, not only end-state targets, to support ongoing oversight. When considering significant transactions or commitments, the board evaluates strategic and cultural fit, value creation potential, and execution risks, often drawing on independent advice when warranted.

Once strategy and objectives are established, the board oversees execution by monitoring performance against agreed indicators and milestones. Depending on the entity, execution oversight may span other business areas, such as operations, commercial functions, communications, or public affairs, that support the enterprise strategy. Boards typically receive updates that integrate strategic and financial results with operational, risk, culture, and stakeholder metrics, enabling a more holistic view of progress. Directors probe the reasons behind under- or over-performance, evaluate how executive management is responding, and consider whether resources and priorities remain appropriately aligned with the strategy. They encourage executive management to surface emerging opportunities and threats, including disruptive technologies, shifts in customer behavior, or regulatory developments, rather than waiting for issues to escalate. Scenario analyses, stress tests, and retrospective reviews on major strategic decisions can be used to understand what has been learned and how those lessons influence future choices.

The board also reviews how strategic objectives and performance outcomes are reflected in executive performance assessments and incentive plans. Directors may ask whether the KPIs used for incentives capture both results and behaviors, balance short- and long-term horizons, and reflect risk considerations. They consider whether incentive design reinforces strategic priorities and the entity's risk appetite, consistent with the board's broader approach to executive performance and compensation oversight. These discussions help the board reinforce alignment among purpose, mission, strategy, risk appetite, and incentive plans and provide additional context for decisions on leadership performance and pay.

Guiding principle 8

Technology and Data

The board oversees technology and data practices and opportunities to confirm they are managed in line with the entity's strategy and risk appetite and used to enhance performance and resilience.

Why this principle matters

Technology and data are central to how entities innovate, compete, and deliver value. They enable new business models, customer experiences, operating efficiencies, and insight-driven decisions that can materially influence long-term strategy and performance. At the same time, they can reshape whole industries and quickly render existing strategies obsolete when disruptive innovations emerge. Boards that understand how technology and data support the entity's strategy, and how they might fundamentally change it, are better positioned to guide choices about where to invest, how fast to move, and which opportunities merit attention. They are also better positioned to anticipate the broader stakeholder impacts of technology choices, including effects on brand reputation, data privacy, identity protection, and the future of work.

These same capabilities create significant risk exposures, including cybersecurity threats, data privacy, system outages, third-party technology failures, and unintended consequences from advanced technologies such as artificial intelligence (AI). Stakeholders increasingly expect boards to have a line of sight into these risks and into the governance approaches that address them. Effective board oversight helps balance opportunity and risk by asking whether technology and data initiatives align with risk appetite, whether security and resilience expectations are embedded, and how management is coordinating technology and data efforts across the entity. Done well, this oversight supports both innovation and resilience.

This principle in the boardroom

The board oversees technology and data priorities as part of its strategy and capital allocation discussions. Directors typically review

Management enablement considerations

Management can provide decision-ready reporting in business terms, free from jargon, and maintain the governance and operating structures that manage day-to-day technology and data activities. Senior leaders, such as the CIO, CTO, and CISO, can prepare roadmaps and investment cases that link initiatives to strategic objectives, expected benefits, key dependencies, and material risks. Examples include establishing clear accountability, reporting lines, and escalation protocols; integrating technology and data risks into the entity's enterprise risk management and internal control activities; and summarizing key indicators, incidents, and emerging risks for board review. Management may also provide the board with security and incident assessments, including internal audit or other independent perspectives, benchmarking against relevant peers, and pre- and

management's view of how technology and data underpin the strategy, create new strategic options, and position the entity for competitive advantage, while also understanding the risks of disruption and execution. Boards may ask how major technology initiatives, such as core system replacements, cloud migrations, new digital channels, or data monetization efforts, advance the entity's purpose, mission, and values. They also consider whether the entity is investing with sufficient ambition and pace to remain competitive, recognizing that excessive caution can itself be a strategic risk. Directors probe whether the portfolio of technology initiatives is realistic given resources and change capacity, how trade-offs are being made among competing projects, and whether risk-taking aligns with the entity's strategy and risk appetite. When appropriate, the board may challenge executive management not only to manage risk prudently, but to pursue innovation decisively in support of long-term value creation.

In addition, boards increasingly consider the broader social and stakeholder implications of technology and data choices, recognizing that digital tools can materially shape relationships with customers, employees, and communities. They may ask how technology-enabled products, platforms, or algorithms affect user behavior, information integrity, privacy, fraud, workforce dynamics, or public trust, and whether these impacts are understood and aligned with the entity's values.

When appropriate, the board also sets high-level expectations for how technology and data are governed across the entity, including how oversight responsibilities are allocated across the board, its committees, and executive management, and sets expectations for policy coverage in critical areas such as cybersecurity, data privacy, third-party technology, and use of advanced analytics and AI. Boards also set expectations for transparency on significant incidents, major investments, and emerging technology risks.

Directors may also discuss how executive management assigns responsibilities among relevant leaders, such as the CIO, CTO, and CISO, and how these leaders coordinate across functions and geographies. Boards generally look for a coherent picture of how technology and data risks are identified, prioritized, and managed within the broader enterprise risk management and internal control activities, while recognizing that day-to-day risk management remains the role of management.

Data quality and data governance remain a critical and ongoing focus. Reliable, decision-useful data supports informed decisions, disciplined execution, and responsible use of analytics and AI, and it helps reduce the potential for loss, regulatory exposure, or missed opportunities. Boards may ask how critical data is identified, who owns it, what standards apply (e.g., accuracy, completeness,

post-implementation reviews of major initiatives or changes. Such assessments are often performed by internal audit or other independent advisors. By translating complex topics into business terms and bringing forward both opportunities and risks, management can enhance the board's ability to exercise effective oversight of technology.

timeliness, and permitted use), and how exceptions are escalated and remediated. Many entities use dashboards that link key technology and data initiatives to strategy and objectives and include relevant risk and performance indicators, supported by clear ownership and standards for key data, including data quality indicators and remediation status for critical data. Boards may request deep dives on topics such as cyber resilience, data governance and data quality, or major transformation programs and, when helpful, tabletop exercises. These discussions help directors evaluate whether technology and data are contributing to performance as intended and whether performance remains within established risk tolerance.

Boards also consider the people, culture, and structures that shape technology outcomes. Directors may ask whether and how the entity attracts and retains technology and data talent and whether the broader workforce is positioned to adapt as digital tools and ways of working evolve. This may include upskilling considerations, where the board assesses whether people across the entity, including board members and those outside formal technology roles, have appropriate opportunities and guardrails to use technology, data, or automation responsibly as tools and ways of working evolve.

Boards may also reflect on their own collective digital fluency, recognizing that effective oversight increasingly requires directors to engage meaningfully with technology-enabled business models, data-driven decisions, and AI-supported processes, even when deep technical expertise resides with management or external advisors. Directors evaluate whether the board and its committees have sufficient expertise and time devoted to technology and data topics, and adjust committee charters, composition, or education plans accordingly. In some cases, boards engage external advisors or schedule focused education sessions to stay current on emerging technologies and their implications. Through these activities, the board keeps technology and data on the governance agenda in a way that supports innovation while maintaining discipline.

Guiding principle 9

Stakeholder Engagement

The board oversees management's approach to stakeholder identification and engagement, promotes credible, balanced communication, engages directly when appropriate, and incorporates relevant stakeholder interests and feedback into strategic discussions to strengthen trust and long-term value creation.

Why this principle matters

Stakeholder relationships contribute meaningfully to long-term value creation and resilience. Shareholders, employees, customers, suppliers, regulators, and communities all influence the entity's ability to execute strategy, adapt to change, and maintain its license to operate. These stakeholder groups do not all affect the entity in the same way or at the same time, and their interests may diverge or conflict depending on context and circumstance. Constructive attention to stakeholder interests, including engagement where appropriate, can strengthen trust, improve access to talent and markets, and provide insight into emerging expectations. Listening systematically to stakeholder perspectives also helps boards understand how the entity is perceived and when its actions may not match its stated purpose, mission, and values. When these relationships are managed thoughtfully and purposefully, they support stability, innovation, and credible communication in both normal and stressed conditions.

Poorly managed stakeholder dynamics can create reputational, regulatory, or operational strain. Misreading stakeholder expectations or responding only when issues have escalated can lead to disputes, regulatory scrutiny, campaigns by investors or civil society, and distraction of leadership attention. Stakeholder expectations can shift quickly, influenced by broader social trends, sector developments, or events involving peers. In practice, many strategic and oversight decisions require trade-offs that benefit certain stakeholders while disadvantaging others, and some decisions may prompt concerns or objections from particular groups. Boards that receive synthesized, decision-useful stakeholder insights from executive management and incorporate them into deliberations are better able to oversee how management anticipates issues and weighs trade-offs. The board retains decision-making authority over priorities and responses, applying judgment as executive management brings forward stakeholder trade-offs and recommended actions.

Management enablement considerations

Management can support board oversight of stakeholder interactions by coordinating relevant channels for understanding stakeholder interests and perspectives and providing integrated, decision-ready insights. Functions such as investor relations, human resources, sustainability, compliance, customer experience, and public affairs often lead relevant communications or maintain information channels with their respective stakeholder groups and consolidate feedback for board review. Management might prepare concise reports that highlight key themes, sentiment trends, and potential implications for strategy, risk, and culture, along with proposed actions or options. When stakeholder engagement is reflected in external reporting or governance communications, management often drafts a clear narrative that reflects what was heard from

This principle in the boardroom

The board oversees how management identifies key stakeholder groups and prioritizes their significance in light of strategy and risk. Directors often review stakeholder maps that describe who the key groups are, what interests they hold, and how they are affected by the entity's activities. They may ask how these maps are updated as strategy evolves, markets change, or new stakeholder groups emerge. Boards also consider whether the ways the entity understands stakeholder interests and perspectives, including through direct engagement when appropriate, are clear and aligned with the entity's purpose and long-term goals. Through these discussions, directors help clarify how the entity stays informed about stakeholder interests and how those insights inform decisions rather than relying only on ad hoc interactions.

Boards often receive synthesized reporting on stakeholder sentiment and themes. This may include insights from employee engagement surveys, retention and safety indicators, customer satisfaction and complaint trends, supplier feedback, investor voting outcomes and engagement topics, regulatory perspectives, or community relations. Directors may request integrated summaries that highlight common themes, areas of alignment and tension, and implications for strategy, risk, culture, or reputation. They may consider whether significant public positioning, external communications, marketing campaigns, or public policy engagement align with the entity's purpose, mission, values, and long-term strategy and objectives, recognizing that such actions can significantly affect stakeholder trust and long-term value. Directors may also ask how management prepares for crisis or emergency communications with key stakeholder groups, including escalation triggers, roles, and approval protocols for time-sensitive messaging. They can ask how management is responding to recurring issues, how stakeholder expectations are evolving, and how feedback is incorporated into plans. These conversations help the board treat stakeholder input as an early-warning system and a source of ideas, not only as a source of pressure.

In defined circumstances, boards may engage directly with stakeholders to complement management-led efforts. Directors might participate in selected meetings with investors on governance, strategy, or compensation topics, following agreed protocols and in coordination with management. Boards may also request opportunities to hear directly from employees through workforce panels, site visits, or town halls, or to engage with community or civil society representatives on issues of particular importance. Boards, together with management, typically set protocols for these interactions that respect management's primary role in day-to-day relationships and protect sensitive information.

shareholders and other stakeholders and how the board considered the feedback and related response options, as appropriate. When significant stakeholder issues arise, such as investor campaigns, workforce actions, or community concerns, management may outline scenarios and responses for board input. Management also takes responsibility to plan and coordinate any director–stakeholder interactions, including preparation and follow-up, so that these engagements are effective, consistent, and aligned with governance roles.

Boards may also consider stakeholder perspectives in strategy, risk, and culture discussions. Directors may ask how stakeholder insights informed major proposals, how key initiatives are expected to affect different stakeholder groups, and how those effects have been communicated. They may challenge management when stakeholder feedback suggests misalignment between stated values and actual practices or when stakeholder concerns could signal emerging risks. At the same time, directors interpret stakeholder input through the lens of their fiduciary duties to the entity and, as applicable, its shareholders or other beneficiaries, weighing competing interests within the boundaries of applicable law, regulation, and governance standards. Incorporating these perspectives supports more holistic decisions and more credible external communication about how the board has considered stakeholder views.

Guiding principle 10

Executive Leadership and Succession

The board appoints the CEO and, as appropriate, other key members of executive management, oversees leadership development and succession plans, and periodically reviews management's talent strategy, leadership pipeline, and capability needs for executing strategy to support leadership continuity and organizational resilience.

Why this principle matters

Executive management is responsible for translating and executing the strategy, purpose, mission, and values into day-to-day decisions and behaviors. The CEO and other members of executive management shape culture, allocate resources, and respond to risks and opportunities in ways that can accelerate or undermine long-term value creation. When the board approaches CEO selection and oversight of other key executive roles with rigor and deliberation, it helps align leadership profiles with the entity's strategic needs and desired culture. The feasibility of the strategy also depends on whether the entity has, or can build, the workforce capabilities required, including evolving skills needs. Clear accountability for these decisions also reinforces independent judgment and provides a basis for constructive challenge when performance or conduct is not consistent with expectations.

Leadership continuity is equally important. Inadequate, reactive, or informal succession planning can result in rushed appointments, loss of institutional knowledge, or prolonged uncertainty during transitions. These outcomes can distract the entity, unsettle employees and stakeholders, erode value, and impact operations. Boards that oversee structured succession planning, covering both emergency scenarios and planned transitions, are better positioned to manage change in a measured way. Regular insight into the talent pipeline also helps boards understand whether the entity is developing future leaders with the capabilities needed for the strategy and evolving risk environment and whether talent and workforce planning supports those needs.

Management enablement considerations

Executive management can maintain disciplined succession processes and provide directors with clear, candid line of sight into talent readiness and risk to support board oversight of executive leadership and succession. This often includes periodic reporting on succession coverage for critical roles, curated exposure to potential successors, and timely escalation of emerging retention or capability concerns. Management can provide workforce planning updates, including priority capability gaps and development actions to build the bench. To support board decision-making on key appointments, management typically prepares role profiles, market intelligence, and assessment summaries, and coordinates transition plans once leadership decisions are made.

This principle in the boardroom

The board appoints and, when necessary, replaces the CEO and, in line with governance expectations and applicable law and regulation, may also have a role in the appointment of other critical executive roles. Directors typically begin by agreeing on the desired profile for the CEO, taking into account the entity's strategy, culture, risk appetite, and stakeholder expectations. They may discuss the balance of experience, leadership style, and values needed at a particular point in the entity's evolution. Many boards also discuss the leadership and workforce capabilities the strategy requires, and how executive management plans to build, hire, or otherwise access critical skills. When a CEO appointment is under consideration, the board evaluates internal and external candidates against this profile and considers how each candidate would work with the existing leadership team. The board also reflects on how the appointment decision and transition plan will be communicated to employees, shareholders, beneficiaries, and other key stakeholders.

Boards oversee the process used to identify and select executive leaders, even when day-to-day steps are delegated to a committee or management. They may review the use of search firms or other external advisors, assessment methods, and reference processes, and consider whether the candidate pool is sufficiently diverse in terms of background, experience, and perspectives. Directors often seek multiple touchpoints with potential CEOs and other key executives, including interviews, presentations, and informal discussions, to form independent views of their readiness and fit. For certain roles expected to provide a more independent perspective, such as the chief audit executive or the head of risk management, board involvement is often more direct. For example, the audit committee may lead the selection process for the chief audit executive and approve the appointment or hiring decision to reinforce independence and objectivity. They also consider contractual and governance aspects of appointments, including terms of employment, performance expectations, conditions for separation, and the degree to which the CEO's leadership style and values align with the board's culture and ways of working, recognizing that these decisions can have long-term implications for both leadership stability and accountability.

Following the appointment of a new CEO, the board plays an active role in supporting a healthy transition and effective onboarding, setting clear expectations for early priorities, decision-making norms, and how the CEO engages with the board and executive management. In parallel, the board maintains a forward-looking focus

on leadership continuity beyond the immediate transition. Directors review emergency CEO succession plans that often specify interim leadership and decision rights in the event of an unexpected vacancy and oversee medium- to long-term succession plans for the CEO and other key roles, including likely internal candidates, development priorities for those candidates, and expected time horizons. Board discussions often test how the pipeline would adapt under different strategic paths, such as a shift in business model or a major transaction, and how talent implications would be managed. Boards may also probe whether development plans are strengthening bench depth for critical roles, not only identifying successors. This ongoing oversight reduces reliance on any single individual and supports continuity through both planned and unplanned transitions.

To understand the strength of the leadership pipeline, boards may seek direct insight into executive and high-potential talent. Directors may ask executive management to organize regular talent reviews, leadership presentations at board or committee meetings, and site visits or workforce sessions that allow them to observe leaders in their operating environments. They may review metrics such as succession coverage for critical roles, diversity in leadership ranks, turnover in key positions, and progress against leadership development objectives and broader workforce capability priorities. These discussions allow the board to test executive management's assessment of the pipeline, identify gaps that could affect strategy execution, and reinforce expectations that leadership development is a strategic priority.

Guiding principle 11

Executive Performance and Compensation

The board evaluates the performance of the CEO and, as appropriate, other key members of executive management, approves executive compensation plans, and oversees compensation and incentive structures to drive long-term performance and reinforce accountability for long-term value creation.

Why this principle matters

Executive performance and compensation strongly influence how effectively the strategy is executed, how risks are taken, and how value is shared among shareholders, beneficiaries, and other stakeholders. When objectives are clear and performance is assessed using a balanced set of measures, executives are more likely to make decisions that advance sustainable value rather than narrow, short-term targets. Well-designed incentives connect leadership behavior to purpose, mission, and values; strategy and objectives; culture; and risk appetite, supporting disciplined capital allocation decisions and prudent risk-taking. This alignment helps attract and retain key talent while reinforcing expectations for ethical conduct and sound judgment.

Conversely, misaligned incentives can drive excessive risk-taking, short-termism, or behavior inconsistent with the entity's values. Perceived disconnects between pay and performance can also erode trust among employees, investors, regulators, and the public. In many markets, executive compensation is subject to extensive disclosure requirements and, in some cases, advisory votes or other mechanisms for owner feedback. Active board oversight of executive performance (CEO, and other management as appropriate) and compensation structures, combined with clear communication about how decisions are made, supports transparency, legitimacy, and confidence in governance.

This principle in the boardroom

In many entities, the board's executive evaluation and compensation decisions focus on the CEO, while oversight of other executives may occur through review of the CEO's assessments and recommendations, consistent with governance standards and

Management enablement considerations

Executive management, typically led by the CEO and the head of human resources, can prepare proposed performance goals and compensation structures that flow from the strategic plan and risk appetite, and provide periodic reporting on results against those plans. Human resources and finance teams typically provide benchmarking data, model potential outcomes under different performance and market scenarios, and administer approved plans using defined processes and controls. They may also compile performance evaluations and pay summaries for board or committee review and highlight any areas where judgment may be required, such as risk or conduct considerations. Investor relations and corporate secretaries support communication of the board's decisions and rationale in disclosures and engagement with shareholders, beneficiaries, and other key stakeholders.

contractual arrangements. Throughout the year, the board receives updates on performance against agreed objectives and measures, questions significant variances, and asks how results were achieved, not only whether targets were met. At the end of the performance period, the board may conduct a formal evaluation of the CEO and review the CEO's assessments of other executive management, considering both outcomes and behaviors. These evaluations provide the foundation for many compensation decisions and may also inform succession planning and leadership development.

Performance assessments often inform the board's decisions on compensation outcomes for the CEO and consideration of the CEO's recommendations for other executive management. The board or a designated committee might have a more explicit role in the performance and compensation process when the executive has formal accountability to the board, such as the chief audit executive. Across these decisions, directors may compare realized or realizable pay to the entity's performance over multiple years and consider whether formulaic results fairly reflect the broader context, including risk and conduct issues. When appropriate and within plan parameters, boards may exercise judgment to adjust outcomes, for example by moderating payouts in light of risk events or by using tools such as deferrals, holding periods, and malus or clawback provisions. Boards may also review how the overall compensation philosophy for the broader workforce aligns with culture and long-term value, while recognizing that detailed pay decisions beyond the executive level remain the responsibility of management.

The board typically approves the executive compensation philosophy and major compensation plans and reviews them periodically for alignment with strategy, objectives, risk appetite, and culture. Through the compensation committee or equivalent, directors consider the mix of fixed and variable pay, the balance between short- and long-term incentives, and the performance measures and time horizons used. They discuss whether the program design promotes long-term decision-making, responsible risk-taking, and desired leadership behaviors. Boards often request benchmarking and scenario analysis, including compensation studies prepared by independent advisors, to inform views on market competitiveness and pay positioning, and to understand how different performance and share-price outcomes translate into realized pay over time.

Boards also oversee how executive compensation is communicated and how external feedback is considered. Directors review disclosures to confirm they clearly explain the link between pay, performance, risk, and the entity's stated values. They may discuss the results of advisory votes or equivalent owner feedback mechanisms and themes raised in investor or other stakeholder engagement on compensation topics. These insights can prompt refinements to plan design, performance measures, or disclosure practices and help the board maintain a transparent, credible approach to executive pay.

Guiding principle 12

Risk Management and Internal Control

The board oversees the entity's approach to managing risk and internal control, including management's monitoring and assurance activities, to support strategy and objectives and strengthen resilience.

Why this principle matters

Oversight of how the entity identifies, assesses, and responds to risk, together with oversight of internal control and assurance activities, is central to how the board oversees the achievement of strategy and objectives. Because all strategies involve uncertainty, a well-governed approach to managing risk can help clarify the trade-offs the entity is prepared to take, how those choices align with risk appetite, and when risks are best addressed through mitigation, transfer, avoidance, or disciplined acceptance. Board oversight of risk includes not only the entity's focus on the downside of risk but also taking advantage of the upside of risk when the opportunity aligns to strategy and risk appetite. Internal control, designed to provide reasonable assurance regarding the achievement of operations, reporting, and compliance objectives, supports reliable execution by promoting sound information, consistent processes, and adherence to applicable requirements and ethical expectations. Assurance activities, including internal audit and other independent reviews, can complement management monitoring and provide additional perspective on how well key risks are being managed and how effectively internal control supports execution. Ongoing monitoring and periodic evaluations can provide timely insight into whether risk responses and internal controls continue to operate as intended, including whether accepted risks remain within agreed boundaries and escalation protocols.

Weak or fragmented risk and control environments can contribute to financial losses, misconduct, regulatory penalties, reputational damage, and threats to long-term viability. Shareholders or other beneficiaries, regulators, and other key stakeholders increasingly expect boards to demonstrate a structured, enterprise-wide approach to risk oversight supported by coherent assurance. As a result, board oversight typically extends beyond reviewing risk assessment results and audit reports, to understanding how governance, culture, incentives, and assurance work together to inform decisions and reinforce resilience.

Management enablement considerations

Executive management is responsible for designing and operating the entity's processes for managing risk and internal control, including monitoring that provides ongoing insight and periodic evaluations of effectiveness. In many entities, business units and functions such as risk, compliance, finance, and legal contribute to identifying risks, implementing responses, tracking obligations, and quantifying impacts, while internal audit and other assurance providers offer independent perspectives. Management can support board oversight by providing periodic, decision-useful reporting that synthesizes significant risks, related responses, key indicators, and relevant monitoring and independent assurance insights, including escalation when risk acceptance is managed within agreed boundaries. When the entity uses

This principle in the boardroom

The board oversees the entity's approach to managing risk and internal control. Effective oversight helps keep discussions of risk and resilience connected to strategy and performance. In many entities, directors approve or oversee how risk is managed and how internal control supports execution, including how responsibilities are allocated among the board, committees, executive management, and assurance functions. Directors often discuss risk appetite or an equivalent decision framework in the context of strategy and consider how management has translated it into policies, processes, and day-to-day decision-making, revisiting it as conditions and priorities change. Boards may also consider whether the level of risk-taking reflected in strategy and capital allocation appears appropriately calibrated, recognizing that both overexposure and underexposure to risk can affect long-term value. These discussions can help confirm that responsibilities remain coherent and that there are no significant gaps or unnecessary overlaps.

Directors often probe key assumptions and seek clarity on how management identifies, assesses, prioritizes, and monitors significant risks, including emerging risks and concentrations. Many boards request scenario analysis or stress testing for severe but plausible events and consider how these insights inform strategic choices, capital allocation, and contingency planning, so that major decisions reflect both opportunity and downside risk.

Oversight of internal control and assurance commonly includes attention to controls over financial reporting and disclosure, operations, and compliance, as well as management's monitoring activities that track and evaluate whether risk responses and related controls are operating as intended. Boards increasingly seek transparency from executive management on where AI, including generative AI, is used in financial reporting processes, accounting judgments, and related controls, and how management assesses the related risks and the design and operation of those controls. Through the audit committee or equivalent, boards typically review internal and external audit plans and reports, significant findings, and remediation progress. Boards also often consider how management monitoring, internal audit, external audit, and other assurance activities fit together to provide a coherent view of effectiveness, including whether assurance providers have appropriate independence, authority, resources, and access to the board. Directors may encourage coordination across assurance activities, such as a Three Lines Model or equivalent, and may ask for reporting that links assurance insights to strategy, performance, and culture rather than focusing only on individual findings. Directors may also explore whether significant findings suggest changes in the entity's risk profile that should inform periodic strategy discussions.

formal risk policies or articulates risk appetite, management typically maintains and refreshes them and supports the board in using them to inform strategic choices. When applicable, management can facilitate independent assurance and periodic testing of business continuity and incident-response plans by enabling appropriate access and sharing readiness insights and lessons learned.

Boards often discuss resilience and preparedness for incidents and disruptions, which can include reviewing business continuity management, including crisis management plans, and how lessons learned are incorporated into the entity's approach to managing risk and internal control, as well as training and readiness activities. Risk culture is often a recurring board topic, with directors reflecting on tone at the top and exploring whether incentives, workloads, and decision-making practices support transparent escalation and balanced risk-taking, particularly during periods of stress.

For deeper guidance on board and executive management roles and governance practices related to risk management and internal control, refer to COSO's Enterprise Risk Management Framework (2017) and Internal Control—Integrated Framework (2013).

Conclusion

Corporate governance is foundational to how boards direct and oversee entities, and how they remain accountable over time. Governance questions rarely arise in isolation. Decisions about accountability, strategy, culture, leadership, and risk often converge, particularly during periods of change. Governance is strengthened when board responsibilities connect and reinforce one another, supporting coherent decision-making and sustained oversight.

Boards often return to governance principles during transition, such as leadership changes, strategic shifts, major transactions, or heightened stakeholder scrutiny. In those moments, this publication can support focused reflection and structured dialogue, helping boards consider whether oversight remains aligned with the entity's purpose, mission, values, strategy and objectives, risk profile, and operating context. Over time, effective governance is reinforced through sustained attention, periodic review, and deliberate follow-through as circumstances evolve.

Appendix

Glossary

This glossary defines selected terms used in this publication when meaning may vary across governance models, industries, and jurisdictions. It is intentionally not comprehensive. Definitions reflect how terms are used in this publication and are written to support consistent interpretation across a global audience.

Accountability	The obligation to be answerable for decisions, actions, and outcomes, including transparent reporting and timely remediation when expectations are not met. In this publication, accountability describes how expectations are set, monitored, and addressed in practice and complements fiduciary duties.
Assurance	Activities that provide objective evidence that support reasonable confidence that key risks, governance processes, and internal control are being managed as intended (e.g., internal audit, external audit, and compliance reviews). Some entities coordinate assurance activities across providers to reduce overlap and strengthen coverage.
Board	The governing body appointed or elected to provide direction and oversight of the entity. In this publication, "board" includes equivalent governing bodies (e.g., boards of directors, supervisory boards, boards of trustees, councils) that hold oversight responsibility under the entity's governance model.
Clawback provisions	Contractual or policy-based mechanisms that allow an entity to recover previously paid incentive compensation under specified circumstances, such as misconduct, material policy violations, or financial restatements.
Code of conduct	A documented set of expectations for integrity, ethical behavior, and decision-making that applies to directors, executive management, and the workforce, with defined processes for escalation and consequences.
Control	As a noun, a policy or procedure that is part of internal control. As a verb, to establish or implement a policy or procedure that supports the achievement of objectives.
Culture	The shared values, norms, and behaviors shaped by leadership and reinforced by people at all levels that influence how individuals act with integrity, make decisions, and respond to risk.
Disclosures	Information an entity shares with shareholders, regulators, and other key stakeholders to provide transparency about performance, governance, and other relevant matters. Disclosures can be mandatory or voluntary and may include financial and non-financial information.
Enterprise risk management	The culture, capabilities, and practices integrated with strategy-setting and performance on which entities rely to manage risk in creating, preserving, and realizing value.
Entity	Any for-profit, not-for-profit, or governmental body. An entity may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure.
Executive management	The chief executive and direct reports responsible for executing strategy and leading the entity. Titles vary by jurisdiction and entity type.

Fiduciary duties	Duties owed by directors to the entity and, as applicable, its owners or other beneficiaries under the entity's governance model and applicable law and regulation. Fiduciary duties commonly include duties of care, loyalty, and good faith, although terminology and emphasis vary by jurisdiction.
Governance model	The way an entity allocates ultimate decision rights and accountability among the board, owners or other beneficiaries, executive management, and other governance bodies. Governance models vary across ownership structures, legal forms, and jurisdictions.
Governance structure	The specific structures and roles used to implement the governance model, including board composition and leadership roles, committee structure, delegations of authority, and the relationship to subsidiary boards or advisory bodies when relevant. Some entities use the term "governance framework" to describe similar concepts. This publication uses "governance structure" to describe the specific structures and roles used to implement the governance model.
Independence	The ability to exercise objective judgment free from bias and undue influence. Independence can be assessed through formal criteria (relationships and interests) and through behavior (willingness to challenge, avoid groupthink, and act in the interests of the entity).
Internal audit	An independent, objective assurance and advisory activity that evaluates and improves the effectiveness of governance, risk management, and internal control. Internal audit typically has direct access to the board or an appropriate committee. For information on the standards and principles that govern internal audit, refer to the IIA's Global Internal Audit Standards.
Internal control	A process, effected by an entity's board, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
Malus	A compensation adjustment mechanism that allows an entity to reduce or cancel unpaid, unvested, or deferred incentive compensation before it is paid or vested, typically in response to misconduct, material risk management failures, financial restatements, or similar events.
Management	Individuals beyond executive management who lead teams, oversee operations, and coordinate work across functions or business lines. Management translates strategy and direction into execution and provides reporting to executive management.
Monitoring	Ongoing and periodic activities used to evaluate whether internal controls, and when applicable, key risk responses, are operating as intended, and to identify issues requiring action. Monitoring can include activities embedded in operations and separate evaluations performed at intervals.
Resilience	The ability to anticipate, withstand, adapt to, and recover from disruption while continuing to pursue objectives.
Purpose, mission, and values	Purpose is the entity's fundamental reason for being and the enduring aim it serves. Mission describes what the entity seeks to achieve and how it intends to deliver on its purpose. Values are the core beliefs and standards of conduct that guide decision-making and behavior. In this publication, "purpose, mission, and values" serve the same anchoring role as COSO ERM's "mission, vision, and core values," reflecting more current language used in many entities today.

Risk appetite	The types and amount of risk the entity is willing to accept in pursuit of value through its strategy and objectives.
Risk profile	The aggregate view of the entity's significant risks at a point in time, considering likelihood, impact, interdependencies, and concentrations, and how these risks may affect performance relative to strategy and business objectives.
Risk response	The approach selected for a risk, such as accepting, avoiding, reducing, sharing or transferring, or pursuing opportunity with informed risk-taking. Controls and monitoring can support different risk responses, including disciplined acceptance within defined parameters.
Risk tolerance	Boundaries of acceptable variation in performance related to achieving business objectives.
Shareholders and other beneficiaries	The person(s) or group(s) to whom the board is accountable under the entity's governance model and legal framework.
Stakeholders	Parties with a genuine or vested interest in the entity, including individuals or groups that may affect or be affected by the entity's activities, performance, or reputation, including shareholders, employees, customers, suppliers, regulators, and communities.
Strategy and objectives	Strategy is a set of informed, sometimes difficult choices an entity makes about how to compete and create long-term value, guided by the entity's unique current and future advantages. It defines where and how the entity will focus its resources, respond to disruption, and differentiate itself in a constantly evolving environment in a manner aligned with its purpose, mission, and values. Objectives are specific, measurable, and time-bound targets that support the achievement of broader strategy and goals.
Sustainability	The long-term viability of the entity and its ability to continue delivering objectives over time. Sustainability topics vary by entity and may include resilience, resource use, workforce and community impacts, and other factors relevant to strategy and stakeholder confidence.
Technology and data	Digital systems, tools, and information assets used to run the entity and support strategy. This includes cybersecurity and third-party technology, as well as data governance, data quality, data security, and permitted use considerations. The term can also include emerging technologies such as AI (including generative AI), which may introduce opportunities and risks.
Three Lines Model	The IIA's Three Lines Model is a principles-based framework that helps the board and executive management clarify responsibilities for governance, risk management, and control activities across the organization in support of achieving objectives and creating and protecting value. Under the model, management (first line) is responsible for owning and managing risks and maintaining effective controls. Functions that provide expertise, support, monitoring, and challenge (second line) assist management in overseeing and managing risk. Internal audit (third line) provides independent and objective assurance and advisory services to the board and executive management on the effectiveness of governance, risk management, and internal control processes.
Tone at the top	Signals from the board and executive management, through words, actions, and decisions, that shape expectations for integrity, accountability, transparency, and risk-taking across the entity.
Whistleblower/ speak-up systems and anti-retaliation	Channels through which employees and other stakeholders can raise concerns, ask questions, or report suspected misconduct, including confidential or anonymous options when appropriate. Anti-retaliation refers to protections and expectations that prohibit negative consequences for good faith reporting.

The Role of the Audit Committee

Introduction

Welcome to the Talk "The Role of the Audit Committee."

Almost all state public retirement system boards utilize committees, and an audit committee is nearly always present. Even among smaller county and municipal systems, where there are typically fewer board committees, an audit committee is found with nearly half of the systems.

For publicly-traded companies, the SEC requires that all boards have an independent audit committee.

An audit committee plays a critical role in maintaining financial integrity and accountability for any organization governed by an independent board of directors or board of trustees.

In summary, the audit committee of a public retirement system board is essential to ensuring the integrity and stability of the system. Through its oversight responsibility, the audit committee plays a vital role in ensuring that the system is managed responsibly and that the interests of the beneficiaries are protected. This includes establishing appropriate internal controls, monitoring the performance of the internal audit function, and ensuring that audit activities are conducted in accordance with policies, procedures, and best practices. Ultimately, the audit committee's primary responsibility is to ensure that the public retirement system operates effectively, efficiently, and with the highest level of integrity.

The purpose of this podcast is to provide an overview of the responsibilities of a board audit committee, specifically for a public retirement system, how the audit committee functions effectively, and key questions that audit committees should ask.

Let's start with a discussion of the responsibilities of the audit committee.

The Role of the Audit Committee

The audit committee of a public retirement system board has several important responsibilities, including:

1. Overseeing the integrity of the system's financial statements, accounting and financial reporting processes, and financial statement audits;
2. Overseeing the evaluation and monitoring of the internal control system by internal and external auditors;
3. Overseeing the performance of the system's independent financial auditor and the internal audit function;
4. Overseeing the independent auditor's qualifications and independence (this applies if the Board has responsibility for selecting the independent auditor);
5. Providing a forum for the resolution of all disputes between management and the internal and/or external auditors regarding financial reporting, risk assessment, internal control and other compliance issues;
6. Overseeing policies and procedures for the receipt and handling of allegations of suspected misconduct; receiving reports on a periodic and as-needed basis regarding significant reports received; and overseeing special investigations and whistleblower cases, as needed, on behalf of the Board;

In addition, many public retirement system boards ask the audit committee to provide oversight of enterprise compliance and ethics, enterprise risk management, and cybersecurity.

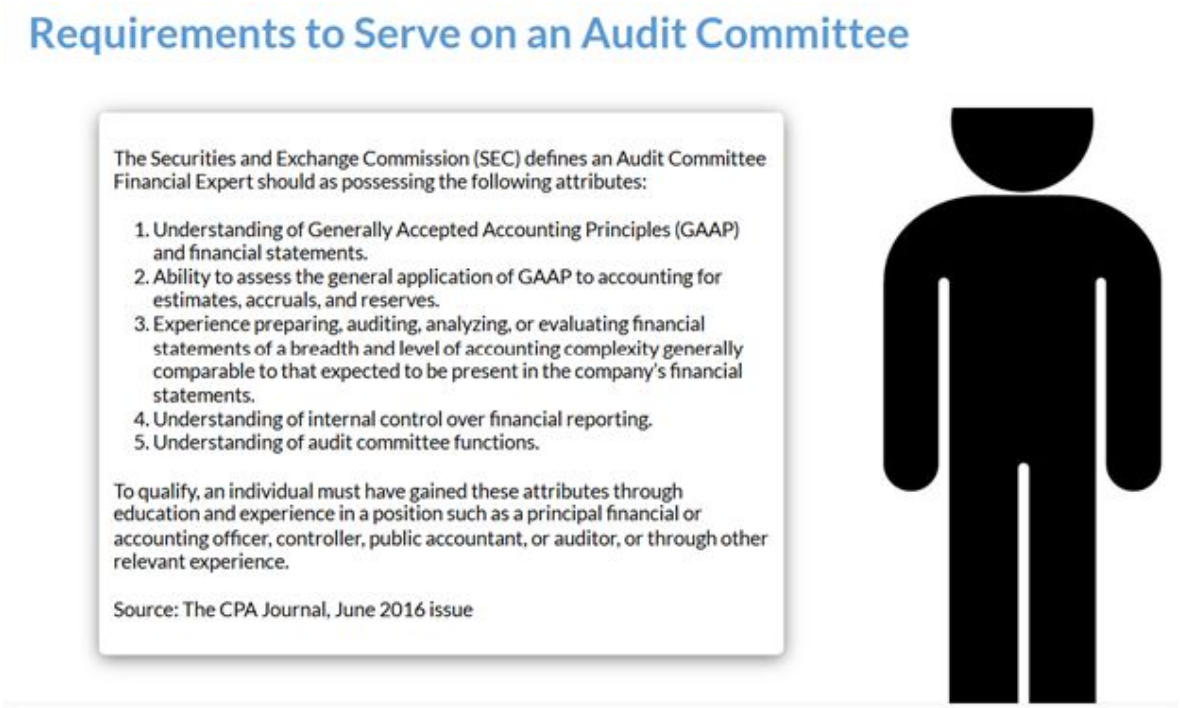
Audit committees often have responsibility for oversight of fraud prevention, including:

The Role of the Audit Committee

- Review antifraud program and controls, including policies and procedures for prevention and detection of fraud.
- Ensure investigations are undertaken if fraud is suspected and review reports and effectiveness of controls.
- Ensure appropriate action is taken against known perpetrators of fraud.

These are all very important areas of board oversight. This assists the board in fulfilling its oversight responsibilities by specifically focusing on all these topics. The audit committee is able to provide more effective and comprehensive oversight than the whole board could achieve given all its other responsibilities.

The Role of the Audit Committee



Who should serve on the Board's audit committee?

For publicly-traded companies, the SEC encourages audit committees to have at least one member who qualifies as a financial expert.

Public retirement systems usually cannot select their own board members or recruit trustees with certain qualifications, so often having trustees with specific financial or auditing expertise to serve on the audit committee is lacking.

Typically, one or more appointed public retirement system trustees are expected to provide specific qualifications and experience, often in the areas of investments, finance, or actuarial science, but this doesn't always result in qualified audit committee candidates.

What are the most desirable qualifications and skills for serving on an audit committee? What does the term "financial literacy," as used by the SEC, actually mean?

Generally this term means the ability to read and understand financial statements. However, as described in the responsibilities of the audit committee, the areas of oversight are much broader that just financial statements.

Some systems use a skills matrix to create an inventory of the experience of their trustees and to identify the skills and experience important to each board committee. Although this doesn't necessarily fill in gaps in expertise, it can help to ensure that the most experienced trustees are assigned to the appropriate committees.

The Role of the Audit Committee

As a practical matter, public retirement boards usually need to help individual trustees attain and supplement their knowledge through continuing education and advice from external experts. The members should collectively possess sufficient knowledge of audit, finance, specific industry knowledge, IT, law, governance, risk, and controls.

The Role of the Audit Committee

The audit committee should regularly meet with key parties both inside and external to the system as part of its ongoing responsibilities.

Internal Audit

The audit committee establishes and protects the internal audit function's independence and qualifications. The Chief Audit Executive, or CAE, is usually a direct report to the audit committee. With that reporting relationship, the committee, with the assistance of staff, is responsible for hiring, evaluating and, as appropriate, terminating the CAE. The committee should also have a succession plan and provide input on the CAE's performance and compensation to the Executive Director. The CAE should have unrestricted access to, communicate, and interact directly with the audit committee, including private meetings without senior management present.

With respect to internal audit, the committee has a number of essential responsibilities to ensure the function meets the needs and expectations of the board and senior management. We will review each one now.

First, the audit committee establishes, approves, and supports the mandate of the internal audit function. The mandate specifies the internal audit function's authority, role, responsibilities, scope, and services of the internal audit function. The mandate is documented in the internal audit charter. The committee should periodically review and approve the Internal Audit Charter with the assistance of the CAE.

The Role of the Audit Committee

The committee should review and approve the system's annual risk-based internal audit plan and receive periodic updates on progress. This includes meeting with the CAE and receiving reports to review the status of audits, audit findings and recommendations and management responses, and monitor actions taken to implement the audit recommendations. The committee also approves of any significant revisions to the internal audit plan.

The committee should ask and ensure there are no unjustified restrictions or limitations on the internal audit function, and that the Internal Audit Office has adequate resources to fulfill the internal audit mandate and achieve the internal audit plan.

Finally, the committee should ensure the CAE develops and maintains a quality assurance and improvement program that covers all aspects of the internal audit function. At least annually, the committee reviews and approves the internal audit function performance objectives, and the results of internal quality assessments. The audit committee should also discuss plans to have an external quality assessment of the internal audit function, at least every five years and require receipt of the complete results of the external quality assessment or self-assessment with independent validation directly from the assessor. The audit committee should review and approve the CAE action plans and timeline to address identified deficiencies or opportunities for improvement, if applicable. The committee should receive periodic reports to monitor the CAE's progress.

External Audit

The audit committee is also usually the primary contact for the independent external auditor. In most systems, this starts with conducting a search for the independent external auditor, with the assistance of staff, and making recommendations to the Board, a process that should occur at least every five years. However, in some systems the independent auditor is selected by the plan sponsor or statutorily provided by another government agency such as the state auditor's office.

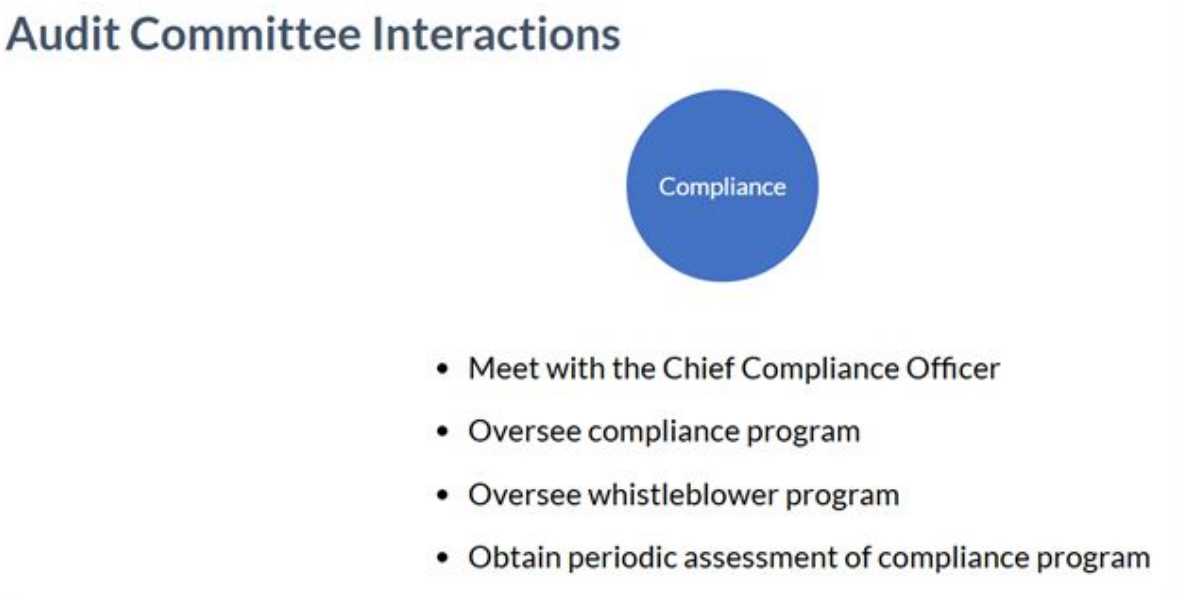
The audit committee should meet with the external financial auditors multiple times throughout the year. The first meeting is typically prior to beginning the annual financial audit, with the objective of reviewing the scope and approach, identifying any other matters of emphasis or potential areas of the operations that should be reviewed (for example, hard-to-value assets, or actuarial schedules), and discussing new accounting pronouncements that may impact financial reporting.

The committee should also meet with the auditors at the conclusion of the financial audit to review the results of the audit engagement, including the audit opinion, any significant findings and recommendations, difficulties encountered, and any significant adjustments proposed by the auditors. The discussion should review the findings and recommendations along with management's responses and actions taken or planned to implement the audit recommendations. The audit committee should also confirm procedures are in place to confirm the independence of the external auditor.

In addition to internal and external audit, there are a number of other areas the Audit Committee interacts with.

External Regulators

When there are reviews or examinations conducted by regulatory agencies, the committee should review the findings and recommendations, management's responses and actions taken to implement the recommendations, and make any recommendations to the full board for action.



Compliance

When the audit committee is charged with oversight of compliance and ethics, the committee should periodically meet with the Chief Compliance Officer, at least annually.

The role of the committee is to oversee the design and implementation of the compliance program, including the policies and procedures to help prevent and detect violations of law or conformance with applicable requirements and to promote business ethics. The committee should review the effectiveness of the system for monitoring compliance, the process for communicating the code of conduct to the organization's personnel, approve the annual compliance plan and ensure that the compliance function has adequate resources to meet its responsibilities. The compliance program should address compliance and ethics activities and reports, including enterprise program compliance, enterprise and Board policy compliance, service provider compliance, and privacy and security compliance. The committee also oversees the whistleblower program, including ensuring that employees and other stakeholders have an independent and confidential means of reporting suspected misconduct or fraud.

The committee should also ensure that periodically there is an independent assessment of the compliance program and review the results.

The Role of the Audit Committee

Enterprise Risk

When the audit committee is also charged with overseeing enterprise risk management, the committee will periodically review the organization's risk profile and should periodically meet with the Chief Risk Officer to review and approve performance and annual risk management plans and ensure the risk management function has adequate resources to meet its responsibilities.

The committee should review the effectiveness of the system for assessing, monitoring, and controlling significant risks or exposures and oversee enterprise risk appetite and tolerances in each area, excluding investment risk, which is usually a responsibility of the investment committee. In addition, the committee should review emerging and significant risks specific to the area of responsibility of the committee, and report those risks to the board. The audit committee also provides an oversight of the adequacy of the combined assurance being provided and provides advice on the risk management process established and maintained by management. The committee should also ensure an independent assessment of the risk management program and review the results.

Cybersecurity, Data Protection, and Disaster Recovery

Increasingly, boards are looking to their audit committee to oversee cybersecurity and data protection. This usually requires the committee to meet with the Chief Technology Officer and, if applicable, the Chief Information Security Officer.

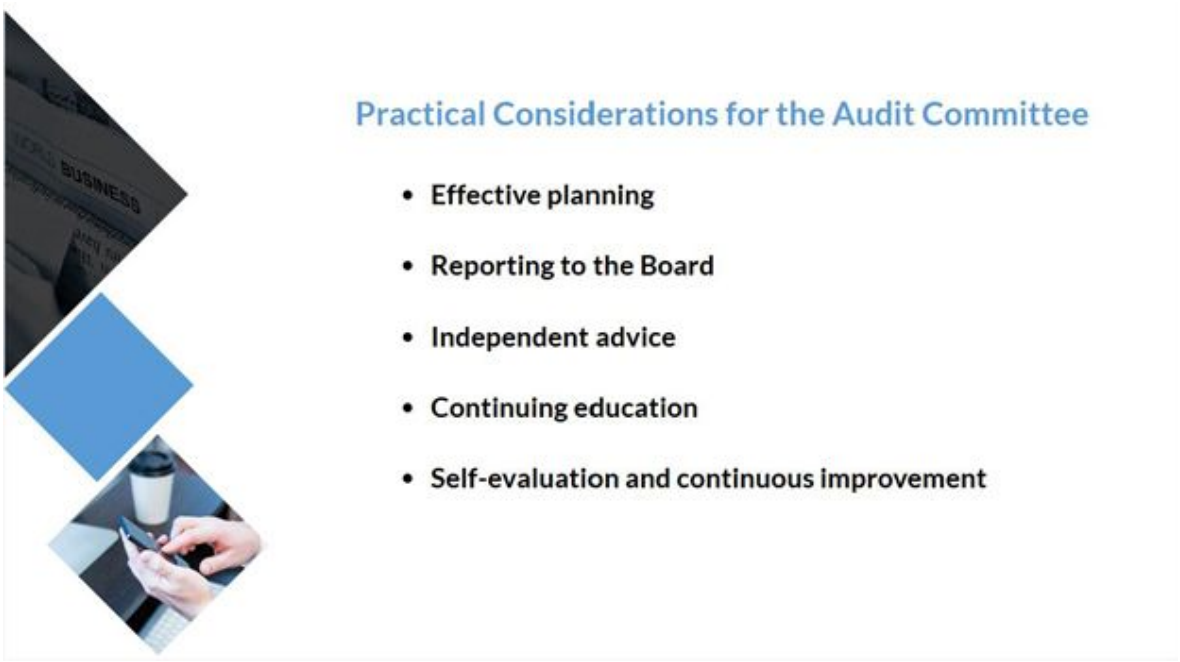
The audit committee should ensure there is an overall cybersecurity plan, as well as an overall data protection plan and individuals responsible for executing the plans. This includes making sure adequate resources are being provided for ongoing testing, improvements, and training in cybersecurity and data protection.

The audit committee should review and advise the Board on privacy and cybersecurity policies, controls, and assessment results. The audit committee should ensure the organization has incident response plans, disaster recovery plans, and contract requirements for third-party access to data.

Special Investigations

As necessary, and with the assistance of staff, the audit committee should also identify the need for independent advisors and/or investigators for special situations, then conduct a search, and make recommendations to the Board. This should include ensuring that there is appropriate independent verification of the performance and exception reports issued by management.

The Role of the Audit Committee



What are some practical considerations for an Audit Committee to operate effectively?

Most audit committees meet quarterly, which provides adequate opportunity to meet with each party on a timely basis and allow effective oversight of activities. The committee should maintain an annual calendar of activities to ensure all responsibilities are completed on a timely basis. In addition, the calendar should be multi-year and include less-than-annual activities such as the external quality assessment of internal audit.

As with all board committees, having an effective reporting process to the full board is important in leveraging the committee's role of improving the board's effectiveness. This includes reporting on both the ongoing responsibilities and activities as well as special investigations and reviews, as required.

When an audit committee has limited relevant experience and expertise in conducting committee activities, it can be helpful to hire an independent audit committee advisor to ensure that the committee is following appropriate practices and asking the right questions.

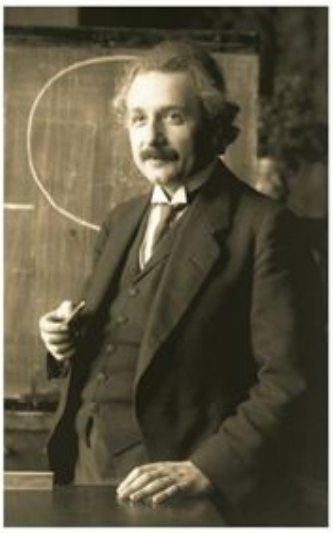
In addition to potentially hiring external advisors, audit committee members should also obtain timely continuing education in areas where there are gaps. This should be included in the mandate of any external advisors that are engaged.

Finally, having a periodic self-evaluation process facilitates a discussion among committee members about what they believe to be working well and where they think the committee can improve. This process can also be helpful in identifying potential needs for external advice or continuing education.

The Role of the Audit Committee

Questions for the Chief Financial Officer

- What is your overall assessment of the company's financial statements, and the level of risk involved in the audit?
- Are the financial statements in the Annual Comprehensive Financial Report, or ACFA, accurate, complete, and compliant with Government Accounting Standards Board, or GASB, requirements?
- What were the key findings and recommendations from the external auditors regarding the ACFR?
- Are there any emerging financial risks or issues that we should be aware of?
- Were there any material audit adjustments or uncorrected misstatements?
- What assumptions and methods were used to calculate the net pension liability and other key metrics?
- Are there any unresolved issues or risks that could affect the ACFR in the future?



Among the most important factors in the success of any board committee, including the audit committee, is asking the right questions. We will now discuss examples of good questions to ask of each key individual that the audit committee works with. These are not meant to be comprehensive but should provide an overview of the types of issues the audit committee should address. We will start with the CFO.

- What is your overall assessment of the company's financial statements, and the level of risk involved in the audit?
- Are the financial statements in the Annual Comprehensive Financial Report, or ACFA, accurate, complete, and compliant with Government Accounting Standards Board, or GASB, requirements?
- What were the key findings and recommendations from the external auditors regarding the ACFR?
- Are there any emerging financial risks or issues that we should be aware of?
- Were there any material audit adjustments or uncorrected misstatements?
- What assumptions and methods were used to calculate the net pension liability and other key metrics?
- Are there any unresolved issues or risks that could affect the ACFR in the future?

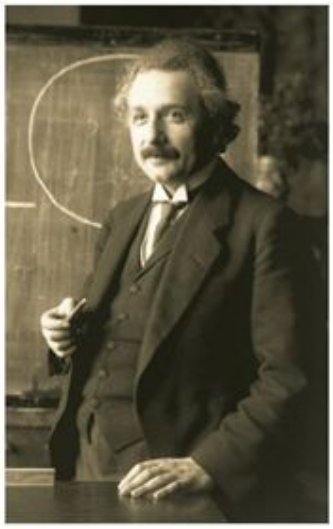
Questions for the Chief Audit Executive

Regarding the independent financial audit:

- What was the extent of your work on the most recent financial audit? If you assisted the external auditor, was there adequate coordination? Did management impose any limitations on you?
- Were there any changes to the scope of work performed from the scope envisioned when it was planned? Were any significant problems encountered?
- What is your evaluation of the external auditors' services for the past year?
- Are you aware of any significant deficiencies or material weaknesses in internal control that management or the external auditors did not identify?

Regarding conflicts of interest:

- Are you aware of any actual or possible illegal or questionable activity or payments? Are you aware of any related party transactions not disclosed in the financial statements?
- Are you aware of any conflicts of interest between officers or employees and the organization?



The Chief Audit Executive, or CAE, is usually a direct report to the Audit Committee. This should be an active relationship that covers several key areas. We will take them one by one.

Regarding the independent financial audit:

- What was the extent of your work on the most recent financial audit? If you assisted the external auditor, was there adequate coordination? Did management impose any limitations on you?
- Were there any changes to the scope of work performed from the scope envisioned when it was planned? Were any significant problems encountered?
- What is your evaluation of the external auditors' services for the past year?
- Are you aware of any significant deficiencies or material weaknesses in internal control that management or the external auditors did not identify?

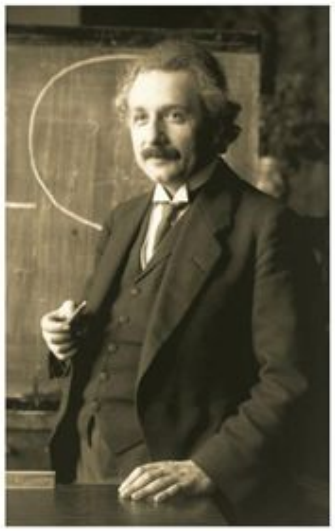
Regarding conflicts of interest:

- Are you aware of any actual or possible illegal or questionable activity or payments? Are you aware of any related party transactions not disclosed in the financial statements?
- Are you aware of any conflicts of interest between officers or employees and the organization?

Questions for the Chief Audit Executive (cont'd)

Regarding internal audit activities:

- What are the department's goals and objectives for this year?
- What will be the scope of your activities this year?
- How will you monitor the organization's code of conduct?
- Do you feel your staffing is adequate?
- How do you ensure auditor independence and objectivity?
- Are there any other items that should be discussed with the audit committee?



Regarding internal audit activities:

- What are the department's goals and objectives for this year?
- What will be the scope of your activities this year?
- How will you monitor the organization's code of conduct?
- Do you feel your staffing is adequate?
- How do you ensure auditor independence and objectivity?
- Are there any other items that should be discussed with the audit committee?

Questions for the CCO, CRO & CTO

Questions for the Chief Compliance Officer

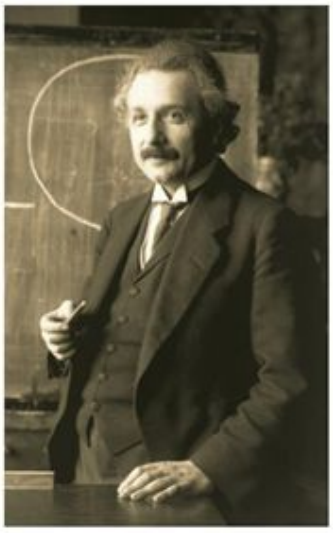
- What measures are in place to assure compliance with regulatory requirements and the system's policies?
- What compliance violations have occurred? Do any indicate a systemic risk or a weak specific control or are they all "one-offs"? Has there been a root cause analysis to see why we have these violations?

Questions for the Chief Risk Officer

- Are there any emerging financial risks or issues that we should be aware of?
- How are we managing the key risks identified, and have there been any significant changes to these risks?

Questions for the Chief Technology Officer

- What are our key cybersecurity risks, and how are we mitigating them?
- What personal data do we maintain and how are we protecting it?
- Who are our key cybersecurity vendors, what do they do, and where do we think we can improve? Do we need additional external assistance in any other areas?
- Are there any recent incidents or breaches, and what have we learned from them?



Although the CCO does not typically report to the Audit Committee, but most frequently to the General Counsel, the Audit Committee has the authority to request periodic meetings to oversee compliance activities. Key questions could include:

- What measures are in place to assure compliance with regulatory requirements and the system's policies?
- What compliance violations have occurred? Do any indicate a systemic risk or a weak specific control or are they all "one-offs"? Has there been a root cause analysis to see why we have these violations?

Similarly, the Chief Risk Officer also usually reports to management, but the Audit Committee should ask for periodic briefings and should consider asking:

- Are there any emerging financial risks or issues that we should be aware of?
- How are we managing the key risks identified, and have there been any significant changes to these risks?

The Chief Technology Officer should keep the Audit Committee appraised of cybersecurity and related risks and mitigations. Potential questions could include:

- What are our key cybersecurity risks, and how are we mitigating them?
- What personal data do we maintain and how are we protecting it?
- Who are our key cybersecurity vendors, what do they do, and where do we think we can improve? Do we need additional external assistance in any other areas?
- Are there any recent incidents or breaches, and what have we learned from them?

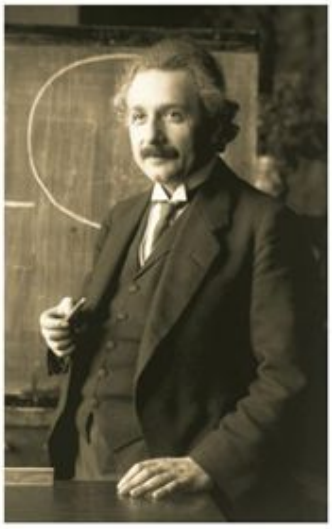
Questions for the Independent External Auditor

Regarding capabilities and process:

- Do you have sufficient knowledge and experience to address the risks and types of transactions managed by the organization, and are your specialists engaged where applicable?
- What technology do you use (e.g. data analytics, AI, remote sensing, etc.) to improve the effectiveness and efficiency of your audits?
- How do you evaluate the reasonableness of significant estimates made by management? How do you challenge these estimates?
- How do you deliver value and insights to management and the committee beyond the audit?

Regarding agency management:

- What is your perspective on management and tone at the top, business trends, and the regulatory environment in financial reporting and standard setting? In instances where the system's needs are evolving, is the audit team also evolving with appropriate talent to serve the system?
- What do you think of management's capabilities and processes? Is the finance function staffed correctly? Does the finance function have appropriate technology to enable it to fulfill its responsibilities?
- What top three areas did you spend the most time discussing with management during the reporting period? Was management cooperative and forthcoming with requested information and documentation in these areas?



The independent external auditor is the most important outside relationship for the Audit Committee. This is an ongoing relationship and the committee should be asking good questions as part of their oversight from several perspectives. Here are some suggested questions to pose:

Regarding capabilities and process:

- Do you have sufficient knowledge and experience to address the risks and types of transactions managed by the organization, and are your specialists engaged where applicable?
- What technology do you use (e.g. data analytics, AI, remote sensing, etc.) to improve the effectiveness and efficiency of your audits?
- How do you evaluate the reasonableness of significant estimates made by management? How do you challenge these estimates?
- How do you deliver value and insights to management and the committee beyond the audit?

Regarding agency management:

- What is your perspective on management and tone at the top, business trends, and the regulatory environment in financial reporting and standard setting? In instances where the system's needs are evolving, is the audit team also evolving with appropriate talent to serve the system?
- What do you think of management's capabilities and processes? Is the finance function staffed correctly? Does the finance function have appropriate technology to enable it to fulfill its responsibilities?

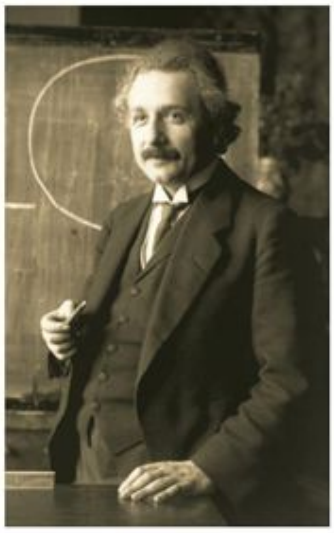
The Role of the Audit Committee

- What top three areas did you spend the most time discussing with management during the reporting period? Was management cooperative and forthcoming with requested information and documentation in these areas?

Questions for the Independent External Auditor (cont'd)

Regarding audit findings:

- When you scoped the audit, what were the key risk areas you wanted to focus on? Did any of them change during the audit? What were the findings?
- Did you find any issues with the system of internal control or the disclosure controls?
- Between last year and this year, were there any notable changes in policies, procedures, controls or the external situation specifically relevant to our organization?
- Is there anything else the committee should know?



Finally, the Audit Committee should have questions of the external auditor regarding audit findings:

- When you scoped the audit, what were the key risk areas you wanted to focus on? Did any of them change during the audit? What were the findings?
- Did you find any issues with the system of internal control or the disclosure controls?
- Between last year and this year, were there any notable changes in policies, procedures, controls or the external situation specifically relevant to our organization?
- Is there anything else the committee should know?

The Role of the Audit Committee

In summary, the audit committee of a public retirement system board is essential to ensuring the integrity and stability of the system.

Today, most Audit Committees at public retirement systems have oversight responsibilities that include internal audit and the independent external audit process, but usually also include risk, compliance, cyber security, and special investigations.

Ideally, an Audit Committee has at least one member with financial expertise, but with public retirement systems this can be a challenge. Consequently, committee assignments need to be carefully considered and continuing education is critical. In some cases it is prudent to bring in independent external experts to advise the committee.

An effective Audit Committee should be interacting with a variety of internal executives, such as the Chief Financial Officer, the Chief Audit Executive, the Chief Compliance Officer, Chief Risk Officer, and Chief Technology Officer, as well as with the independent external auditor and any outside regulators. Consequently, it is very helpful to have a committee calendar that identifies and plans for key committee activities well in advance.

One of the most important considerations for any board committee is to know what questions to ask. With the varied responsibilities of the Audit Committee, having standard questions to ask of each individual who interacts with the committee can be very helpful in ensuring key topics are addressed.

School Employees Retirement System of Ohio
Serving the People Who Serve Our Schools®

INTERNAL AUDIT

FY2027 Audit Plan

FY2027 Audit Plan

Table of Contents

Executive Summary

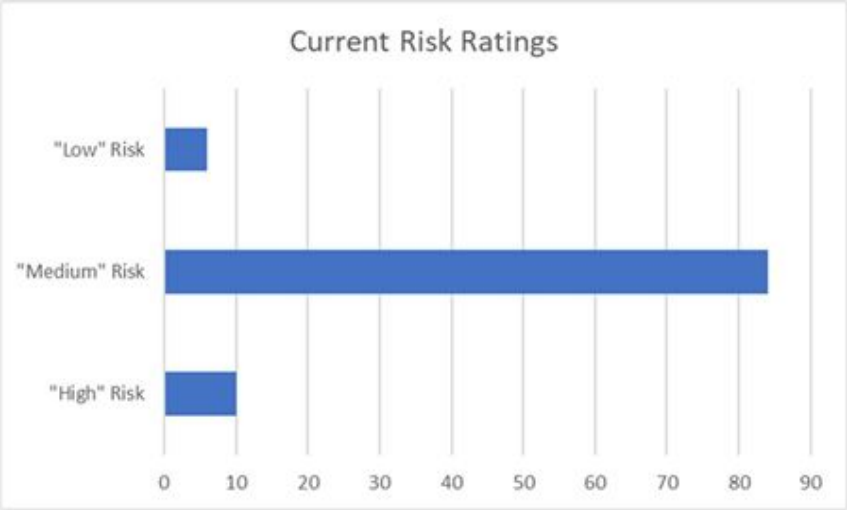
As required by the 2024 Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA) and by the School Employees Retirement System (SERS)' Internal Audit Charter, the following Internal Audit Plan is submitted for Fiscal Year 2027.

SERS' Internal Audit aims to maximize its resources to provide reasonable coverage for activities believed to require the most attention based on SERS' strategies, objectives and risks. The Internal Audit plan is designed to provide coverage of key risks, with consideration of resource availability. Although the audit plan considers a wide-ranging scope of activities, it does not provide coverage for all SERS' components or systems.

The Internal Audit Plan was developed based on conducting risk assessments, incorporates feedback from SERS' management, and auditor judgment. Proposed audits and audit objectives are designed to provide assurance that management has identified key risks, and that management is sufficiently mitigating those risks to an acceptable level.

RISK ASSESSMENT SUMMARY

The risk assessment identifies management and the Audit Committee's perceived level of risk. The risk assessment aligns internal audit resources to those areas that pose the highest risk to SERS' ability to achieve its objectives. Of the 100 auditable areas, six (6) areas have a low-risk rating, 84 areas have a medium risk rating, and ten (10) areas have a high-risk rating compared to FY26 with 94 auditable areas, nine (9) low-risk rated, 79 areas medium risk rated, and six (6) areas with a high-risk rating. See Exhibit 1 and Exhibit 2 for additional details.



AUDIT PLAN SUMMARY

Internal Audit's primary activities include audits and management advisory services. Internal Audit's focus is to actively assist management in addressing investment, operational, cyber, technology, reputational, compliance and regulatory risks. This focus is on department-level control processes, higher risk audit areas, and to provide management with value added recommendations.

The FY2027 audit plan defines specific audit areas intended to be performed in the upcoming year. The specific audit areas are selected from a population of auditable units within each department. The audit plan groups the auditable units, from high to low in terms of risk, based on the risk assessments performed by Internal Audit. The FY2027 audit plan resulted in 100 auditable units compared to 94 in FY2026.

In FY2027, Internal Audit intends to complete the below projects. These include nine audits, three compliance reviews, two consulting projects, and six advisory projects.

Audit

- Continuous auditing/monitoring
- Health Care Audits (pharmacy/medical)
- Health Care Premiums
- Experience Study
- Member Service Team (MST)
- Qualified Excess Benefit Arrangement
- ETF Investments
- IT Change Management
- Investment Compliance with Clearwater

Compliance

- Investment Incentive Compensation
- Undue Influence
- Conflict of Interest

Consulting

- Fiduciary Audit
- Health Care documentation

Advisory Services/Other

- Disaster Recovery Plan
- ORSC Annual Audit Report
- FY28 Audit Planning
- Open audit recommendations
- Audit Committee meeting preparation
- Senior Leadership Team/Director/ other meetings

These audits will evaluate the adequacy and effectiveness of controls, efficiency of operations, safeguarding of assets, and reliability of reporting. When applicable, the audits will assess compliance with applicable laws, regulations, policies, contracts, and ethics.

Interim changes to the audit plan will occur from time to time due to changes in business risks, timing of SERS' initiatives, and staff availability.

FY2027 ANNUAL AUDIT PLAN – PROJECT SUMMARY

Department	Process/ Auditable Area	Est. Hours	Description of IA Activity
Compliance			
1. Executive	Undue Influence	16	Annual evaluation of filings of key SERS leadership to ensure any undue influence is properly reviewed and reported to the Board.
2. Executive	Investment Incentive Compensation	60	Annually review of payment accuracy against policy requirements for investment incentive compensation program.
3. Executive	Conflict of Interest	60	Annual evaluation of disclosure filings by external investment managers and ethics filings by Investment Department personnel to ensure any potential conflicts are properly identified, evaluated, and managed to avoid a conflict of interest.
Audit			
4. All	Continuous auditing	200	Various testing to frequently monitor and assess transactions and controls in real time.
5. Health Care	Pharmacy/Medical	20	Minor IA involvement to review scope, report, and remediation.
6. Health Care	Health Care Premiums	120	Evaluates the accuracy and completeness of entering health care premium data into the system.
7. Finance	Experience Study	80	Ensuring the pension system tables are updated accurately and completely based on the actuarial report.
8. Member Services	MST	120	Review Member Service Team processes, policies and procedures.
9. Member Services	QEBA	80	Ensure the benefits paid above the IRC guidelines are correct.
10. Investments	ETF Investments	60	Review of portfolio holdings, trading activity, and compliance.
11. Information Technology	IT Change Management	160	Review IT change management process.
12. ERM	Invest Compliance	100	Ensure Clearwater is accurate regarding investment compliance req.
Consulting			
13. All	Fiduciary Audit	200	Assist management with responding to the Fiduciary audit requests.
14. Administrative	Health Care Documentation	40	Accurate retention of employee and dependent HC information.
Advisory/Other			
15. All	Disaster Recovery Plan	10	Provide independent insight into how SERS restores critical systems.
16. Executive	ORSC Annual Report	20	Prepare the Audit Committee's annual activities report for the Ohio Retirement Study Council by March 31st.
17. Internal Audit Admin	FY28 IA Audit Plan	80	Conduct risk assessment with input from numerous sources and incorporate audit priorities within the annual audit plan.
18. All	Recommendations	40	Follow-up to ensure action plans are effective and timely.
19. Executive	AC meeting prep	80	Prepare documentation for quarterly Audit Committee meetings.
20. Executive/SERS	SLT/Director/other meetings	300	Departmental consulting and special projects related to various processes.

FY2027 - ESTIMATED QUARTERLY ENGAGEMENT SCHEDULE

Project	Q1	Q2	Q3	Q4
Compliance				
Undue Influence	■			
Investment Incentive Compensation	■			
Conflict of Interest	■			
Audit				
Continuous Auditing	■	■	■	■
Pharmacy/Medical (Outsourced/Consulting)			■	■
Health Care Premiums				■
Experience Study	■	■		
Member Services Team (MST)		■		
Qualified Excess Benefit Arrangement (QEBA)			■	
ETF Investments		■		
IT Change Management			■	
Investment Compliance with Clearwater				■
Consulting				
Fiduciary Audit	■	■	■	■
Health Care Documentation			■	
Advisory/Other				
Disaster Recovery Plan		■		■
ORSC Audit Committee Annual Report		■		
FY28 Internal Audit Plan				■
Open Audit Recommendations	■	■	■	■
Audit Committee Preparation	■	■	■	■
Senior Leadership Team/Director/other meetings	■	■	■	■

I. OVERVIEW AND REQUIREMENTS

INTRODUCTION

This Internal Audit Plan outlines the priorities, scope, and approach of the Internal Audit function for Fiscal Year 2027. The plan has been developed in alignment with the 2024 Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA) and is designed to provide independent, objective assurance and advisory services.

Given the structure of a one-person Internal Audit function, this plan emphasizes a risk-based, high-impact approach, leveraging other assurance providers where appropriate and focusing audit efforts on areas of greatest risk to the pension plan.

MISSION

The mission of the SERS Internal Audit Department is to provide independent, objective assurance and consulting activities designed to improve management practices, identify operational improvement, and reduce SERS' risk exposure.

PURPOSE

The purpose of Internal Audit is to strengthen SERS' ability to create, protect, and sustain value by providing the Audit Committee and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

VISION

The vision of SERS' Internal Audit is to be a highly regarded internal audit organization that adds value and mitigates risk by working collaboratively with SERS' leadership to provide objective insights and innovative recommendations to improve operations.

INDEPENDENCE

In order to be effective, fulfill its role, and accomplish its objectives, Internal Audit must be independent of management and objective in performance of its work. The Chief Audit Officer (CAO) reports directly to the Audit Committee and administratively to the Executive Director.

REQUIREMENTS

The IIA's *Global Internal Audit Standards (2024),* specifically Standard 9.4 on the Internal Audit Plan, requires that:

- The chief audit executive (CAE) must create an internal audit plan that supports achievement of the organization's objectives.
- The CAE must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the CAE's understanding of the organization's governance, risk management, and control processes.
- The assessment must be performed at least annually, be dynamic and updated timely in responses to changes in the organization's business, risk operations, programs, systems, controls, and organizational culture.

II. THE INTERNAL AUDIT PROCESS

The FY27 Internal Audit Plan is designed to provide audit coverage across the entire organization by deploying Internal Audit resources in an effective and efficient manner.

This document describes the systematic process used by internal audit to develop its risk assessment and annual audit plan process. Risk assessment is inherently subjective; as such, quantitative analysis is supplemented with Internal Audit judgment and management input.

The following outlines the Audit Plan development and execution:

Audit Plan Development		Audit Plan Execution		
IA STRATEGIC PLAN, RISK ASSESSMENT AND AUDIT UNIVERSE	**AUDIT PLAN**	**PLANNING**	**FIELDWORK & DOCUMENTATION**	**REPORT TO AUDIT COMMITTEE**
▪ Develop Internal Audit Strategic Plan to align with mission, vision, and values of SERS Strategic Plan. ▪ Perform risk assessment with management. ▪ Measure the risk of each area identified in the audit universe and assign a risk rating (High, Medium, Low) ▪ Evaluate current audit universe by utilizing multiple sources of information. ▪ Update audit universe to include added or removed audit areas.	▪ Establish a schedule of audits by process/area based on annual risk assessment and previous year's audit results.	▪ Audit engagement memo sent to department being audited. ▪ Internal Audit meets with department management to review risk areas and determine audit scope.	▪ Internal Audit performs audit. ▪ Any recommendations are reviewed with department management. ▪ Exit meeting held to finalize any recommendations and review management's plan for remediation.	▪ Complete audits reported to Audit Committee. ▪ Outstanding recommendations shared with Audit Committee. ▪ Status of annual audit plan shared with Audit Committee.

III. RISK ASSESSMENT AND AUDIT UNIVERSE

RISK ASSESSMENT

The objective of the risk assessment was to perform an entire business risk assessment of SERS to align internal audit resources to those areas that pose the highest risk to SERS' ability to achieve its objectives.

The risk assessment (Exhibit 1 and Exhibit 2) covered all of SERS to ensure that the scope of the final audit plan was comprehensive and covered all operations at SERS. Additionally, efforts were made to ensure key members of management and the Audit Committee were interviewed and their views on risk were considered. Discussions focused on the current state of activities as well as near-term changes that may affect processes and risk.

The risk assessment serves as the basis for prioritizing and allocating internal audit resources, specifically to those areas posing a greater degree of risk to SERS.

Changes that occurred during the year, as well as anticipated changes in the near term, were also considered and analyzed (i.e. process changes, key personnel changes, information system changes, etc.) to help assess SERS' current and emerging risks.

In addition to the above, Internal Audit collaborated with Enterprise Risk Management (ERM) as it relates to their evaluation of risk. This involved including ERM in the risk assessment meetings with management to ensure overall alignment between Internal Audit and ERM. This also involved comparing ERM's risk assessments to the IA risk assessment used for audit planning purposes while maintaining organizational independence.

Internal Audit's risk assessment is solely for the purpose of developing the audit plan and focuses on auditable entities, not the entire universe of risks facing SERS. Also, the assessment does not seek to determine or evaluate management's risk tolerance or risk appetite.

AUDIT UNIVERSE

The audit universe (Exhibit 1 and Exhibit 2) is the collective body of potentially auditable functions that exist within SERS. The audit universe was developed based on identified significant processes and functions. The primary source for determining the significant processes and functions was inquiries of management and reviewing SERS' reporting structure.

Each audit unit has an objective, or a specific result that SERS expects to achieve. Each objective has associated risks, or factors that may affect the attainment of the objectives. Each risk has associated controls, or activities performed to reduce the risk. Each audit tests the controls to ensure they are operating as intended.

RISK FACTORS AND WEIGHTING

The primary objective of this risk scoring method is to focus audit resources on areas of high and moderate risk, ensuring thorough coverage over several years.

Risk factors are selected based on guidance from the IIA, historical knowledge related to pensions and established internal auditing practices.

Each risk factor is scored according to its potential effect on SERS, with weighted values assigned within each audit unit. Risk scoring is based on numerical values from lowest to highest (i.e. 1 being the lowest and 5 being the highest). After rating the various risk factors, their weights are combined to yield a composite risk score for each area. The risk scores are then rated from low, medium, and high (low risk rating 1-2.25, medium risk rating 2.26-3.74, high risk rating 3.75-5). This composite score guides the prioritization of areas in the annual audit plan.

The risk assessment process involved nine meetings with management. In these meetings management and IA assigned risk scoring to the following risk factors for each audit unit:

Risk Factors	Weight	Description
A. Control Design and Effectiveness	20%	Assessed reliability of internal controls are important in judging the likelihood of errors in the system; consider known problems/prior audit results.
B. Impact to Members, Retirees, Employers, Public, Reputation	20%	Impact to SERS' constituents; management or other stakeholder concerns can influence the priority of an auditable area; consider reputational impact to SERS by failure of a sensitive process.
C. Changes in Organization, Programs, and Operations	15%	A dynamic change to systems/processes/people, increases probability of efficiencies as well as errors.
D. Complexity of Activities, Operations, and/or Systems	15%	Degree of process complexity or perceived impact of IT controls.
E. Dollar Materiality/Operational Impact	15%	Financial statement impact, relative importance, or sensitivity to ongoing operations.
F. Impact of Fraud, Waste, or Data Loss	15%	Impact of illegal acts, wasteful spending, or sensitive data loss can result in a heightened consequence regardless of the dollar amount.

A. CONTROL DESIGN AND EFFECTIVENESS

The assessed reliability of the internal control system is important in judging the likelihood of errors in the system. Internal controls consider the adequacy of written procedures and whether or not controls have been previously tested.

B. IMPACT TO MEMBERS, RETIREES, EMPLOYERS, PUBLIC, REPUTATION

Management or other stakeholder concerns can influence the priority of an auditable area and could take priority over other risk factors in some cases. The reputation of SERS can be impacted by failures in certain sensitive processes. Amount of impact the audit area has on SERS' constituents. Includes concern for public perception. Concern about adverse publicity; laws and regulations; customer demands; and political exposure.

C. CHANGES IN ORGANIZATION, PROGRAMS, AND OPERATIONS

A dynamic environmental change, in terms of systems/processes/people, increases the probability of efficiencies as well as errors occurring. Changes in operations can impact the efficiency and effectiveness of the organization's performance. Criteria include changes in staff size, processing changes (manual to computerized), systems (input and/or output), as well as staff turnover. This area includes concerns of rapid growth in personnel size or additional programs added to an operational area.

Changes in operation to meet statutory, regulatory, and legal requirements, and/or to address organizational restructuring including modifications to manual or automated procedures such as increased use of technology. Changes in operations since this area was last audited may have a significant impact on accuracy and timeliness of work completed, efficiency and effectiveness of operation, and the reliability of work products and records.

D. COMPLEXITY OF ACTIVITIES, OPERATIONS, AND/OR SYSTEMS

Complexity includes amount of time, number of steps, techniques or procedures, degree of difficulty, training necessary, and interaction with other organizations/divisions necessary to complete a work task or process a transaction. Complexity can increase both the probability of error and the effort required to monitor the system. Includes complexity of federal and state laws, rules and regulations governing a particular program.

Computer applications affect the accuracy and timeliness of completed work tasks, as well as the productivities of the staff. Information systems should process information in a secure, reliable and accurate manner.

Age, condition, efficiency and effectiveness of the data processing system specific to this audit area, and the perceived impact of general information technology controls related to: consistent use of an acceptable systems development methodology (including programmer and user documentation and testing procedures), consistent use of an acceptable project management system, effective computer maintenance change controls (to assure application program changes are properly authorized, managed, and recorded), and effective logical access security to guard against unwarranted access and unauthorized changes to computer programs or data.

E. DOLLAR MATERIALITY/OPERATIONAL IMPACT

Materiality focuses on the organizational impact due to financial statement materiality, relative importance, and/or sensitivity to negative public exposure of a process or system.

F. IMPACT OF FRAUD, WASTE, OR DATA LOSS

Risk inherent in a process or system that employees (including management) individually, or in collusion with others, commit fraud, resulting in financial loss or unauthorized use of financial instruments, physical assets and/or confidential information. For IT systems, also consider the level and type of security threat(s) present (e.g., a firewall has a higher level of security threat associated with it than an internal file server).

The composite risk rating system is a point in time assessment and ratings may vary based on an individual's perspective or recent event history. Ratings are designed to evaluate SERS risk exposures related to governance, operations, and information systems regarding achievement of their strategic objectives; reliability of financial information; effectiveness and efficiency of operations; safeguarding of assets; and compliance with laws, regulations, and contracts.

To minimize the potential for duplication of effort and to maximize the amount of coverage achieved, the CAO will consider other assurance providers (both internal and external) and their scope and intended reliance by internal audit.

COMBINED RISK RATING

After rating the above six risk factors, their weights are combined to yield a composite risk rating for each auditable area. The combined risk rating is the primary determinant of risk when determining the allocation of internal audit resources and development of the annual audit plan. Results for the risk assessment are as follows:

	Low	Medium	High	Total
Combined Risk Rating	6	84	10	100

IV. AUDIT PLAN

The annual audit plan was prepared using the risk assessment process and identifies individual projects to be completed during the FY2027 audit plan. The types of projects include audit, compliance, consulting, and advisory services. These are outlined as follows:

	Audit	Compliance	Consulting / Special Projects	Advisory Services
Focus	Assess evidence available to provide assurance on an audit objective	Determine specific steps to test with management's agreement and report on results	Respond to requests for formal study or assessment with recommendations; no assurance provided	Prepare material for quarterly Audit Committee meetings, participate in management meetings, etc.
Deliverable	Audit report for distribution unless protected by statute	Compliance report for distribution unless protected by statute	Can vary by project. May or may not include a written report.	Verbal discussion or a brief memo to management
Estimated Level of Effort	~940 hours	~140 hours	~240 hours	~530 hours

The audit plan is a methodical approach to scheduling audits based on reviewing the combined risk rating for each auditable area (low, medium, or high), the length of time since the last audit, and available internal audit resources. Throughout the year Internal Audit will stay in regular communications with each department. If new or evolving risks arise, the audit plan will be updated accordingly. Additionally, audits may be performed at the express request of the Audit Committee.

Internal Audit serves a critical role in assisting the Audit Committee to facilitate its risk oversight responsibilities.

In selecting specific projects for inclusion in the annual audit plan, IA places priority on providing coverage of high-risk operations and of areas of interest to senior management.

The FY2027 audit plan includes 1,316 hours to provide for project-related time compared to 1,330 hours in the FY2026 audit plan. Non-project related time is budgeted for 764 hours compared to 750 in the FY2026 audit plan. The project-related time includes time budgeted for audits, compliance, and consulting/special projects. Non-project related time includes time associated with vacation, holidays, senior-leadership team meeting and director meeting attendance, audit committee meeting preparation, training, and other administrative matters. The time allocations are summarized in the FY2027 Annual Audit Plan Hours Summary (Exhibit 3). The time summary shows how the time will be allocated among project-related and non-project related time.

CONTINUOUS AUDITING

Continuous auditing involves testing multiple areas to monitor and assess transactions and controls in real time. Testing includes frequent testing of areas like payables, credit card transactions, and member refunds. The test frequency varies—bi-monthly, quarterly, or annually—depending on the area.

CO-SOURCED/OUTSOURCED AUDITS

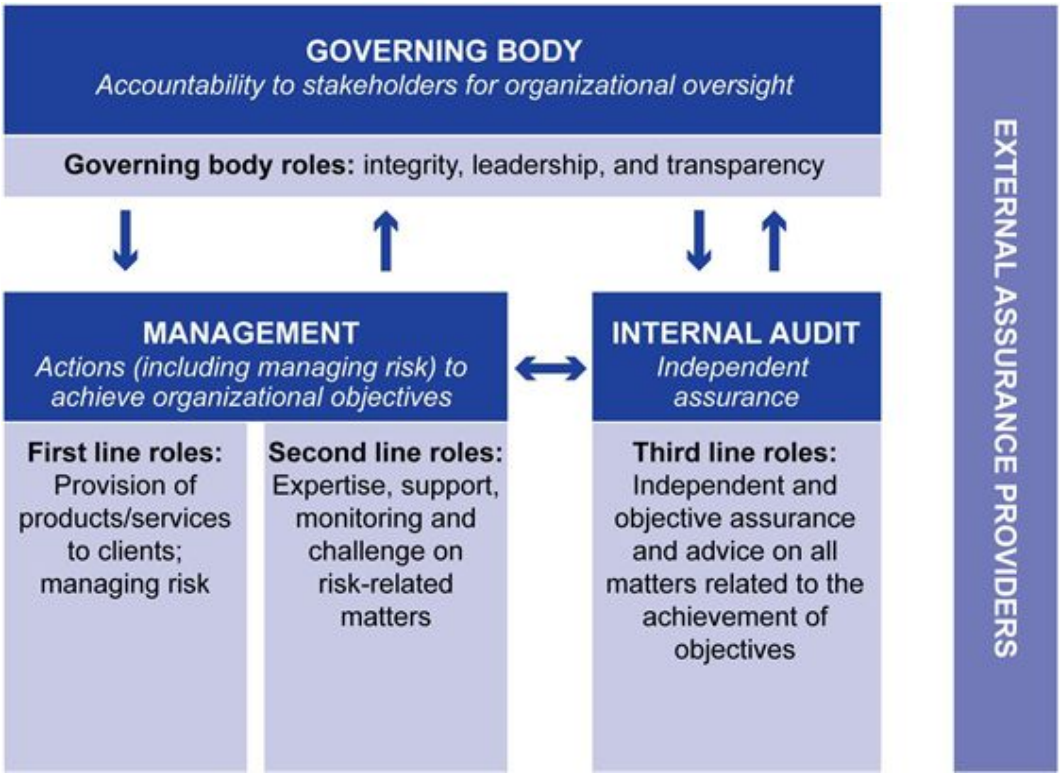
Based on resource constraints and/or outside expertise, an audit or project may be co-sourced or outsourced. These projects often follow an agile audit approach. Agile auditing includes being flexible and focusing resources on identified critical risks.

EXTERNAL AUDITORS

Internal Audit continues to coordinate its audit plan with SERS' external auditors to ensure appropriate coverage is achieved through the internal and external audit plans. As part of the audit planning process, IA met with the external auditors and discussed areas covered in the annual financial statement audit. IA excluded these areas in the FY27 audit plan to avoid duplication of audit coverage.

An evaluation of third-party assurance activities was conducted to maximize audit coordination efforts and coverage.

THREE LINES OF DEFENSE MODEL (INSTITUTE OF INTERNAL AUDITORS)



NOTE: Internal Audit's plan incorporates audit coverage from external audit; 3rd party external reviews within Executive, Health Care, Administrative Services, and Member Services; and 2nd Line of Defense SERS' monitoring within investment compliance, investment accounting, and IT security. Internal Audit's review of selected auditable units is not intended to offer a complete opinion on every aspect of the category. Rather, Internal Audit judgmentally evaluates the auditable unit and focuses its scope and objectives on key risks and controls to evaluate and report the results to the Audit Committee. SERS is not "relying" on the work of the external auditors, rather avoiding duplication of efforts by not allocating Internal Audit hours to these areas.

NOTE: FY27 plan involved extensive independent research, coordination with other assurance service providers, and management's involvement in identifying audit priorities - including nine departmental/senior leadership meetings involving approximately 40 leaders. ERM staff were also included in these meetings to share information and provide added input on risk.

Internal Audit (IA) will evaluate the auditable areas and make modifications throughout the year based upon changes to SERS' risk profile. IA will also participate in SERS' strategic planning process and align IA's plan with appropriate assurance and consulting activities.

Exhibit 1

Risk Rating – Highest to Lowest
(Risk Assessment and Audit Universe)

Exhibit 1

SERS			Risk Factors										
2027 Risk Assessment - Highest to Lowest	20%	20%	15%	15%	15%	15%	100%						
Auditable Area	**A. Control Design and Effectiveness**	**B. Impact to Members, Retirees, Employers, Public, Reputation**	**C. Changes in Organization, Programs, Operations**	**D. Complexity of Activities, Operations, or Systems**	**E. Dollar Materiality/ Operational Impact**	**F. Impact of Fraud, Waste, or Data Loss**	**Combined Risk Rating**	**Risk Rating**	**Last Year Audited**	**Internal Audit Planned FY27 Coverage**	**FY27 Planned Hours**	**External Audit**	**Fiduciary Audit**
Retirement - Benefits / Calculations / Estimates	3	5	3	4	5	5	4.15	High	FY2020			X	
Application Management - Software Management/SMART	3	5	3	4	5	5	4.15	High	FY2020				X
Investment Accounting - Custody & Master Record Keeper	2	5	4	4	5	5	4.10	High	-			X	
Member Withdrawals / Refunds & Lump Sum	3	4	4	4	5	5	4.10	High	FY2021			X	
Enterprise Risk Management -Information Security Program (Fraud Program)	4	4	4	4	3	5	4.00	High				X	
Identity and Access Management (IAM)	3	4	3	4	5	5	3.95	High	FY2024			X	X
Enterprise Risk Management - Information Security Program	2	5	3	4	5	5	3.95	High	FY2019			X	X
Alternative Investments - Real Assets, Private Equity/Credit, Opportunistic	2	4	4	5	5	4	3.90	High	-			X	X
Member Self-Service Portal (MSS)	3	5	3	4	3	5	3.85	High	FY2026				
Disability - Benefits / Calculations	2	4	3	4	5	5	3.75	High	FY2023			X	
Experience Study (every five years)	4	4	4	4	4	2	3.70	Medium	FY2027	X	80		
Enterprise Risk Management - Investment Compliance (part of Conflict of Interest)	4	4	4	4	3	3	3.70	Medium	FY2026	X (in addition to conflict of interest - investment compliance with Clearwater)	100		X
Health Care Fund Revenue - Premiums, Rebates, Funding Allocation	2	5	3	3	5	3	3.50	Medium	FY2016	X (Updating Premiums)	120	X	X
Employer Reporting and Remittance of Contributions	2	5	2	3	5	4	3.50	Medium	FY2023			X	
Taxes	3	4	4	4	3	3	3.50	Medium					
Legal - HIPAA	2	5	3	3	4	4	3.50	Medium	-				
Required Minimum Distribution (RMD)	3	4	3	3	4	4	3.50	Medium	FY2026				
Business Continuity / Disaster Recovery	3	4	3	3	5	3	3.50	Medium	FY2021				X
Claims - Medical and Pharmacy	2	4	3	4	5	3	3.45	Medium	FY2026	X	20	X	X
Purchasing	2	4	3	3	4	5	3.45	Medium	FY2026				
Cloud Based Computing	3	3	4	3	4	4	3.45	Medium	FY2022				X
Funding Levels - Compliance and Return Rate	2	5	3	4	5	1	3.35	Medium	-				
Financial Reporting / ACFR	2	4	3	4	3	4	3.30	Medium	-			X	
Payment Processing / Payables	2	4	2	3	4	5	3.30	Medium	FY2022			X	
Infrastructure	3	3	2	3	5	4	3.30	Medium	FY2025				X
Health Care Vendor Management and Reconciliation	2	4	3	4	4	3	3.30	Medium					
Investment Management Fees	2	4	3	4	4	3	3.30	Medium	-				X
Investment Governance & Management - SERS Investment Committee	2	4	3	4	4	3	3.30	Medium	FY2016				X
Member Account Maintenance	2	4	3	3	3	5	3.30	Medium	FY2022			X	
Enterprise Risk Management - BC/DR	2	4	3	3	5	3	3.30	Medium	FY2021				X
IT Change Management	2	3	4	4	3	4	3.25	Medium	FY2017	X	160	X	X
Survivor - Benefits / Calculations	2	3	3	4	3	5	3.25	Medium	FY2024			X	
Enterprise Risk Management - Vendor Risk Management	2	5	2	3	4	3	3.20	Medium					X
Investment Accounting - Operational Due Diligence	2	4	3	4	3	3	3.15	Medium	-			X	
Web Self Service - *eSERS*	2	4	3	3	4	3	3.15	Medium	-				
Investment Risk Management	2	4	3	4	3	3	3.15	Medium	-				X

SERS

2027 Risk Assessment - Highest to Lowest

			Risk Factors										
	20%	20%	15%	15%	15%	15%	100%						
Auditable Area	A. Control Design and Effectiveness	B. Impact to Members, Retirees, Employers, Public, Reputation	C. Changes in Organization, Programs, Operations	D. Complexity of Activities, Operations, or Systems	E. Dollar Materiality/ Operational Impact	F. Impact of Fraud, Waste, or Data Loss	Combined Risk Rating	Risk Rating	Last Year Audited	Internal Audit Planned FY27 Coverage	FY27 Planned Hours	External Audit	Fiduciary Audit
Capital Calls and Distributions	2	4	2	3	4	4	3.15	Medium	FY2021				
Records Management / Imaging	2	4	3	3	3	4	3.15	Medium	-				X
Death Benefits - SSN Matches/Proof of Life	2	4	3	3	3	4	3.15	Medium	FY2022				
Identify and Access Management (NetSuite, Clear Water, Adaptive, Bank Accounts)	3	2	3	3	4	4	3.10	Medium	FY2026				
Fixed Income, US/Non-US Equity, Foreign Currency, Mutual Funds, Cash Equivalents	2	3	4	4	4	2	3.10	Medium	-			X	X
Investor Owned ETFs	2	3	4	4	4	2	3.10	Medium	-	X	60		
Enterprise Risk Management -Information Security Program (HIPAA Compliance)	2	3	3	3	4	4	3.10	Medium				X	
IT Vendor Management and transmission/retention of data	3	4	2	2	3	4	3.05	Medium	FY2019				X
Confidential Data Management (Health Care)	2	4	2	3	3	4	3.00	Medium					
Interest and Dividend Income	2	4	3	2	3	4	3.00	Medium	-			X	X
Mobile Device Security	3	3	2	3	3	4	3.00	Medium					X
Physical Access - IT General Controls	2	4	2	3	3	4	3.00	Medium	FY2016			X	X
Asset Management - Hardware	3	3	2	3	3	4	3.00	Medium	FY2019				X
Enterprise Risk Management - Enterprise Risk Program	2	4	2	2	4	4	3.00	Medium					X
Retiree Accounting	2	4	3	3	3	3	3.00	Medium	-				
Investment Due Diligence Review (Existing Investments)	2	4	3	4	2	3	3.00	Medium	-				X
MST / Online Chat	2	4	3	3	3	3	3.00	Medium	-	X (MST only)	120		X
Portability - Retirement System Transfers / Calculations	2	4	3	3	3	3	3.00	Medium	FY2016				
Employee Health Care Plan / Costs	2	3	3	2	4	4	2.95	Medium	FY2017				
Medicare B Fund - Retirement Benefit Payments	2	3	3	3	3	4	2.95	Medium				X	
Health Care Plan - Participant Eligibility / Calculation / Service	2	3	3	3	3	4	2.95	Medium				X	
Legal - WCAG 2.0 AA compliance	2	3	3	3	3	4	2.95	Medium					
Enterprise Risk Management - Insurance	2	2	2	2	5	5	2.90	Medium					
Government Relations - Legislation (Advocacy, Monitoring, Response)	2	5	3	3	3	1	2.90	Medium	-				
Contract Administration and Monitoring	3	3	3	2	3	3	2.85	Medium	FY2016				
Confidential Data Management (Member Services)	2	4	2	2	3	4	2.85	Medium	-				
Enterprise Risk Management - Artificial Intelligence Governance	3	3	3	3	2	3	2.85	Medium					
Legal - Contract Review & Execution	1	4	2	2	4	4	2.80	Medium	FY2016				
Vehicles/Fleet/Accident Reporting	2	3	3	3	3	3	2.80	Medium					
IT Governance	3	4	3	2	2	2	2.75	Medium	FY2018				X
Service Purchase Credit / Calculation	3	3	3	2	1	4	2.70	Medium	FY2023				
Retirement - Application Process	2	4	3	3	2	2	2.70	Medium	-				
Mail Room / Print Operations	2	3	2	3	3	3	2.65	Medium	FY2019				
Legal - Litigation	1	4	2	3	4	2	2.65	Medium	-			X	
Employee Payroll, Timekeeping & Leave	2	3	2	2	3	4	2.65	Medium	FY2021			X	X
Investment Incentive Compensation	2	3	3	3	2	3	2.65	Medium	FY2026	X	60		X
Treasury/Cash Management	2	2	3	2	3	4	2.60	Medium	-			X	
Information and Communications	2	4	3	2	2	2	2.55	Medium	-				
Building Services (OSERS Building, Land, Furniture, Security, Safety)	2	3	2	2	3	3	2.50	Medium	-				
Budget Processing & Reporting	2	3	2	2	4	2	2.50	Medium	-				

Exhibit 1

SERS			Risk Factors										
2027 Risk Assessment - Highest to Lowest	20%	20%	15%	15%	15%	15%	100%						
Auditable Area	**A. Control Design and Effectiveness**	**B. Impact to Members, Retirees, Employers, Public, Reputation**	**C. Changes in Organization, Programs, Operations**	**D. Complexity of Activities, Operations, or Systems**	**E. Dollar Materiality/ Operational Impact**	**F. Impact of Fraud, Waste, or Data Loss**	**Combined Risk Rating**	**Risk Rating**	**Last Year Audited**	**Internal Audit Planned FY27 Coverage**	**FY27 Planned Hours**	**External Audit**	**Fiduciary Audit**
Personnel Management	2	3	3	2	3	2	2.50	Medium	-				X
Counseling	2	3	3	2	3	2	2.50	Medium					
Reemployed Retirees / QEBA	2	3	2	4	1	3	2.50	Medium	-	X (QEBA)	80		
Tenant Services (OSERS - Suite and Parking services)	2	2	2	2	3	4	2.45	Medium	FY2024				
Cash and Receivables (Operations)	2	2	2	2	3	4	2.45	Medium	-			X	
Legal - Administrative Rules, Public Records Requests, Other	1	3	2	3	3	3	2.45	Medium					
Board Governance	1	3	2	3	3	3	2.45	Medium					
Securities Lending	2	2	3	3	2	3	2.45	Medium	-			X	
Unitized Accounting Practices	2	2	3	3	3	2	2.45	Medium	-			X	
QEBA (Shared with Member Services)	2	2	2	4	2	3	2.45	Medium	-				
Investment Data Management / Maintenance / Retention	1	2	3	3	2	4	2.40	Medium	-				
Member Statements	2	4	3	2	2	1	2.40	Medium	FY2024				
Legal - Tax Compliance	1	4	2	2	4	1	2.35	Medium	FY2016				
Legal - Sensitive Data Handling (Division Of Property Orders, Power of Attorney)	1	4	2	2	2	3	2.35	Medium	FY2016				
Information Governance	2	3	2	2	2	3	2.35	Medium					
Government Relations - Proxy Voting	2	3	3	2	2	2	2.35	Medium	-				
Capital Project Activities	2	1	2	2	3	4	2.25	Medium	-				
Travel Expenses	2	4	2	1	1	3	2.25	Medium	-				
Conflicts of Interest (Investment Managers / Vendors)	1	3	2	2	2	3	2.15	Low	FY2026	X	60		X
Policy / Procedure - Development, Review, and Monitoring	1	3	3	2	2	1	2.00	Low	FY2017				X
Undue Influence Forms (certain SERS associates)	1	3	2	1	1	4	2.00	Low	FY2026	X	16		X
Fixed Assets / Inventory	2	1	2	2	2	3	1.95	Low	-			X	
Employment Practices (Recruitment, onboarding, separations, etc.)	2	2	2	1	1	1	1.55	Low	-				
Other Benefits	2	1	2	1	1	2	1.50	Low	-				

Exhibit 2

Risk Rating – By Department
(Risk Assessment and Audit Universe)

Exhibit 2

SERS			Risk Factors										
2027 Risk Assessment - by Department	20%	20%	15%	15%	15%	15%	100%						
Auditable Area	A. Control Design and Effectiveness	B. Impact to Members, Retirees, Employers, Public, Reputation	C. Changes in Organization, Programs, Operations	D. Complexity of Activities, Operations, or Systems	E. Dollar Materiality/ Operational Impact	F. Impact of Fraud, Waste, or Data Loss	Combined Risk Rating	Risk Rating	Last Year Audited	Internal Audit Planned FY27 Coverage	FY27 Planned Hours	External Audit	Fiduciary Audit
Building & Tenant Services													
Building Services (OSERS Building, Land, Furniture, Security, Safety)	2	3	2	2	3	3	2.50	Medium	-				
Tenant Services (OSERS - Suite and Parking services)	2	2	2	2	3	4	2.45	Medium	FY2024				
Capital Project Activities	2	1	2	2	3	4	2.25	Medium	-				
Health Care													
Health Care Fund Revenue - Premiums, Rebates, Funding Allocation	2	5	3	3	5	3	3.50	Medium	FY2016	X (Updating Premiums)	120	X	X
Claims - Medical and Pharmacy	2	4	3	4	5	3	3.45	Medium	FY2026	X	20	X	X
Health Care Vendor Management and Reconciliation	2	4	3	4	4	3	3.30	Medium					
Confidential Data Management (Health Care)	2	4	2	3	3	4	3.00	Medium					
Medicare B Fund - Retirement Benefit Payments	2	3	3	3	3	4	2.95	Medium				X	
Health Care Plan - Participant Eligibility / Calculation / Service	2	3	3	3	3	4	2.95	Medium				X	
Finance													
Purchasing	2	4	3	3	4	5	3.45	Medium	FY2026				
Employer Reporting and Remittance of Contributions	2	5	2	3	5	4	3.50	Medium	FY2023			X	
Investment Accounting - Custody & Master Record Keeper	2	5	4	4	5	5	4.10	High	-			X	
Financial Reporting / ACFR	2	4	3	4	3	4	3.30	Medium	-			X	
Retiree Accounting	2	4	3	3	3	3	3.00	Medium	-				
Payment Processing / Payables	2	4	2	3	4	5	3.30	Medium	FY2022			X	
Investment Accounting - Operational Due Diligence	2	4	3	4	3	3	3.15	Medium	-			X	
Contract Administration and Monitoring	3	3	3	2	3	3	2.85	Medium	FY2016				
Budget Processing & Reporting	2	3	2	2	4	2	2.50	Medium	-				
Treasury/Cash Management	2	2	3	2	3	4	2.60	Medium	-			X	
Unitized Accounting Practices	2	2	3	3	3	2	2.45	Medium	-			X	
Travel Expenses	2	4	2	1	1	3	2.25	Medium	-				
Cash and Receivables (Operations)	2	2	2	2	3	4	2.45	Medium	-			X	
Fixed Assets / Inventory	2	1	2	2	2	3	1.95	Low	-			X	
Identify and Access Management (NetSuite, Clear Water, Adaptive, Bank Accounts)	3	2	3	3	4	4	3.10	Medium	FY2026				
QEBA (Shared with Member Services)	2	2	2	4	2	3	2.45	Medium	-				
Taxes	3	4	4	4	3	3	3.50	Medium	-				
Experience Study (every five years)	4	4	4	4	4	2	3.70	Medium	-	X	80		
Web Self Service - *eSERS*	2	4	3	3	4	3	3.15	Medium	-				

SERS			Risk Factors										
2027 Risk Assessment - by Department	20%	20%	15%	15%	15%	15%	100%						
Auditable Area	**A. Control Design and Effectiveness**	**B. Impact to Members, Retirees, Employers, Public, Reputation**	**C. Changes in Organization, Programs, Operations**	**D. Complexity of Activities, Operations, or Systems**	**E. Dollar Materiality/ Operational Impact**	**F. Impact of Fraud, Waste, or Data Loss**	**Combined Risk Rating**	**Risk Rating**	**Last Year Audited**	**Internal Audit Planned FY27 Coverage**	**FY27 Planned Hours**	**External Audit**	**Fiduciary Audit**
Legal, Communications, & Government Relations													
Funding Levels - Compliance and Return Rate	2	5	3	4	5	1	3.35	Medium	-				
Government Relations - Legislation (Advocacy, Monitoring, Response)	2	5	3	3	3	1	2.90	Medium	-				
Legal - Litigation	1	4	2	3	4	2	2.65	Medium	-			X	
Legal - HIPAA	2	5	3	3	4	4	3.50	Medium	-				
Information and Communications	2	4	3	2	2	2	2.55	Medium	-				
Legal - Tax Compliance	1	4	2	2	4	1	2.35	Medium	FY2016				
Legal - Sensitive Data Handling (Division Of Property Orders, Power of Attorney)	1	4	2	2	2	3	2.35	Medium	FY2016				
Legal - Administrative Rules, Public Records Requests, Other	1	3	2	3	3	3	2.45	Medium					
Legal - Contract Review & Execution	1	4	2	2	4	4	2.80	Medium	FY2016				
Legal - WCAG 2.0 AA compliance	2	3	3	3	3	4	2.95	Medium					
Government Relations - Proxy Voting	2	3	3	2	2	2	2.35	Medium	-				
Vehicles/Fleet/Accident Reporting	2	3	3	3	3	3	2.80	Medium					
Mail Room / Print Operations	2	3	2	3	3	3	2.65	Medium	FY2019				
Board Governance	1	3	2	3	3	3	2.45	Medium					
Administrative Services													
Personnel Management	2	3	3	2	3	2	2.50	Medium	-				X
Employee Payroll, Timekeeping & Leave	2	3	2	2	3	4	2.65	Medium	FY2021			X	X
Employee Health Care Plan / Costs	2	3	3	2	4	4	2.95	Medium	FY2017				
Policy / Procedure - Development, Review, and Monitoring	1	3	3	2	2	1	2.00	Low	FY2017				X
Other Benefits	2	1	2	1	1	2	1.50	Low	-				
Employment Practices (Recruitment, onboarding, separations, etc.)	2	2	2	1	1	1	1.55	Low	-				
Information Governance	2	3	2	2	2	3	2.35	Medium					
Records Management / Imaging	2	4	3	3	3	4	3.15	Medium	-				X

Exhibit 2

SERS

2027 Risk Assessment - by Department

Auditable Area	A. Control Design and Effectiveness	B. Impact to Members, Retirees, Employers, Public, Reputation	C. Changes in Organization, Programs, Operations	D. Complexity of Activities, Operations, or Systems	E. Dollar Materiality/ Operational Impact	F. Impact of Fraud, Waste, or Data Loss	Combined Risk Rating	Risk Rating	Last Year Audited	Internal Audit Planned FY27 Coverage	FY27 Planned Hours	External Audit	Fiduciary Audit
Risk Factors	20%	20%	15%	15%	15%	15%	100%						
Investments													
Alternative Investments - Real Assets, Private Equity/Credit, Opportunistic	2	4	4	5	5	4	3.90	High	-			X	X
Investment Management Fees	2	4	3	4	4	3	3.30	Medium	-				X
Investment Governance & Management - SERS Investment Committee	2	4	3	4	4	3	3.30	Medium	FY2016				X
Fixed Income, US/Non-US Equity, Foreign Currency, Mutual Funds, Cash Equivalents	2	3	4	4	4	2	3.10	Medium	-			X	X
Investment Risk Management	2	4	3	4	3	3	3.15	Medium	-				X
Investment Due Diligence Review (Existing Investments)	2	4	3	4	2	3	3.00	Medium	-				X
Interest and Dividend Income	2	4	3	2	3	4	3.00	Medium	-			X	X
Capital Calls and Distributions	2	4	2	3	4	4	3.15	Medium	FY2021				
Securities Lending	2	2	3	3	2	3	2.45	Medium	-			X	
Investment Data Management / Maintenance / Retention	1	2	3	3	2	4	2.40	Medium	-				
Investor Owned ETFs	2	3	4	4	4	2	3.10	Medium	-	X	60		
Below are reviews performed each year													
Investment Incentive Compensation	2	3	3	3	2	3	2.65	Medium	FY2026	X	60		X
Conflicts of Interest (Investment Managers / Vendors)	1	3	2	2	2	3	2.15	Low	FY2026	X	60		X
Undue Influence Forms (certain SERS associates)	1	3	2	1	1	4	2.00	Low	FY2026	X	16		X
Member Services													
Retirement - Benefits / Calculations / Estimates	3	5	3	4	5	5	4.15	High	FY2020			X	
Member Withdrawals / Refunds & Lump Sum	3	4	4	4	5	5	4.10	High	FY2021			X	
Survivor - Benefits / Calculations	2	3	3	4	3	5	3.25	Medium	FY2024			X	
Member Account Maintenance	2	4	3	3	3	5	3.30	Medium	FY2022			X	
Disability - Benefits / Calculations	2	4	3	4	5	5	3.75	High	FY2023			X	
Required Minimum Distribution (RMD)	3	4	3	3	4	4	3.50	Medium	FY2026				
Death Benefits - SSN Matches/Proof of Life	2	4	3	3	3	4	3.15	Medium	FY2022				
MST / Online Chat	2	4	3	3	3	3	3.00	Medium	-	X (MST only)	120		X
Counseling	2	3	3	2	3	2	2.50	Medium					
Confidential Data Management (Member Services)	2	4	2	2	3	4	2.85	Medium	-				
Portability - Retirement System Transfers / Calculations	2	4	3	3	3	3	3.00	Medium	FY2016				
Member Statements	2	4	3	2	2	1	2.40	Medium	FY2024				
Service Purchase Credit / Calculation	3	3	3	2	1	4	2.70	Medium	FY2023				
Retirement - Application Process	2	4	3	3	2	2	2.70	Medium	-				
Member Self-Service Portal (MSS)	3	5	3	4	3	5	3.85	High	FY2026				
Reemployed Retirees / QEBA	2	3	2	4	1	3	2.50	Medium	-	X (QEBA)	80		

SERS				Risk Factors									
2027 Risk Assessment - by Department	**20%**	**20%**	**15%**	**15%**	**15%**	**15%**	**100%**						
Auditable Area	**A. Control Design and Effectiveness**	**B. Impact to Members, Retirees, Employers, Public, Reputation**	**C. Changes in Organization, Programs, Operations**	**D. Complexity of Activities, Operations, or Systems**	**E. Dollar Materiality/ Operational Impact**	**F. Impact of Fraud, Waste, or Data Loss**	**Combined Risk Rating**	**Risk Rating**	**Last Year Audited**	**Internal Audit Planned FY27 Coverage**	**FY27 Planned Hours**	**External Audit**	**Fiduciary Audit**
Information Technology													
Application Management - Software Management/SMART	3	5	3	4	5	5	4.15	High	FY2020				X
Identity and Access Management (IAM)	3	4	3	4	5	5	3.95	High	FY2024			X	X
Business Continuity / Disaster Recovery	3	4	3	3	5	3	3.50	Medium	FY2021				X
IT Vendor Management and transmission/retention of data	3	4	2	2	3	4	3.05	Medium	FY2019				X
Infrastructure	3	3	2	3	5	4	3.30	Medium	FY2025				X
Cloud Based Computing	3	3	4	3	4	4	3.45	Medium	FY2022				X
Mobile Device Security	3	3	2	3	3	4	3.00	Medium					X
IT Change Management	2	3	4	4	3	4	3.25	Medium	FY2017	X	160	X	X
Physical Access - IT General Controls	2	4	2	3	3	4	3.00	Medium	FY2016			X	X
Asset Management - Hardware	3	3	2	3	3	4	3.00	Medium	FY2019				X
IT Governance	3	4	3	2	2	2	2.75	Medium	FY2018				X
WCAG 2.0 AA compliance	2	3	3	3	4	4	3.10	Medium					
ERM													
Enterprise Risk Management - Information Security Program	2	5	3	4	5	5	3.95	High	FY2019			X	X
Enterprise Risk Management -Information Security Program (HIPAA Compliance)	2	3	3	3	4	4	3.10	Medium				X	
Enterprise Risk Management -Information Security Program (Fraud Program)	4	4	4	4	3	5	4.00	High				X	
Enterprise Risk Management - Vendor Risk Management	2	5	2	3	4	3	3.20	Medium					X
Enterprise Risk Management - Investment Compliance (part of Conflict of Interest)	4	4	4	4	3	3	3.70	Medium	FY2026	X (in addition to conflict of interest - investment compliance with Clearwater)	100		X
Enterprise Risk Management - BC/DR	2	4	3	3	5	3	3.30	Medium	FY2021				X
Enterprise Risk Management - Enterprise Risk Program	2	4	2	2	4	4	3.00	Medium					X
Enterprise Risk Management - Insurance	2	2	2	2	5	5	2.90	Medium					
Enterprise Risk Management - Artificial Intelligence Governance	3	3	3	3	2	3	2.85	Medium					

Exhibit 3

FY2027 Audit Plan Hours Summary

SERS
FY2027 Audit Plan Hours Summary

	Budget
Audits	
Continuous Auditing/Monitoring	200
Health Care Audits (Pharmacy/Medical Claims) (Outsourced)	20
Health Care Premiums	120
Experience Study	80
Member Service Team (MST)	120
Qualified Excess Benefit Arrangement (QEBA)	80
ETF Investments	60
IT Change Management	160
Investment Compliance with Clearwater	100
	940
Consulting	
Fiduciary audit	200
Health Care documentation	40
	240
Compliance	
Investment Incentive Compensation	60
Undue Influence	16
Conflict of Interest	60
	136
Total project-related time	1,316
Advisory/Other	
Disaster Recovery Plan	10
ORSC Annual Audit Report	20
FY28 Audit Planning	80
Open audit recommendations	40
Audit Committee meeting preparation	80
SLT/Director/other meetings	300
	530
Vacation/Holidays/Training	234
Total Budgeted Audit Hours:	**2,080**