The Metropolitan Water District of Southern California

Agenda

The mission of the Metropolitan Water District of Southern California is to provide its service area with adequate and reliable supplies of high-quality water to meet present and future needs in an environmentally and economically responsible way.

Audit Committee
M. Ramos, Chair
R. Crane, Vice Chair
D. De Jesus
L. Fong-Sakai
G. Gray, Emeritus

Audit Committee - Final

Meeting with Board of Directors *

March 9, 2026

2:00 p.m.

Monday, March 9, 2026 Meeting Schedule
09:00 a.m. EOT
11:00 a.m. LEG
12:30 p.m. BREAK
01:00 p.m. OPE
02:00 p.m. AUDIT
03:30 p.m. OWA

Written public comments received by 3:00 p.m. the business day before the meeting is scheduled will be posted under the Submitted Items and Responses tab available here: https://mwdh2o.legistar.com/Legislation.aspx.

The listen-only phone line is available at 1-877-853-5257; enter meeting ID: 873 4767 0235.

Members of the public may present their comments to the Board on matters within their jurisdiction as listed on the agenda teleconference and in-person. To provide public comment by teleconference dial 1-833-548-0276 and enter meeting ID: 876 9484 9772 or to join by computer click here.

Disclaimer: Written and oral public comments are received in compliance with the Ralph M. Brown Act. Please note that Metropolitan does not endorse or ensure the accuracy or reliability of the information provided as public comment or by third parties.

MWD Headquarters Building • 700 N. Alameda Street • Los Angeles, CA 90012
Teleconference Locations:
3008 W. 82nd Place • Inglewood, CA 90305
11973 Fuerte Drive • El Cajon, CA 92020

---

* The Metropolitan Water District's meeting of this Committee is noticed as a joint committee meeting with the Board of Directors for the purpose of compliance with the Brown Act. Members of the Board who are not assigned to this Committee may participate as members of the Board, whether or not a quorum of the Board is present. In order to preserve the function of the committee as advisory to the Board, members of the Board who are not assigned to this Committee will not vote on matters before this Committee.

US 2-145

1. Opportunity for members of the public to address the committee on matters within the committee's jurisdiction (As required by Gov. Code Section 54954.3(a))

2. MANAGEMENT ANNOUNCEMENTS AND HIGHLIGHTS

A. General Auditor's Quarterly Report **21-5463**

Attachments: 03092026 AUDIT 2A Report
03092026 AUDIT 2A Presentation

**** CONSENT CALENDAR ****

3. COMMITTEE ACTION (ONLY)

A. Approval of the Minutes of the Audit Committee for December 8, 2025 **21-5464**

Attachments: 03092026 AUDIT 3A (12082025) Minutes

4. COMMITTEE ITEMS (FOR BOARD CONSIDERATION)

NONE

**** END OF CONSENT CALENDAR ****

5. COMMITTEE ITEMS (ACTION FOR BOARD CONSIDERATION)

NONE

6. COMMITTEE ITEMS (INFORMATIONAL FOR BOARD CONSIDERATION)

NONE

7. COMMITTEE ITEMS (INFORMATIONAL)

a. Discussion on Cybersecurity Audit: Inventory & Control of Operational Technology Assets [Any discussion of threats to public services or facilities to be heard in closed session; conference with Keith Nobriga, Group Manager, Integrated Operations Planning & Support Services, Tae Yun, Section Manager, Water Operations & Planning, and Scott Suzuki, General Auditor - may be heard in closed session pursuant to Government Code Section 54957(a)] **21-5470**

Attachments: 03092026 AUDIT 7a C-L

b. Independent Auditor Macias Gini & O'Connell, LLP's Report on the Single Audit **21-5520**

Attachments: 03092026 AUDIT 7b C-L
03092026 AUDIT 7b Presentation

c. Discussion on amendments to the Metropolitan Water District Administrative Code Section 6451 regarding the Audit Department Charter **21-5448**

Attachments: 03092026 AUDIT 7c C-L
03092026 AUDIT 7c Presentation

d. Discussion on the results of the Audit Department's internal Quality Assurance & Improvement Program for Fiscal Year 2024/25 **21-5521**

Attachments: 03092026 AUDIT 7d C-L
03092026 AUDIT 7d Presentation

e. Overview of the Institute of Internal Auditors' Three Lines Model **21-5467**

Attachments: 03092026 AUDIT 7e C-L
03092026 AUDIT 7e Presentation

f. Annual Internal Audit Plan and Risk & Control Discussion **21-5465**

Attachments: 03092026 AUDIT 7f C-L
03092026 AUDIT 7f Presentation

g. Study, advise, or recommend on Board member/Board committee audit assignment requests **21-5469**

Attachments: 03092026 AUDIT 7g C-L

8. FOLLOW-UP ITEMS

NONE

9. FUTURE AGENDA ITEMS

10. ADJOURNMENT

NOTE: This committee reviews items and makes a recommendation for final action to the full Board of Directors. Final action will be taken by the Board of Directors. Committee agendas may be obtained on Metropolitan's Web site https://mwdh2o.legistar.com/Calendar.aspx. This committee will not take any final action that is binding on the Board, even when a quorum of the Board is present.

Writings relating to open session agenda items distributed to Directors less than 72 hours prior to a regular meeting are available for public inspection at Metropolitan's Headquarters Building and on Metropolitan's Web site https://mwdh2o.legistar.com/Calendar.aspx.

Requests for a disability-related modification or accommodation, including auxiliary aids or services, in order to attend or participate in a meeting should be made to the Board Executive Secretary in advance of the meeting to ensure availability of the requested service or accommodation.

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Committee Item
INFORMATION

Audit Committee

3/9/2026 Committee Meeting

2A

Subject

General Auditor’s Quarterly Report

Executive Summary

This item presents Audit Department activities during the past quarter, including progress on the audit plan and copies of the final reports issued.

Applicable Policy

Metropolitan Water District Administrative Code Section 6451(d)(2): Audit Department Charter

Details & Background

General Auditor’s Quarterly Report

The first part of the report (**Attachment 1**) is provided in dashboard format and comprises these elements:

1. Status of audit plan projects
2. Audit plan hours, planned and actual
3. Audit plan project count, including additions and deletions
4. Areas current audits are covering
5. Internal audit resource statistics, including use of contractors and professional licensing and certification
6. Status of internal audit recommendations
7. External quality assessment status
8. Independence and objectivity impairments
9. Current fiscal year department budget performance
10. Key message points of interest

The second part of the report (**Attachment 2**) breaks down the Audit Plan by project type (audit, advisory, Board request) and by project status (planned, in progress, completed), and includes the project title.

Final Reports Issued From October 1, 2025, to December 31, 2025

1. **Cybersecurity Audit: Inventory & Control of Operational Technology Assets** issued December 17, 2025 (**Attachment 3**)
   - Audit's scope covered all Operational Technology hardware assets, including desktops, laptops, network devices, servers, and non-computing/IoT (Internet of Things) devices, that were supported by Control System Applications Services Team (CSAST) and physically connected to networks maintained by the Integrated Operations Planning & Support Services (IOPSS) Group as of June 30, 2025.
   - Audit's objective was to determine whether all hardware assets supported by CSAST and connected to the IOPSS networks are actively managed to determine the totality of assets that need to be monitored and protected.
   - Three (3) recommendations with the following ratings: one **Priority 2**, two **Priority 3**.
2. **First Follow-up Review: Check with Order** issued December 18, 2025 (**Attachment 4**)
   - Review's objective and scope were limited to management's corrective actions, as of June 30, 2025 (except as noted otherwise), resulting from our audit recommendations for the three (3) audit recommendations made and accepted in the original audit, Report on Review of Check with Order, Audit No. 20-1031, dated November 30, 2020 (less-than-satisfactory rating).
   - Status of the four (4) recommendations: one **Implemented**, two **In Process**, one **Closed**.

Attachment 1 – General Auditor's Quarterly Report FY 25-26 Q2

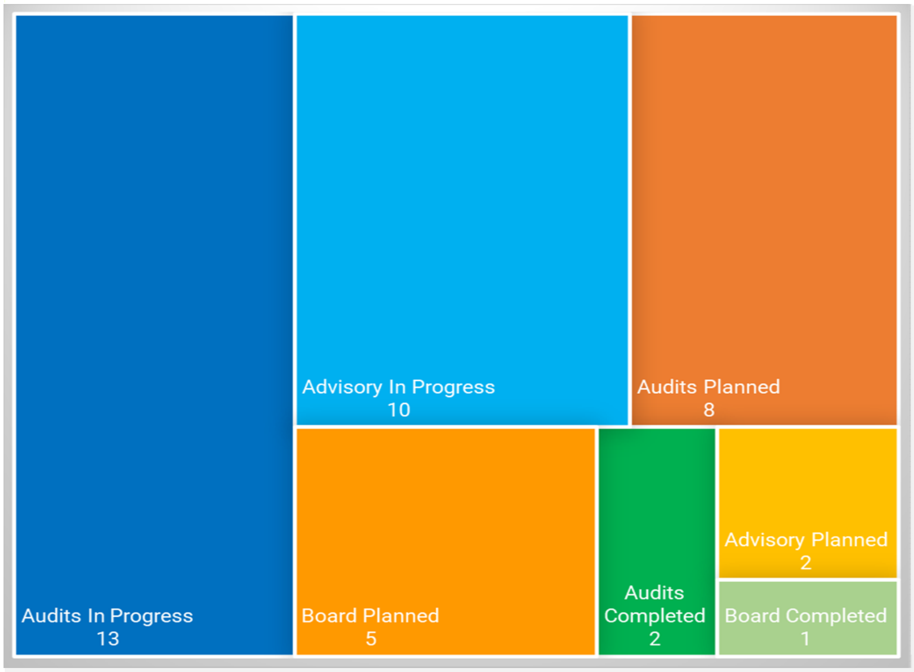
Attachment 2 – Audit Plan Status as of 2025-12-31

Attachment 3 – Inventory and Control of Operational Technology Assets (24-32) Public Information 2025-12-17

Attachment 4 – First Follow-up Review of Check with Order (20-1031) Final Report 2025-12-18

METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
OFFICE OF THE GENERAL AUDITOR
DASHBOARD AS OF DECEMBER 31, 2025

1 AUDIT PLAN STATUS - PROJECTS



2 AUDIT PLAN STATUS - HOURS

7/1/25 AUDIT PLAN	11,817
ADJUSTMENTS	1,040
ROLLING PLAN	12,857
ACTUAL HOURS	6,078
ESTIMATE TO COMPLETE	7,758
REQUIRED HOURS	13,836
HOURS AVAILABLE/(OVER)	(979)

3 AUDIT PLAN CHANGES

AUDIT PLAN PROJECTS - 10/1/25	41
ADDED Q2	
See key message points	-
DELETED Q2	
None	-
TOTAL	41

4 CURRENT ASSURANCE COVERAGE/WORK IN PROGRESS

Administrative Services	Cybersecurity
Bay Delta	IT
Centralized Grants & Research	Program Management (engineering)
Conveyance & Distribution	Water Resource Implementation

5 INTERNAL AUDIT RESOURCES

POSITIONS AUTHORIZED	14
VACANT	3
CONTRACTORS (INTERNAL AUDIT)	-
CERTIFIED PUBLIC ACCOUNTANTS	5
CERTIFIED INTERNAL AUDITORS	6
RESOURCE ADEQUACY	NO

6 OPEN RECOMMENDATIONS

	P1	P2	P3	OTHER	TOTAL
PRIOR FY	7	18	17	64	106
NEW	0	4	2	NA	6
RESOLVED	0	0	0	(4)	(4)
CURRENT	7	22	19	60	108

7 QUALITY ASSURANCE & IMPROVEMENT

EXTERNAL QUALITY ASSESSMENT	DUE 2028

8 IMPAIRMENTS

INDEPENDENCE	NONE
OBJECTIVITY	NONE

9 FISCAL BUDGET

	BUDGET	ACTUAL	FY BUDGET	VARIANCE	%
$	2,893,888	2,275,575	5,421,600	618,313	21%

10 KEY MESSAGE POINTS

Resource adequacy is RE vacant audit manager position; collaborating w HRS to fill
Follow-up reviews will confirm the status of open recommendations; management reports 81 of 108 have been implemented/closed

METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
OFFICE OF THE GENERAL AUDITOR
AUDIT PLAN STATUS AS OF DECEMBER 31, 2025

AUDITS	STATUS	TITLE
23	PLANNED 8	Contract Administration Program (4) Enterprise Risk Management (2) IT Governance (17) P-Card Program (3) Power Market Operations (7) Recruiting Process (5) Security Contract (1) State Audit Monitoring (8)
	IN PROGRESS 13	1CSR Bay Delta Disaster Preparedness (9) CLCA Contract Compliance (11) CRA Discharge Line Isolation Couplings Rehabilitation Project (15) CRA Maintenance (10) Cybersecurity: Inventory & Control of Operational Technology Software Assets (16) Operations Audit: Sole Source Contracts (6) Oracle Enterprise Business Suite Security (20) PlanNet Consulting Project Controls & Reporting System (PCRS) Pure Water State Funding Audit (12) Real Property Business Management System (14) Resource Experts
	COMPLETED 2	Cybersecurity: Inventory & Control of IT Software Assets (19) Cybersecurity: Inventory & Control of Operational Technology Assets (18)

ADVISORY	STATUS	TITLE
12	PLANNED 2	Governance Risk Compliance (GRC) Platform (22) Safety Equipment Purchase Process (21)
	IN PROGRESS 10	Board Expense Policy Deepfake Identity Awareness and Response Enterprise Content Management System (26) Grants (23) METCON (24) Oracle Services Procurement (30) PeopleSoft Time & Labor Power Operations Risk Oversight Committee (29) Process Matters Efficiency Initiative (27) WINS (25)

BOARD REQUESTS	STATUS	TITLE
6	PLANNED 5	Affordability Conjunctive Use Knowledge Transfer MOUs - Third Parties Real Estate - Qualifications
	COMPLETED 1	Colorado River Water Users Association Review (28)

Office of the General Auditor

Cybersecurity Audit: Inventory & Control of Operational Technology Assets

Project Number: 24-32
December 17, 2025

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

PUBLIC INFORMATION

TABLE OF CONTENTS

PUBLIC INFORMATION

Executive Summary

BACKGROUND

The Center for Internet Security (CIS) is a community-driven nonprofit that has developed the CIS Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data. Its mission is "to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats." Organizations can implement the CIS Critical Security Controls (CIS Controls), a set of 18 controls with detailed safeguards, to improve their cybersecurity posture.

The first CIS control is for the inventory and control of enterprise assets and requires organizations to effectively manage all enterprise assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to determine the totality of assets that need to be monitored and protected within the enterprise.

WHAT WE DID

Our audit scope covered all OT hardware assets, including desktops, laptops, network devices, servers, and non-computing/IoT (Internet of Things) devices, that were supported by CSAST and physically connected to networks maintained by the IOPSS Group (IOPSS networks) as of June 30, 2025.

Our audit objective was to determine whether all hardware assets supported by CSAST and connected to the IOPSS networks are actively managed to determine the totality of assets that need to be monitored and protected.

WHAT WE CONCLUDED

[REDACTED]

WHAT WE RECOMMEND

[REDACTED]

Management agreed with our observations and recommendations.

Information has been removed from this Executive Summary as it contains an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and is for distribution or consideration in a closed session and not subject to the California Public Record Act pursuant to Government Code Section 7929.200.

NUMBER OF RECOMMENDATIONS

Count	Priority	Response time
0	PRIORITY 1	Response time: Immediate
1	PRIORITY 2	Response time: Within 90 days
2	PRIORITY 3	Response time: Within 180 days

PUBLIC INFORMATION

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Date: December 17, 2025

To: Audit Committee

From: Scott Suzuki, CPA, CIA, CISA, CFE, General Auditor

Subject: Cybersecurity Audit: Inventory & Control of Operational Technology Assets (Project Number 24-32)

We have completed a cybersecurity audit of inventory and control of Operational Technology assets for the Integrated Operations Planning & Support Services Technology Group (IOPSS).

Due to the sensitive nature of the critical infrastructure information, details of our observations and recommendations were shared with select members of the Board and management in a separate confidential report not subject to public release.

Supplemental information, including our scope and objectives, is included in Appendix A. Appendix B includes a description of our new recommendation priority rating system.

We appreciate the courtesies and cooperation provided by the IOPSS Group.

The results in this report will be summarized for inclusion in a status report to the Board. If you have any questions regarding our audit, please do not hesitate to contact me directly at 213.217.6528 or Assistant General Auditor Kathryn Andrus at 213.217.7213.

Attachments

cc: Board of Directors
General Manager
General Manager-Designate
General Counsel
Ethics Officer
Office of the General Manager Distribution
Assistant General Managers
External Affairs Distribution
Integrated Operations Planning & Support Services Group Manager
External Auditor

RESULTS

The Recognition, Results Overview, and Observations & Recommendations sections have been removed from this report as they contain an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and are for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.

EVALUATION OF MANAGEMENT'S RESPONSE

Internal Audit considers management's response appropriate to the recommendations.

AUDIT TEAM

Sherman Hung, CISA, Principal Auditor

PUBLIC INFORMATION

APPENDIX A: SUPPLEMENTAL INFORMATION

SCOPE & OBJECTIVES

Our audit scope covered all OT hardware assets, including desktops, laptops, network devices, servers, and non-computing/IoT (Internet of Things) devices, that were supported by CSAST and physically connected to networks maintained by the IOPSS Group as of June 30, 2025.

Our audit objective was to determine whether all hardware assets supported by CSAST and connected to IOPSS networks are actively managed to accurately know the totality of assets that need to be monitored and protected.

EXCLUSIONS

Our audit scope did not include: (1) software assets, (2) data, (3) hardware assets maintained by the Information Technology Group, (4) cloud-based servers, nor (5) servers on virtual machines.

PRIOR AUDIT COVERAGE

We completed the following audit with a similar scope: Cybersecurity Audit: Inventory & Control of IT Assets, Project Number 23-31, issued on March 26, 2025.

AUTHORITY

We performed this audit in accordance with the General Auditor's Internal Audit Plan for FY 2024/25 approved by the Board.

PROFESSIONAL INTERNAL AUDIT STANDARDS

Our audit was conducted in conformance with the Global Internal Audit Standards issued by the International Internal Audit Standards Board.

FOLLOW-UP REVIEWS

The Office of the General Auditor has implemented a new follow-up process to ensure management has effectively implemented corrective action related to our recommendations. Management is required to report recommendation implementation status to our office within six months following the issuance of this report, and a first follow-up review will occur shortly thereafter. All audit recommendations are expected to be implemented within a year of this report, and if necessary, a second follow-up review will occur approximately six months after issuance of the first follow-up review report. Any audit recommendations not implemented after the second follow-up review will be shared with the Board/Audit Committee at its next scheduled meeting.

INTERNAL CONTROL SYSTEM

An internal control system is a continuously operating and integrated component of Metropolitan's operations. Internal controls are implemented by the Metropolitan management and seek to provide reasonable (not absolute) assurance that Metropolitan's business objectives will be achieved. However, limitations are inherent in any internal control system, no matter how well designed, implemented, or operated. Because of these limitations, errors or irregularities may occur and may not be detected.

Specific examples of limitations include, but are not limited to, poor judgment, carelessness, management override, or collusion. Accordingly, our audit would not necessarily identify all internal control weaknesses or resultant conditions affecting operations, reporting, or compliance. Additionally, our audit covers a point in time and may not be representative of a future period due to changes within Metropolitan and/or external changes impacting Metropolitan.

METROPOLITAN'S RESPONSIBILITY FOR INTERNAL CONTROL

It is important to note that Metropolitan management is responsible for designing, implementing, and operating a system of internal control. The objectives of internal controls are to provide reasonable assurance as to the reliability and integrity of information; compliance with policies, plans, procedures, laws, and regulations; the safeguarding of assets; the economic and efficient use of resources; and the accomplishment of established goals and objectives. In fulfilling this responsibility, management judgment is required to assess the expected benefits and related costs of internal control policy and procedures and to assess whether those policies and procedures can be expected to achieve Metropolitan's operational, reporting, and compliance objectives.

PUBLIC INFORMATION

APPENDIX B: PRIORITY RATING DEFINITIONS

The Office of the General Auditor utilizes a priority rating system to provide management a measure of urgency in addressing the identified conditions and associated risks. We assess the significance of each observation identified during the audit using professional judgment and assign priority ratings to each recommendation using the criteria listed below. Factors taken into consideration in assessing the priority include the likelihood of a negative impact if not addressed, the significance of the potential impact, and how quickly a negative impact could occur.

PRIORITY	1	2	3
Definition	Observation is *serious* enough to warrant *immediate* corrective action. The condition may represent a serious financial, operational, or compliance risk. A priority 1 recommendation may result from a key control(s) being absent, not adequately designed, or not operating effectively.	Observation is of a *significant* nature and warrants *prompt* corrective action. It may represent a moderate financial, operational, or compliance risk. A priority 2 recommendation may result from a process or less critical control(s) not being adequate in design and/or not operating effectively on a consistent basis.	Observation involves an internal control issue or compliance lapse that can be corrected in the *timely* course of normal business. A priority 3 recommendation may result from a process or control that requires enhancement to better support Metropolitan's objectives and manage risk.
Response Time	Immediate	Within 90 Days of report issuance	Within 180 Days of report issuance

PUBLIC INFORMATION

APPENDIX C: MANAGEMENT'S RESPONSE

The Management Response has been removed from this report as it contains an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and is for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.

Office of the General Auditor

First Follow-up Review: Check with Order

Project Number: 20-1031
December 18, 2025

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

TABLE OF CONTENTS

Executive Summary

BACKGROUND

In November 2020, the Office of the General Auditor completed an original audit of the controls on initiating, authorizing, paying, and distributing accounts payable transactions classified as "Check with Order" (CWO). These transactions occur when an employee requests the return of a signed check for manual delivery to the payee or when a vendor asks to pick up their check directly from the treasury operation team. We also evaluated physical controls over access to the vault room and check stock. Finally, we evaluated the review and approval controls for compliance with sound segregation of duties practices.

The original audit report was issued with a less-than-satisfactory rating and four (4) recommendations regarding checks returned to requestors, reliance on checks, treasury vault access controls, and vendor master file maintenance. Management agreed with three (3) of the four (4) recommendations and partially agreed with one (1) of the recommendations.

In January 2024, management notified us that the three (3) agreed-to recommendations had been implemented, and the one (1) partially agreed-to recommendation had no action taken. Based on this, we initiated our follow-up review on the implemented recommendations.

WHAT WE DID

Our review objective and scope were limited to management's corrective actions resulting from our audit recommendations as of June 30, 2025 (except as noted otherwise) for the three (3) audit recommendations made and accepted in the original audit, Report on Review of Check with Order, Audit No. 20-1031, dated November 30, 2020.

WHAT WE CONCLUDED

Management has implemented one (1) recommendation, two (2) recommendations are in process, and one (1) recommendation has been closed.

RECOMMENDATION STATUS

1	2	0	1
IMPLEMENTED	IN PROCESS	NOT IMPLEMENTED	CLOSED

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Date: December 18, 2025

To: Audit Committee

From: Scott Suzuki, CPA, CIA, CISA, CFE, General Auditor

Subject: First Follow-up Review: Check with Order
(Project Number 20-1031)

This report presents the results of our first follow-up review of check with order as of June 30, 2025, original Audit No. 20-1031, dated November 30, 2020.

The follow-up review concluded that the Finance & Administration Group implemented one of the four recommendations, vendor master file maintenance. The recommendations regarding checks returned to requestors and treasury vault access are in process. The recommendation regarding reliance on checks has been closed, as management deemed the risk of using electronic transfers (i.e., ACH) greater than that of issuing checks.

During this follow-up review, we noted several ancillary opportunities for improvement, which have been communicated to management and are included under the Results section. We will conduct a second follow-up review approximately six months after the date of this report to review the implementation status of the two (2) remaining recommendations. We will not follow up on ancillary recommendations as part of the follow-up process, but they will be considered for inclusion in a future audit.

We appreciate the courtesies and cooperation provided by the Finance & Administration Group.

If you have any questions regarding our review, please do not hesitate to contact me directly at 213.217.6528 or Assistant General Auditor Kathryn Andrus at 213.217.7213.

Attachments

cc: Board of Directors
General Manager
General Manager-Designate
General Counsel
Ethics Officer
Office of the General Manager Distribution
Assistant General Managers
Finance & Administration Group Distribution
External Auditor

RESULTS

RECOMMENDATIONS & CURRENT STATUS

1 Checks Returned to Requestors

Checks to be hand-delivered should be returned to an individual other than the requestor.

Recommendation 1
Signed checks should be mailed directly to the payees. In circumstances where mailing is not feasible, someone other than the requestor, preferably a third-party service, should make the delivery. We recommend that the Chief Financial Officer and the Chief Administrative Officer work together to develop policies and procedures to reduce the utilization of checks with orders.

Returning signed checks (negotiable instruments) to the requestor increases the risk that those checks might be altered or delivered to an unauthorized party, placing unnecessary risk on Metropolitan and its employees.

Current Status
In Process.

On February 18, 2021, a district-wide memo was distributed by the Chief Financial Officer and Chief Administrative Officer implementing a revised process for requesting and handling Checks with Orders (CWOs), which took effect on March 1, 2021. The main policy enhancements were:

- Section Manager approval must be obtained (regardless of dollar value).
- Group Manager and Finance approval must be obtained when the check is returned to the requestor (regardless of dollar value).
- Requestor must include a note to the Buyer affirming that the vendor was contacted and will not accept a credit card (P-Card) or standard payment terms (Net 30 days).
- Requestor is to include a note to the Approver that provides a business justification explaining why a CWO is needed for payment.
- Urgent requests shall be labeled as urgent and indicated as such in the applicable iProcurement field.

First, we compared the utilization of checks requested for return during the original audit with those issued during our follow-up review, with the scope of each review covering one calendar year of activity. We noted a 93% decrease from 1,070 checks to 72 checks.

Second, we selected 15 checks requested for return issued between January 1 and December 31, 2023, and reviewed them against current policy.

We performed testing, including both those processed through the requisition process and those submitted directly to accounts payable for processing, and noted three (20%) checks were returned to requestors contrary to the new policy. Upon further review, we noted that these three checks returned to the requestor were for payments that did not utilize the requisition process.

Ancillary Opportunity for Improvement 1

During our review of the 15 checks requested for return issued between January 1 and December 31, 2023 and selected for testing, we also noted:

(1) Ten (67%) requests did not include a note to the Buyer that the Vendor will not accept P-Card or Standard Payment Terms (Net 30 days).

(2) Ten (67%) requests did not include a note to the Approver that provides a business justification explaining why a check requested for return was needed for payment.

(3) One (7%) check requested for return, with a change in the person picking up the check, did not have an email documenting the change. Additionally, this requirement was not included in the updated policy.

We recommend management:

(1) Incorporate into the revised process:

  a. The procedure for returning checks for payments not utilizing the requisition process.

  b. The email notification process to inform Treasury of changes to the person authorized to pick up the check requested for return.

(2) Ensure the person picking up the check is independent of the check request process.

(3) Provide training on the revised process to ensure all those involved in the requesting, processing, and receipt of requested checks returned understand the requirements and their responsibilities.

(4) Conduct periodic reviews to ensure adherence to the revised process and procedures.

2 Reliance on Checks

Organizations should use payment processes that reduce opportunities for fraud by leveraging electronic payments.

Recommendation 2

We noted Metropolitan's ongoing dependence upon printing accounts payable checks. Shifting to payment via Automated Clearing House (ACH) decreases the risk associated with altered or misappropriated checks. Additionally, ACH payments lower transaction costs, are operationally more efficient, and are environmentally friendly.

Reliance on printed checks increases the exposure to altered, counterfeit, or misappropriated checks, potentially resulting in financial loss.

Current Status

Closed.

Management partially agreed with the recommendation. Management determined that increasing ACH transactions is not viable at this time due to the lack of commercially available account validation tools and the increasing cyber risk associated with processing payments electronically. As management has assumed the risk of issuing checks over our recommendation of using electronic transfers (i.e., ACH), we consider this recommendation closed.

3 Treasury Vault Access

Staff duties and responsibilities should define the physical and logical vault access granted.

Recommendation 3

We recommend that the CFO organization maintain authority over access to the vault, evaluate physical access controls, and reconcile these settings against staff duties and responsibilities. We also recommend that management perform periodic access reviews. We understand that management has begun reviewing these procedures.

Failure to maintain access controls could result in unauthorized access to confidential financial systems.

Current Status

In Process.

Treasury has not assumed ultimate approval over all access to the vault. Treasury performed a review ancillary to a system upgrade in 2022 and indicated informal reviews had occurred annually. No further documented reviews could be provided.

Based on management's actions, we consider this recommendation still in process. Treasury should assume access control authority over the vault and should formalize reviews over all those with vault access to ensure that their duties and responsibilities necessitate access. To align the frequency of access reviews with best practice, Treasury should conduct the reviews more frequently than annually (e.g., semiannually).

Ancillary Opportunity for Improvement 2

During our review of the vault room access list, we noted an executive leader was granted access to the vault room due to their oversight of the Treasury function.

This presents a potential segregation of duties conflict, given the breadth of the executive leader's responsibilities in overseeing multiple interconnected functional areas. Access should be based on the principle of least privilege, which is to grant access to the fewest number of individuals and only at the level necessary to allow for the effective execution of an individual's job responsibilities.

We recommend removing the vault room access for the executive leader. If management deems the access as appropriate, we recommend implementing mitigating controls that allow for the timely monitoring of those accessing the vault.

4 Vendor Master File Maintenance

Adequately controlled, the master file ensures properly segregated duties, use of authorized vendors, accurate cash disbursements, and proper tax reporting.

Recommendation 4
We recommend management update the vendor master file and conduct periodic reviews.

Incomplete or outdated vendor records could result in erroneous payments and inaccurate or incomplete reporting.

Current Status
Implemented.

Per the Purchasing System Procedures for Updating Vendors or Suppliers in Oracle, the vendor master file is updated annually by inactivating vendors with no transactional activity within the last three years. Administrative Services Management provided Inactive Vendor Reports for 2021, 2022, and 2023, supporting the performance of periodic reviews. We compared Active Vendors as of January 2020 and March 2024, and noted that the number of vendors without a tax ID decreased by 74%, the number of active vendors decreased by 30%, and the number of vendors with missing addresses decreased by 29%.

Based on the actions taken by management, we consider this recommendation implemented.

AUDIT TEAM

Kathryn Andrus, CPA, CIA, Assistant General Auditor
Chris Gutierrez, CPA, CIA, Program Manager - Audit
Lina Tan, Principal Auditor

APPENDIX A: IMPLEMENTATION STATUS DEFINITIONS

Professional internal auditing standards require internal auditors to confirm that management has implemented internal audit recommendations. The Office of the General Auditor has established follow-up reviews as part of its service portfolio to assess the implementation status of each recommendation from original audits.

Management is required to report recommendation implementation status to our office within six months following the issuance of the original audit report, and a first follow-up review will occur shortly thereafter. All audit recommendations are expected to be implemented within one year of the original audit report. If necessary, a second follow-up review will occur approximately six months after issuing the first follow-up review report. Any audit recommendations not implemented after the second follow-up review will be shared with the Board/Audit Committee at its next meeting.

To facilitate our follow-up reviews, we developed a classification system that rates actions taken by management to implement our recommendations.

IMPLEMENTATION STATUS	
IMPLEMENTED	Management has fully implemented our recommendation, as verified by the follow-up review. No further follow-up is to occur.
IN PROCESS	Management has partially implemented our recommendation. Additional follow-up will occur upon implementation of the remaining actions.
NOT IMPLEMENTED	Management has yet to take action to implement our recommendation. Additional follow-up to occur.
CLOSED	The recommendation has not been implemented, and no further follow-up review will occur due to one of the following conditions: 1. Alternative Action Taken: Management took corrective action that differed from our recommendation. The corrective action sufficiently mitigates the risks associated with the recommendation. 2. No Longer Applicable: Circumstances have changed, and the observation/recommendation is no longer applicable. 3. Risk Assumed: Management has accepted the risk of not implementing or partially implementing our recommendation. The Board of Directors has been apprised of the status. 4. Other: Current status was discussed with the Board, and while our recommendation has been partially implemented, the Board requested no additional follow-up review.

Audit Committee

General Auditor's Quarterly Report

Item 2A

March 9, 2026

Presented by: Scott Suzuki

Item 2A
Audit Department Dashboard

Subject

General Auditor’s Quarterly Report

Purpose

Provide a focused view of the internal audit dashboard elements as of December 31, 2025 and a summarization of issued reports

1. Audit Plan Status – Projects

2. Audit Plan Status – Hours

2 AUDIT PLAN STATUS - HOURS	
7/1/25 AUDIT PLAN	11,817
ADJUSTMENTS	1,040
ROLLING PLAN	12,857
ACTUAL HOURS	6,078
ESTIMATE TO COMPLETE	7,758
REQUIRED HOURS	13,836
HOURS AVAILABLE/(OVER)	(979)

3. Audit Plan Changes

3 AUDIT PLAN CHANGES	
AUDIT PLAN PROJECTS - 10/1/25	**41**
ADDED Q2	
See key message points	-
DELETED Q2	
None	-
TOTAL	**41**

4. Current Assurance Coverage/Work in Progress

4 CURRENT ASSURANCE COVERAGE/WORK IN PROGRESS	
Administrative Services	Cybersecurity
Bay Delta	IT
Centralized Grants & Research	Program Management (engineering)
Conveyance & Distribution	Water Resource Implementation

5. Internal Audit Resources

5 INTERNAL AUDIT RESOURCES	
POSITIONS AUTHORIZED	14
VACANT	3
CONTRACTORS (INTERNAL AUDIT)	-
CERTIFIED PUBLIC ACCOUNTANTS	5
CERTIFIED INTERNAL AUDITORS	6
RESOURCE ADEQUACY	NO

6. Open Recommendations

6 OPEN RECOMMENDATIONS					
	P1	P2	P3	OTHER	TOTAL
PRIOR FY	7	18	17	64	106
NEW	0	4	2	NA	6
RESOLVED	0	0	0	(4)	(4)
CURRENT	7	22	19	60	108

7. Quality Assurance & Improvement

7 QUALITY ASSURANCE & IMPROVEMENT	
EXTERNAL QUALITY ASSESSMENT	DUE 2028

8. Impairments

8 IMPAIRMENTS	
INDEPENDENCE	NONE
OBJECTIVITY	NONE

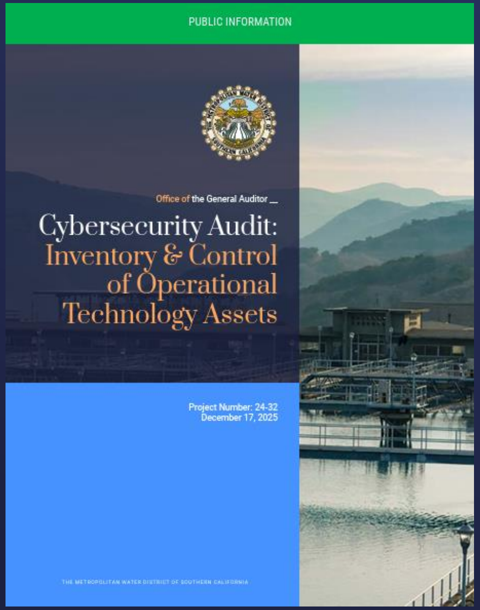
9. Fiscal Budget

9 FISCAL BUDGET					
	BUDGET	ACTUAL	FY BUDGET	VARIANCE	%
$	2,893,888	2,275,575	5,421,600	618,313	21%

10. Key Message Points

10 KEY MESSAGE POINTS
Resource adequacy is RE vacant audit manager position; collaborating w HRS to fill Follow-up reviews will confirm the status of open recommendations; management reports 81 of 108 have been implemented/closed

Final Reports Issued

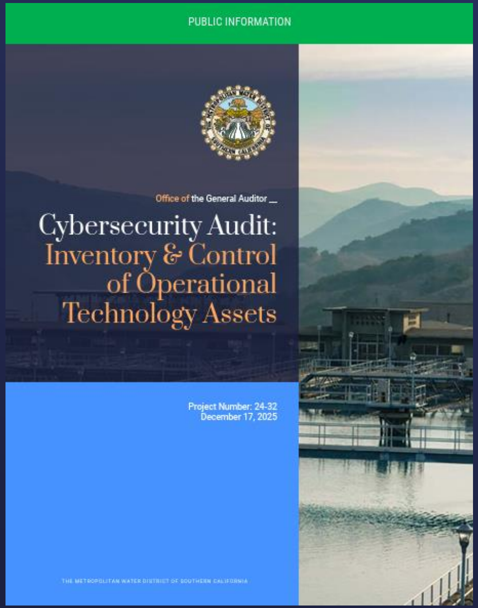


1. Cybersecurity Audit: Inventory & Control of Operational Technology Assets

Background

- Center for Internet Security
- Critical Security Controls

Final Reports Issued



1. Cybersecurity Audit: Inventory & Control of Operational Technology Assets (con't)

Objectives & Conclusions

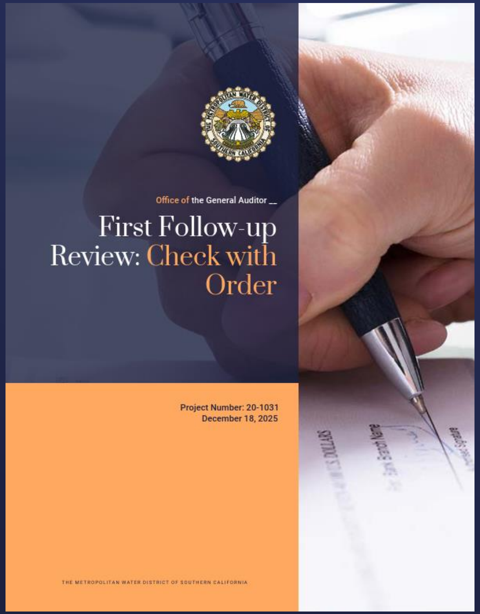
Determine whether specific hardware assets are actively managed to determine totality of assets.

Conclusions were provided in a separate confidential report.

Recommendations

One (1) Priority 2 recommendation and two (2) Priority 3 recommendations

Final Reports Issued



2. First Follow-up Review: Check with Order

Background

- Original report dated November 30, 2020
- Less-than-satisfactory rating, including four (4) recommendations

Conclusion

- One (1) recommendation Implemented, two (2) recommendations In Process, one (1) recommendation Closed

General Auditor's Quarterly Report

Questions?

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

1928

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

MINUTES

Audit Committee

December 8, 2025

Chair Armstrong called the meeting to order at 12:32 p.m.

Members present: Directors Armstrong, Fong-Sakai, and Ramos (teleconference posted location).

Members absent: Director De Jesus and Gray.

Other Board Members present: Directors Ackerman, Alvarez, Bryant, Cordero, Crane, Dennstedt, Erdman, Fellow, Garza, Jay, Katz, Kurtz, Lewitt, Miller, Ortega, Pressman, Seckel, and Shepherd Romey.

Committee Staff present: Andrus, Deshmukh, Elias, Hudson, Parsons, Rubin, Suzuki, and Upadhyay.

1. OPPORTUNITY FOR MEMBERS OF THE PUBLIC TO ADDRESS THE COMMITTEE ON MATTERS WITHIN THE COMMITTEE'S JURISDICTION

NONE

2. MANAGEMENT ANNOUNCEMENTS AND HIGHLIGHTS

A. Subject: General Auditor's Quarterly Report

Presented by: Scott Suzuki, General Auditor

Mr. Suzuki reported on the General Auditor's activities for the quarter ended September 30, 2025.

The following Directors asked questions and provided comments:

1. Armstrong
2. Garza
3. Ortega
4. Seckel

Staff responded to the Directors' questions and comments.

CONSENT CALENDAR

3. COMMITTEE ACTION (ONLY)

A. Subject: Approval of the Minutes of the Special Audit Committee for June 23, 2025, and September 23, 2025

Director Fong-Sakai made a motion, seconded by Director Armstrong, to approve the consent calendar for item 3A.

The vote was:

Ayes:	Directors Armstrong, Fong-Sakai, and Ramos
Noes:	None
Abstentions:	None
Absent:	Director De Jesus and Gray

The motion for item 3A passed by a vote of 3 ayes, 0 noes, 0 abstain, and 2 absent.

4. COMMITTEE ITEMS (FOR BOARD CONSIDERATION)

NONE

<u>END OF CONSENT CALENDAR ITEMS**</u>**

5. COMMITTEE ITEMS (ACTION FOR BOARD CONSIDERATION)

NONE

6. COMMITTEE ITEMS (INFORMATIONAL FOR BOARD CONSIDERATION)

NONE

7. COMMITTEE ITEMS

a. Subject: Discussion on Cybersecurity Audit: Inventory and Control of IT Assets [Any discussion of threats to public services or facilities to be heard in closed session; conference with Charles Eckstrom, Group Manager of Information Technology, Jacob Margolis, Director of Info Tech Services, and Scott Suzuki, General Auditor – may be heard in closed session pursuant to Gov. Code Section 54957(a)]

Presented by: Scott Suzuki, General Auditor

There were no questions or comments in the open session on Cybersecurity Audit: Inventory and Control of IT Assets.

No directors requested a closed session discussion on Cybersecurity Audit: Inventory and Control of IT Assets.

b. Subject: Discussion on Independent Auditor Macias Gini & O'Connell, LLP's Report for Fiscal Year 2024/25

Presented by: David Bullock, Partner at Macias Gini & O'Connell, LLP

Ms. Andrus introduced Mr. David Bullock, Partner at Macias Gini & O'Connell, LLP, who presented the Independent Auditor's Report for fiscal year 2024/25.

The following Director provided a comment:

1. Armstrong

c. Subject: Discussion on Digital Disruption

Presented by: Chris Gutierrez, Program Manager – Audit

Ms. Andrus introduced Mr. Chris Gutierrez, who presented on Digital Disruption.

The following Directors asked questions and provided comments:

1. Seckel
2. Ortega
3. Crane

Staff responded to the Directors' questions and comments.

d. Subject: Annual Audit Department Charter Review

Presented by: Kathryn Andrus, Assistant General Auditor

Ms. Andrus presented the Annual Audit Department Charter Review.

The following Directors asked questions and provided comments:

1. Ortega
2. Kurtz

Staff responded to the Directors' questions and comments.

e. Subject: Study, advise, or recommend on Board member/Board committee audit assignment requests

Presented by: Scott Suzuki, General Auditor

Mr. Suzuki introduced the item to study, advise, or recommend on Board member/Board committee audit assignment requests.

There were no questions or comments.

8. FOLLOW-UP ITEMS

NONE

9. FUTURE AGENDA ITEMS

Chair Armstrong requested a discussion on individual Board members' requests at the next meeting.

10. ADJOURNMENT

Meeting adjourned at 1:52 PM

Jeff Armstrong
Chair

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Committee Item
INFORMATION

Audit Committee

3/9/2026 Committee Meeting

7a

Subject

Discussion on Cybersecurity Audit: Inventory & Control of Operational Technology Assets [Any discussion of threats to public services or facilities to be heard in closed session; conference with Keith Nobriga, Group Manager, Integrated Operations Planning & Support Services, Tae Yun, Section Manager, Water Operations & Planning, and Scott Suzuki, General Auditor – may be heard in closed session pursuant to Gov. Code Section 54957(a)]

Executive Summary

This item will be called if sensitive information not released in the public version of this report is requested for discussion in closed session.

Details and Background

See Item 2a

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Committee Item
INFORMATION

Audit Committee

3/9/2026 Committee Meeting

7b

Subject

Independent Auditor Macias Gini & O'Connell, LLP's Report on the Single Audit

Executive Summary

This item will share information from the external auditor, hired to perform the Single Audit for fiscal year 2024/25. A Single Audit is required when the District expends $750,000 or more in aggregate federal monies within a fiscal year. In performing the Single Audit, the external auditor rendered unmodified opinions for both major programs and noted no control deficiencies or instances of noncompliance.

Applicable Policy

Metropolitan Water District Administrative Code Section 6450(e): Powers and Duties

Details and Background

The Single Audit is an audit of the entity's financial statements and internal controls over expenditures related to major federal program awards.

The purpose of the Single Audit is to verify compliance with federal regulations, evaluate the recipient's internal controls, and promote accountability.

The requirement for a Single Audit is triggered when grant recipients, in this case the District, expend $750,000 or more in aggregate federal financial assistance within their fiscal year. The $750,000 threshold increases to $1 million beginning with Metropolitan's fiscal year 2025/26. Single Audits must be performed by independent auditors in accordance with Government Auditing Standards.

Single Audits are comprised of two main sections:

- Financial Statements: An opinion on whether the financial statements are presented fairly in accordance with Government Auditing Standards.
- Programmatic Compliance Evaluation: An opinion on whether the entity complied with laws, regulations, and provisions of contracts or grant agreements that have a direct and material effect on a major federal program.

The Office of the General Auditor is the contract administrator for the four-year independent (external) auditor contract with Macias Gini & O'Connell, LLP, which is in place through fiscal year 2025/26. The contract is for the performance of the annual independent audit of Metropolitan's financial statements and the Single Audit, in years when the spending threshold of federal financial assistance is met.

Metropolitan's Administrative Code 6450(e) requires the General Auditor to transmit all reports issued by the District's external auditors to the Audit Committee, including any comments on the external auditor's reports that the General Auditor deems necessary.

Attachment 1 – The Metropolitan Water District of Southern California – Single Audit Reports – FYE 6.30.25

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Single Audit Reports

For the Fiscal Year Ended June 30, 2025

MGO. Certified Public Accountants

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Single Audit Reports
For the Fiscal Year Ended June 30, 2025

Table of Contents

MGO. | Certified Public Accountants

Independent Auditor's Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

The Board of Directors of
The Metropolitan Water District of Southern California

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards*), the financial statements of the business-type activities and fiduciary activities of the Metropolitan Water District of Southern California (Metropolitan), as of and for the fiscal year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise Metropolitan's basic financial statements, and have issued our report thereon dated November 4, 2025. Our report included an emphasis of matter paragraph for Metropolitan's adoption of Governmental Accounting Standards Board Statement No. 101, *Compensated Absences*.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered Metropolitan's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of Metropolitan's internal control. Accordingly, we do not express an opinion on the effectiveness of Metropolitan's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses or significant deficiencies may exist that were not identified.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether Metropolitan's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Macias Gini & O'Connell LLP

Los Angeles, California
November 4, 2025

mgo. | Certified Public Accountants

Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control Over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by the Uniform Guidance

The Board of Directors of
The Metropolitan Water District of Southern California

Report on Compliance for Each Major Federal Program

Opinion on Each Major Federal Program

We have audited the Metropolitan Water District of Southern California (Metropolitan) compliance with the types of compliance requirements identified as subject to audit in the *OMB Compliance Supplement* that could have a direct and material effect on each of Metropolitan's major federal programs for the fiscal year ended June 30, 2025. Metropolitan's major federal programs are identified in the summary of auditor's results section of the accompanying schedule of findings and questioned costs.

In our opinion, Metropolitan complied, in all material respects, with the compliance requirements referred to above that could have a direct and material effect on each of its major federal programs for the fiscal year ended June 30, 2025.

Basis for Opinion on Each Major Federal Program

We conducted our audit of compliance in accordance with auditing standards generally accepted in the United States of America (GAAS); the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards*); and the audit requirements of Title 2 U.S. *Code of Federal Regulations* Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). Our responsibilities under those standards and the Uniform Guidance are further described in the Auditor's Responsibilities for the Audit of Compliance section of our report.

We are required to be independent of Metropolitan and to meet our other ethical responsibilities, in accordance with relevant ethical requirements relating to our audit. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion on compliance for each major federal program. Our audit does not provide a legal determination of Metropolitan's compliance with the compliance requirements referred to above.

Responsibilities of Management for Compliance

Management is responsible for compliance with the requirements referred to above and for the design, implementation, and maintenance of effective internal control over compliance with the requirements of laws, statutes, regulations, rules and provisions of contracts or grant agreements applicable to Metropolitan's federal programs.

Auditor's Responsibilities for the Audit of Compliance

Our objectives are to obtain reasonable assurance about whether material noncompliance with the compliance requirements referred to above occurred, whether due to fraud or error, and express an opinion on Metropolitan's compliance based on our audit. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS, *Government Auditing Standards*, and the Uniform Guidance will always detect material noncompliance when it exists. The risk of not detecting material noncompliance resulting from fraud is higher than for that resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Noncompliance with the compliance requirements referred to above is considered material if there is a substantial likelihood that, individually or in the aggregate, it would influence the judgment made by a reasonable user of the report on compliance about Metropolitan's compliance with the requirements of each major federal program as a whole.

In performing an audit in accordance with GAAS, *Government Auditing Standards*, and the Uniform Guidance, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material noncompliance, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding Metropolitan's compliance with the compliance requirements referred to above and performing such other procedures as we considered necessary in the circumstances.
- Obtain an understanding of Metropolitan's internal control over compliance relevant to the audit in order to design audit procedures that are appropriate in the circumstances and to test and report on internal control over compliance in accordance with the Uniform Guidance, but not for the purpose of expressing an opinion on the effectiveness of Metropolitan's internal control over compliance. Accordingly, no such opinion is expressed.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and any significant deficiencies and material weaknesses in internal control over compliance that we identified during the audit.

Report on Internal Control Over Compliance

A *deficiency in internal control over compliance* exists when the design or operation of a control over compliance does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with a type of compliance requirement of a federal program on a timely basis. A *material weakness in internal control over compliance* is a deficiency, or a combination of deficiencies, in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency in internal control over compliance* is a deficiency, or a combination of deficiencies, in internal control over compliance with a type of compliance requirement of a federal program that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over compliance was for the limited purpose described in the Auditor's Responsibilities for the Audit of Compliance section above and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies in internal control over compliance. Given these limitations, during our audit we did not identify any deficiencies in internal control over compliance that we consider to be material weaknesses, as defined above. However, material weaknesses or significant deficiencies in internal control over compliance may exist that were not identified.

Our audit was not designed for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, no such opinion is expressed.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on the requirements of the Uniform Guidance. Accordingly, this report is not suitable for any other purpose.

Report on Schedule of Expenditures of Federal Awards Required by the Uniform Guidance

We have audited the financial statements of the business-type activities and fiduciary activities of Metropolitan, as of and for the fiscal year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise Metropolitan's basic financial statements. We issued our report thereon dated November 4, 2025, which contained unmodified opinions on those financial statements, and included an emphasis of matter paragraph for Metropolitan's adoption of Governmental Accounting Standards Board Statement No. 101, *Compensated Absences*. Our audit was conducted for the purpose of forming opinions on the financial statements that collectively comprise the basic financial statements. The accompanying schedule of expenditures of federal awards is presented for purposes of additional analysis as required by the Uniform Guidance and is not a required part of the basic financial statements. Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. The information has been subjected to the auditing procedures applied in the audit of the financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the schedule of expenditures of federal awards is fairly stated in all material respects in relation to the basic financial statements as a whole.

Macias Gini & O'Connell LLP

Los Angeles, California
January 23, 2026

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Schedule of Expenditures of Federal Awards

For the Fiscal Year Ended June 30, 2025

Federal Grantor/Pass-Through Entity/Program Title or Cluster	Assistance Listing Number (ALN)	Grant / Pass-Through Entity's Identifying Number	Federal Expenditures	Passed Through to Subrecipients
U.S. Department of Agriculture:				
Passed through Yorba Linda Water District				
Community Project Funding - Congressionally Directed Funding				
Helicopter Hydrant	10.723	AO-5305	$ 291,183	$ -
Total U.S. Department of Agriculture			291,183	-
U.S. Department of the Interior:				
Direct Programs				
Water Recycling and Desalination Construction Programs				
Pure Water Southern California - Large Scale	15.504	R25AP00229-1	19,990,373	4,168,545
Planning for Pure Water Southern California Program	15.504	R24AP00286-1	3,889,919	264,035
Assistance Listing Total			23,880,292	4,432,580
Direct Programs				
WaterSMART (Sustain and Manage America's Resources for Tomorrow)				
Regional Public Agency Turf Replacement Program	15.507	R22AP00505-2	275,241	-
Turf Replacement Incentive - Residential & Commercial	15.507	R23AP00426-1	998,362	-
Assistance Listing Total			1,273,603	-
Total U.S. Department of the Interior			25,153,895	4,432,580
U.S. Department of Homeland Security:				
Passed through California Governor's Office of Emergency Services (CalOES)				
Disaster Grants - Public Assistance (Presidentially Declared Disasters)	97.036	FEMA-4683-DR-CA037-91117	395,810	-
Hazard Mitigation Grant	97.039	FEMA-4569-DR-CA037-91117	27,641	-
Total U.S. Department of Homeland Sercurity			423,451	-
Total Expenditures of Federal Awards			**$ 25,868,529**	**$ 4,432,580**

See accompanying notes to the schedule of expenditures of federal awards.

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Notes to the Schedule of Expenditures of Federal Awards
For the Fiscal Year Ended June 30, 2025

NOTE 1 – GENERAL

The accompanying Schedule of Expenditures of Federal Awards (Schedule) presents the activity of all federal award programs of the Metropolitan Water District of Southern California (Metropolitan). The information in this Schedule is presented in accordance with the requirements of Title 2 U.S. *Code of Federal Regulations* Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). Metropolitan's reporting entity is defined in Note 1 in the notes to Metropolitan's basic financial statements.

NOTE 2 – BASIS OF ACCOUNTING AND PRESENTATION

Expenditures reported in the accompanying Schedule are presented using the accrual basis of accounting. Such expenditures are recognized following the cost principles contained in the Uniform Guidance, wherein certain types of expenditures are not allowable or are limited as to reimbursement. Pass-through entity identifying numbers are presented where applicable. Metropolitan did not elect to use the 10% de minimis cost rate as covered in 2 CFR Section 200.414 Indirect (Facilities & Administration) costs.

NOTE 3 – RELATIONSHIP TO BASIC FINANCIAL STATEMENTS

Expenditures of federal awards are reported in Metropolitan's basic financial statements as expenditures in the business-type activities. Federal award expenditures agree or can be reconciled with the amounts reported in Metropolitan's basic financial statements.

NOTE 4 – DIRECT AND PASS-THROUGH FEDERAL AWARDS

Federal awards may be granted directly to Metropolitan by a federal granting agency or may be granted to other government agencies which pass-through federal awards to Metropolitan. The Schedule includes both of these types of federal award programs when related expenditures are incurred.

NOTE 5 – U.S. DEPARTMENT OF THE INTERIOR – BUREAU OF RECLAMATION (USBR) – WATER RECYCLING AND DESALINATION CONSTRUCTION PROGRAMS (ALN 15.504)

Metropolitan incurred eligible pre-award costs associated with the USBR Water Recycling and Desalination Construction Programs grant during fiscal years 2020 through 2025. A total of $14,987,808 was claimed as allowable pre-award expenditures in accordance with the grant agreement provisions and are included in the total expenditures reported on the SEFA for fiscal year 2024-25.

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Notes to the Schedule of Expenditures of Federal Awards (Continued)
For the Fiscal Year Ended June 30, 2025

NOTE 5 – U.S. DEPARTMENT OF THE INTERIOR – BUREAU OF RECLAMATION (USBR) – WATER RECYCLING AND DESALINATION CONSTRUCTION PROGRAMS (ALN 15.504) - Continued

Period of Expenditure	R25AP00229	R24AP00286	Reported Pre-award Amount
FY2019-20	$ 207,357	$ —	$ 207,357
FY2020-21	682,908	—	682,908
FY2021-22	2,361,895	—	2,361,895
FY2022-23	4,332,086	—	4,332,086
FY2023-24	3,340,070	2,450,972	5,791,042
FY2024-25	1,612,520	—	1,612,520
Total Pre-award[1]	12,536,836	2,450,972	14,987,808
FY2024-25	7,453,537	1,438,947	8,892,484
Total Expenditures	$ 19,990,373	$ 3,889,919	$ 23,880,292

NOTE 6 – U.S. DEPARTMENT OF HOMELAND SECURITY – DISASTER GRANTS PUBLIC ASSISTANCE (ALN 97.036)

Metropolitan incurred eligible expenditures under the Federal Emergency Management Agency (FEMA) Disaster Grants – Public Assistance program during fiscal year 2022–23. In fiscal year 2024–25, the California Governor's Office of Emergency Services (CalOES) approved Metropolitan's Project Worksheet Nos. 477 and 964 under this program.

The total expenditures of $395,810 reported on the SEFA represent the eligible costs incurred and subsequently approved under these two project worksheets, as summarized below:

Project WS No.	Period of Expenditure	Amount Reported on SEFA
477	2022-23	$ 321,484
964	2023-24	74,326
		$ 395,810

[1] Per agreements, the pre-award periods are from April 3, 2020 through January 10, 2025, and from September 27, 2023 through May 20, 2024, for R25AP00229 and R24AP00286, respectively.

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Schedule of Findings and Questioned Costs
For the Fiscal Year Ended June 30, 2025

Section I – Summary of Auditor's Results

Financial Statements

Type of report the auditor issued on whether the financial statements audited were prepared in accordance with GAAP:	Unmodified
Internal control over financial reporting:	
• Material weakness(es) identified?	No
• Significant deficiency(ies) identified?	None reported
Noncompliance material to the financial statements noted?	No

Federal Awards

Internal control over major federal programs:	
• Material weakness(es) identified?	No
• Significant deficiency(ies) identified?	No
Type of auditor's report issued on compliance for the major federal programs:	Unmodified
Any audit findings disclosed that are required to be reported in accordance with 2 CFR 200.516(a)?	No

Identification of major federal programs:

Name of Federal Program or Cluster	Assistance Listing Number
Water Recycling and Desalination Construction Programs	15.504
WaterSMART (Sustain and Manage America's Resources for Tomorrow)	15.507

Dollar threshold used to distinguish between type A and type B programs:	$776,056
Auditee qualified as a low-risk auditee?	No

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Schedule of Findings and Questioned Costs (Continued)
For the Fiscal Year Ended June 30, 2025

Section II – Financial Statement Findings

No current year findings are reported.

Section III – Federal Award Findings and Questioned Costs

No current year findings are reported.

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA
Summary Schedule of Prior Audit Findings
For the Fiscal Year Ended June 30, 2025

There were no prior year audit findings.

Federal Awards (Single Audit) Results

Metropolitan Water District of Southern California

PRESENTED BY:

David Bullock
Partner
March 9, 2026

Metropolitan Water District of Southern California
Agenda

SECTION I
Single Audit Overview

SECTION II
Scope of the Audit

SECTION III
MGO Deliverables

SECTION IV
Audit Results

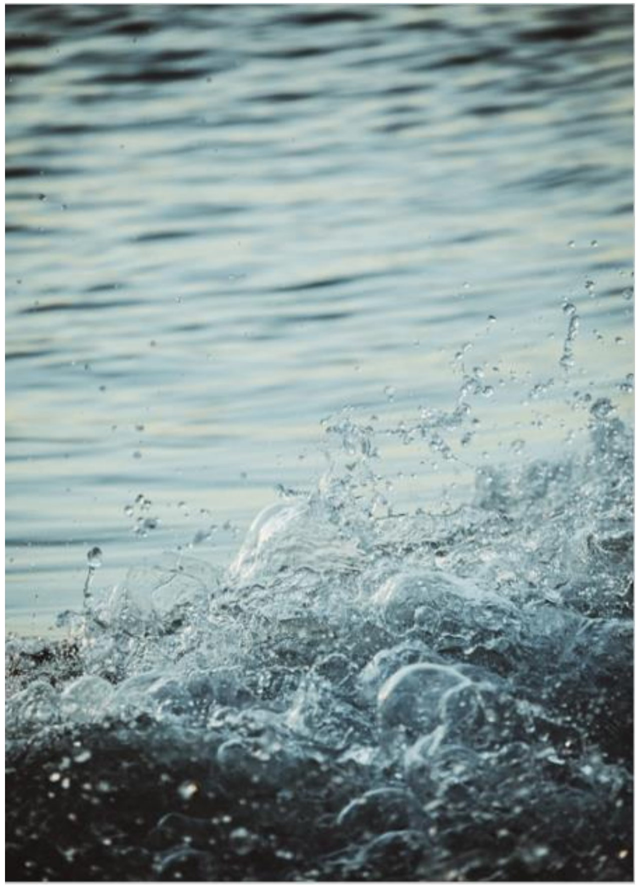
FISCAL YEAR 2024 – 2025 SINGLE AUDIT RESULTS

Single Audit Overview

Single Audit Overview

Single Audit under Uniform Guidance (2 CFR Part 200)

- Federal rules governing how organizations manage and spend federal awards
- Covers both financial management and compliance requirements
- Federal expenditures of $750,000 or more (FY 2025)
- Major program testing of federal grant compliance and internal controls over compliance
- Examples of key areas reviewed include internal controls, allowable costs, allowable activities, matching and reporting
- Schedule of Expenditures of Federal Awards (SEFA)



FISCAL YEAR 2024 – 2025 SINGLE AUDIT RESULTS

Scope of the Audit

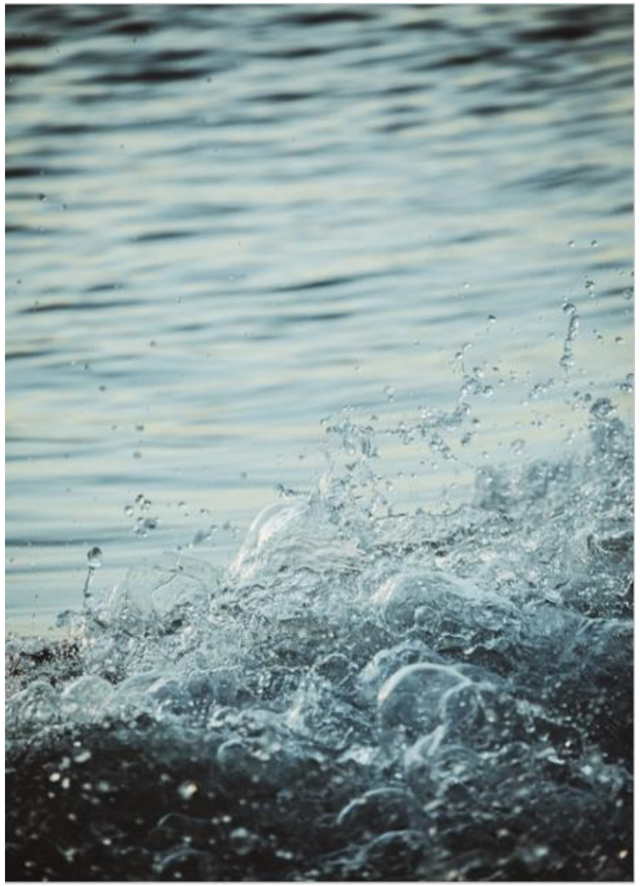
Scope of the Audit

Federal Compliance Audit (Uniform Guidance)

- Federal expenditures as presented in the Schedule of Expenditures of Federal Awards (SEFA) – page 6
- Notes to the SEFA – page 7
- Schedule of Findings and Questioned Costs – page 9

Federal Award Programs Audited (Major Programs)

- Water Recycling and Desalination Construction Programs (ALN #15.504)
- WaterSMART (Sustain and Manage America's Resources for Tomorrow) (ALN #15.507)



FISCAL YEAR 2024 – 2025 SINGLE AUDIT RESULTS

MGO Deliverables

MGO Deliverables

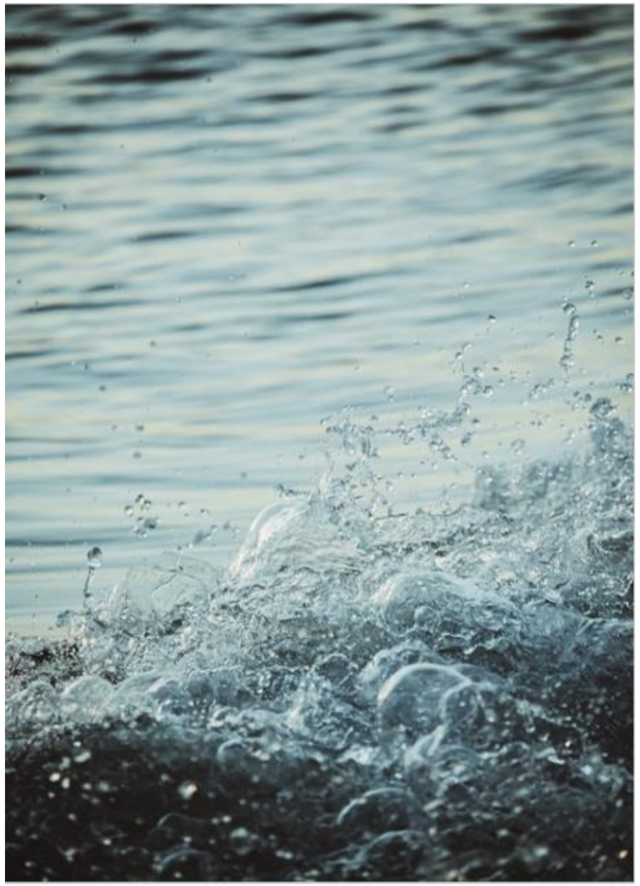
Single Audit Issued on January 23, 2026

- Independent Auditor's Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

- Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control Over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by the Uniform Guidance

Other Federal Compliance Submission

- Federal Audit Clearinghouse Data Collection Form
    - Completed



FISCAL YEAR 2024 – 2025 SINGLE AUDIT RESULTS

Audit Results

Audit Results

Financial Statement Audit Results (presented December 8, 2025)

- Reporting on Internal Controls:
    - No significant deficiencies
    - No material weaknesses

Single Audit Results

- Single Audit under the OMB Uniform Guidance:
    - Unmodified opinions rendered for both major programs
    - No control deficiencies
    - No instances of non-compliance

Questions?

mgocpa.com

Audit Committee

3/9/2026 Committee Meeting

7c

Subject

Discussion on amendments to the Metropolitan Water District Administrative Code Section 6451 regarding the Audit Department Charter

Executive Summary

This item will review proposed amendments to the General Auditor's portions of the Administrative Code that will update the Audit Department's Charter (Section 6451) to conform with new professional internal auditing standards and recommendations. While the proposed changes significantly revise the existing Charter/ Administrative Code, the changes mainly codify the Office of the General Auditor's existing practices and will require no additional resources.

Applicable Policy

Metropolitan Water District Administrative Code Section 6451: Audit Department Charter

Related Board Action(s)/Future Action(s)

Approval for the proposed amendments will be requested at the June 2026 Audit Committee and Board of Directors' meetings. Recommendations to update Administrative Code Section 2421 pertaining to the Audit Committee will be made at a future Audit Committee meeting.

Details & Background

Amendments to Section 6451 (Audit Department Charter)

The Institute of Internal Auditors (IIA), an organization that sets worldwide professional internal auditing standards that the General Auditor conforms to, released updated Standards (Global Internal Audit Standards), effective January 9, 2025.

Professional internal auditing standards require the chief audit executive (General Auditor) to develop and maintain an internal audit charter that, at a minimum, specifies:

(1) The Purpose of Internal Auditing;

(2) The internal audit function's commitment to adhering to the Global Internal Audit Standards;

(3) The internal audit function's mandate, including scope and types of services to be provided, and the Board's responsibilities and expectations regarding management's support of the internal audit function; and

(4) The internal audit function's organizational position and reporting relationships.

The IIA released a standards and guidance tool, Guide to Customizing the Model Internal Audit Charter for Public Sector Use, for public sector agencies to consider when updating their internal audit charters to conform with the Standards and best practices of internal audit functions.

The District's Audit Department Charter is contained within Metropolitan Water District Administrative Code Section 6451. An annual review of the Charter is required by Section 6451(e), and this was completed at the December 2025 Audit Committee meeting, where future action to update the Charter was discussed. Audit Department staff reviewed the charter against the tool and proposed amending Section 6451 as follows:

1. Subsection (a) Purpose
   - Rename and update internal audit's Purpose as prescribed in the Standards. This will replace the former mission, which the Audit Department will revise and release separately.
   - Move items previously described in the Scope of Work to the new Role subsection.
2. Subsection (b) Accountability
   - Add a reference to reporting significant issues related to risk management.
3. Subsection (c) Professional Standards
   - Update to conform to new Standard references (delete former Standard references).
   - Add requirements of Audit Department staff regarding unbiased mental attitude, impairment disclosure, professional objectivity, balanced assessment, and precautions to avoid conflicts of interest.
4. Subsection (d) Authority
   - Update to specify that the Audit Department's authority is created by its direct reporting relationship to the Board and the express authority granted to the Audit Department by the Board.
   - Add Audit Department access specifics (e.g., full and unrestricted; data, information), authority to issue communications, express prohibition on conducting services in areas over which internal audit has operational responsibility, time restrictions on auditing areas previously worked in, and a description of situations when the charter may require review and revision.
   - Move Authority from former subsection (e) to set the order of the remaining mandate Standard elements (e) Role and (f) Responsibilities.
   - Renumber subsections to avoid previous repetition of numbering.
5. Subsection (e) Role
   - Move content formerly in the Scope of Work to this new section in alignment with the Standards.
   - Clarify the role of the Audit Department.
   - Update the existing list of services with additional items covering operations/programs and process compliance.
   - Add a new section for the provision of advisory services.
6. Subsection (f) Responsibilities
   - Update to include clarifications to the existing list of responsibilities the General Auditor is responsible for ensuring the Audit Department carries out.
   - Add that the audit plan may be changed in response to changes in Metropolitan's business, risks, operations, programs, systems, and controls.
   - Add that recommendations not implemented by management and disagreements on audit recommendations are referred to the Audit Committee.

- Add assurance that the Audit Department collectively possesses or obtains the necessary knowledge, skills, and other competencies and qualifications.
- Expand on the requirements of the quality assurance and improvement program, including defining internal and external quality assessments, requirements, and reporting of results.
- Refine reporting on information items related to trends and emerging issues.
- Expand on coordination with other assurance and advisory providers.
- Add references to Standards conformance, ethical behavior, and reporting of behavior inconsistent with the District's ethical expectations.
- Add reporting of objectivity or independence issues.
- Add engagement conformance/compliance with Standards, laws, and regulations.
- Add resolution of conflicts between the Administrative Code, policy and procedures, and Standards.
- Add reference to confidentiality and safeguarding records and information.
- Add consideration of emerging trends and successful internal auditing practices.

7. Subsection (g) Independence
    - Add a new subsection that affirms the position of the Audit Department in the District.
    - Define functional reporting for the General Auditor to the Board and administrative reporting to the General Manager.
    - Explain that directly reporting to the Board provides the General Auditor organizational authority and status to bring matters directly to senior management and escalate matters to the Board.
    - Require annual reporting of organizational independence to the Board and disclosure to the Board of any interference encountered related to the scope, performance, or communication of internal audit work or results.
8. Subsection (h) Communications
    - Add a new subsection covering specific reporting required by the General Auditor to the Board and management.
    - Define specific communications to include: (1) the Audit Department mandate, (2) internal audit plan performance, (3) Audit Department budget, (4) significant change to the internal audit plan or budget, (5) impairments to independence, (6) quality assurance and improvement program results, (7) significant risks or control issues, (8) results of assurance or advisory services, (9) resource requirements, and (10) unacceptable acceptance of risk by management.

Attachment 1 – Metropolitan Water District Administrative Code Section 6451: Audit Department Charter (Redline)

Attachment 2 – Metropolitan Water District Administrative Code Section 6451: Audit Department Charter (Clean)

Division VI

PERSONNEL MATTERS

Chapter 4

OFFICERS

Article 4

GENERAL AUDITOR

§ **6451. Audit Department Charter.**

(a) Purpose – The purpose of the Audit Department is to strengthen Metropolitan's ability to create, protect, and sustain value by providing the Board of Directors and management with independent, risk-based, and objective assurance, advice, insight, and foresight. The Audit Department enhances Metropolitan's: successful achievement of its objectives; governance, risk management, and control processes; decision-making and oversight; reputation and credibility with its stakeholders; and ability to serve the public interest.~~Mission and Scope of Work - The mission of the Audit Department is to provide independent, professional, objective assurance and consulting services designed to add value and improve Metropolitan's operations. It helps the District accomplish its objectives by using a proactive, systematic approach to evaluate and improve the effectiveness of governance, risk management, and internal control. The scope of work of the Audit Department is to determine whether the District's network of governance, risk management, and internal control, as designed and represented by District management, is adequate and functioning in a manner to ensure:~~

~~(1) Risks are appropriately identified, managed and monitored;~~

~~(2) Significant financial, managerial and operating information is accurate, reliable and timely;~~

~~(3) Employees' actions are in compliance with policies, standards, procedures and applicable laws and regulations;~~

~~(4) Resources are acquired economically, used efficiently, and adequately protected;~~

~~(5) Programs, plans, and objectives are achieved;~~

~~(6) Quality and continuous improvement are fostered in the District's control process;~~

~~(7) Significant legislative or regulatory issues impacting the District are recognized and addressed appropriately; and~~

~~(8) Information technology is governed and systems and applications are securely deployed and monitored.~~

Metropolitan's Audit Department is most effective when: internal auditing is performed by competent professionals in conformance with The Institute of Internal Auditor's Global Internal Audit Standards (Standards), which are set in the public interest; the Audit Department is independently positioned with direct accountability to the Board of Directors; and internal auditors are free from undue influence and committed to making objective assessments.~~Opportunities for improving management internal control, efficiency and the District's image may be identified during audits. They will be communicated to the appropriate level of District management.~~

(b) Accountability – ~~–~~The General Auditor shall be accountable to the Board of Directors and the Audit Committee to:

(1) Advise on the adequacy and effectiveness of the District's processes for controlling its activities and managing its risks;

(2) Report significant issues related to the processes for controlling the activities of the District and managing its risks, including potential improvements to those processes, and provide information concerning such issues through to resolution; and

(3) Coordinate with other District control and monitoring functions (e.g., risk management, legal, finance, ethics, security, environmental).

(c) Professional Standards – The Audit Department shall govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements. ~~mandatory guidance, including the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*. This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the Audit Department's performance.~~ These documents constitute the operating procedures for the department and constitute an addendum to the charter. ~~The Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers shall also be adhered to as applicable.~~ In addition, Audit Department staff shall adhere to Metropolitan's policies and procedures, the California Government Code; and the Audit Department's Policies and Procedures Manual.

Internal auditors will:

(1) Maintain an unbiased mental attitude that allows them to perform engagements objectively such that they believe in their work product, do not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance.

(2) Disclose impairments of independence or objectivity, in fact or appearance, to appropriate parties and at least annually.

(3) Exhibit professional objectivity in gathering, evaluating, and communicating information.

(4) Make balanced assessments of all available and relevant facts and circumstances.

(5) Take necessary precautions to avoid conflicts of interest, bias, and undue influence.

(d) Authority – —The Audit Department's authority is created by its direct reporting relationship to the Board of Directors. Such authority allows for unrestricted access to the Board of Directors.

(1) The Board of Directors authorizes the General Auditor and Audit Department staff members to:

(i) Have full and unrestricted access to all functions, data, records, information, physical property, and personnel, pertinent to carrying out internal audit responsibilities, subject to the requirements of safekeeping, confidentiality, and applicable processes;

(ii) Have full and free access to the Audit Committee, subject to applicable law;

(iii) Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue communications to accomplish the function's objectives; and

(iv) Obtain the necessary assistance of District personnel, as well as other specialized services from within or outside the District to complete internal audit services.

(2) Internal auditors will have no direct operational responsibility or authority over any of the activities they review. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, or engage in other activities that may impair their judgment. Accordingly, the General Auditor and Audit Department staff are not authorized to:

(i) Perform any operational duties for the District or member agencies;

(ii) Initiate or approve transactions external to the Audit Department;

(iii) Direct the activities of any District employee not employed by the Audit Department, except to the extent such employees have been appropriately assigned to internal auditing teams or to otherwise assist the internal auditors; or

(iv) Assess specific operations for which they had responsibility within the previous year.

Circumstances may justify a follow-up discussion between the General Auditor, Board of Directors, and senior management on the internal audit mandate or other aspects of the internal audit charter. Such circumstances may include but are not limited to: a significant change in the Standards; a significant reorganization within the District; significant changes in the Direct Report Team, Board of Directors, and/or senior management; significant changes to the District's strategies, objectives, risk profile, or the environment in which the District operates; or new laws or regulations that may affect the nature and/or scope of internal audit services.

This Charter shall be reviewed at least annually by the Audit Committee and Board of Directors.

(e) Role – The primary role of the Audit Department is to conduct internal audit activities and deliver internal audit services. The scope of internal audit services covers the entire breadth of the District, including all of Metropolitan's activities, assets, and personnel. The scope of work of the Audit Department also encompasses, but is not limited to, objective examinations of evidence to provide independent assurance and advisory services to the Board of Directors and management to determine whether the District's network of governance, risk management, and internal control, as designed and represented by District management, is adequate and functioning in a manner to ensure:

(1) Risks related to the achievement of Metropolitan's strategic objectives are appropriately identified, managed and monitored;

(2) The integrity of information and the means used to identify, measure, analyze, classify, and report such information is reliable;

(3) Actions by Metropolitan's officers, directors, management, employees, contractors, or relevant parties are in compliance with Metropolitan's policies, procedures and applicable laws, regulations, and governance standards;

(4) Resources and assets are acquired economically, used efficiently and sustainably, and adequately protected;

(5) The results of operations and programs are consistent with established goals and objectives;

(6) Quality and continuous improvement are fostered in the District's control process;

(7) Significant legislative or regulatory issues impacting the District are recognized and addressed appropriately;

(8) Information technology is governed and systems and applications are securely deployed and monitored;

(9) Operations and programs are being carried out effectively, efficiently, ethically, and equitably; and

(10) Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact Metropolitan.

The nature and scope of advisory services may be agreed with by management requesting the service, provided the Audit Department does not assume management responsibility. Opportunities for improving the efficiency of governance, risk management, and internal control may be identified during advisory engagements, and will be communicated to the appropriate level of District management.

(~~d~~f) Responsibilities – ~~—~~The Audit Department shall carry out the following responsibilities:

(1) Develop and present a flexible annual audit plan to the Audit Committee and Board of Directors for review and approval. This plan should be developed utilizing a risk-based methodology and should include input and discussion on risks or internal control concerns identified by m~~M~~anagement or the Board of Directors. Review and adjust the internal audit plan, as necessary, in response to changes in Metropolitan's business, risks, operations, programs, systems, and controls;

(2) Report periodically to the Audit Committee and District management the status of the current year's audit plan and the ~~sufficiency of department~~ resources limitations on the audit plan. Communicate with the Audit Committee and senior management if there are significant interim changes to the internal audit plan;

(3) Submit audit reports to the Audit Committee and District management communicating the General Auditor's opinion regarding the internal control structure, identifying significant control issues, and providing related recommendations;

(4) Evaluate the ~~adequacy and timeliness~~ responsiveness of District management's responses to, and the corrective action taken on, all recommendations noted in ~~such~~ audit reports. Conduct follow-up reviews as necessary and periodically report to the Audit Committee and senior management the status of District management's progress. Referrals to the Audit Committee shall be made for recommendations not agreed to by management or determined to be not fully implemented upon secondary follow-up review;

(5) Ensure the selection, development and supervision of competent and professional audit staff. Ensure the Audit Department collectively possesses or obtains the

knowledge, skills, and other competencies and qualifications needed to meet the requirements of the Standards and fulfill the internal audit mandate;

(6) Develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the Audit Department.~~Perform a quality assurance program by which the General Auditor evaluates internal auditing activities against professional standards. Obtain an external quality assurance review as required by the Standards;~~

(i) The program will include external and internal assessments of the Audit Department's conformance with the Standards, as well as performance measurement to assess the Audit Department's progress toward the achievement of its objectives and promotion of continuous improvement. The program will also assess, if applicable, compliance with laws and/or regulations relevant to internal auditing. Also, if applicable, the assessment will include plans to address the Audit Department's deficiencies and opportunities for improvement.

(ii) Annually, the General Auditor will communicate with the Audit Committee and senior management about the Audit Department's quality assurance and improvement program, including the results of internal assessments (ongoing monitoring and periodic self-assessments) and external assessments. External assessments will be conducted at least once every five years by a qualified, independent assessor or assessment team from outside Metropolitan; qualifications must include at least one assessor holding an active Certified Internal Auditor credential.

(7) Perform advisory services to assist District management in meeting its objectives. Examples may include facilitation, process design, training, and assessment services;

(8) Evaluate additions or changes in internal control processes coincident with their development and implementation;

(9) Keep the Audit Committee and senior management informed as appropriate through information items of ~~significant emerging~~ trends and ~~best practices in internal auditing and governance~~emerging issues that could impact the District;

(10) Assist in the investigation of significant suspected fraudulent activities within the District. Assure reporting to the Audit Committee on the results, as appropriate; ~~and~~

(11) Coordinate activities and consider relying on the work of other internal and external providers of assurance and advisory services ~~with external auditors~~ to minimize duplication of effort. ~~and to e~~Ensure that significant issues raised as a result of their review~~,~~ are appropriately addressed. If the General Auditor cannot achieve an appropriate level of coordination, the issue must be communicated to senior management and, if necessary, escalated to the Audit Committee;

(12) Ensure that internal auditors:

(i) Conform with the Standards, including the principles of Ethics and Professionalism: integrity, objectivity, competency, due professional care, and confidentiality.

(ii) Understand, respect, meet, and contribute to the legitimate and ethical expectations of the District and be able to recognize conduct that is contrary to those expectations.

(iii) Encourage and promote an ethics-based culture in the District.

(iv) Report organizational behavior that is inconsistent with the District's ethical expectations, as described in applicable laws, regulations and policies and procedures.

(13) Ensure that the Audit Department remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. If the General Auditor determines that objectivity or independence may be impaired in fact or appearance, the details of the impairment, including the actions or safeguards employed to address the impairment, will be disclosed to the Audit Committee and/or management as appropriate.

(14) Ensure internal audit engagements are performed, documented, and communicated in accordance with the Standards and laws and/or regulations.

(15) Ensure adherence to Metropolitan's relevant policies and procedures unless such policies and procedures conflict with the internal audit charter or the Standards. Any such conflicts will be resolved or documented and communicated to the Audit Committee and senior management.

(16) Be accountable for confidentiality and safeguarding records and information; and

(17) Consider emerging trends and successful practices in internal auditing.

~~(e) Authority - The General Auditor and Audit Department staff members are authorized to:~~

~~(1) Have unrestricted access to all functions, records, property, and personnel, subject to the requirements of safekeeping, confidentiality, and applicable process;~~

~~(2) Have full and free access to the Audit Committee, subject to applicable law;~~

~~(3) Allocate resources, set frequencies, select the subject, determine scopes of work, and apply the techniques required to accomplish audit objectives; and~~

~~(4) Obtain the necessary assistance of personnel within units of the District where they perform audits, as well as other specialized services from within or outside the District.~~

~~The General Auditor and Audit Department staff are not authorized to:~~

~~(1) Perform any operational duties for the District;~~

~~(2) Initiate or approve accounting transactions external to the Audit Department; or~~

~~(3) Direct the activities of any District employee not employed by the Audit Department, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.~~

~~This Charter shall be reviewed at least annually by the Audit Committee and Board of Directors.~~

(g) Independence – The General Auditor will be positioned at a level in the District that enables internal audit services and responsibilities to be performed without interference from management, thereby establishing the independence of the Audit Department. The General Auditor will report functionally to the Board of Directors through the Audit Committee and administratively (e.g., board support, finance, human resources) to the General Manager. This positioning provides the organizational authority and status to bring matters directly to senior management and escalate matters to the Board of Directors, when necessary, without interference, and supports the internal auditors' ability to maintain objectivity.

(1) The General Auditor will confirm to the Audit Committee, at least annually, the organizational independence of the Audit Department. If the governance structure does not support organizational independence, the General Auditor will document the characteristics of the governance structure limiting independence and any safeguards employed to achieve the principle of independence.

(2) The General Auditor will disclose to the Audit Committee any interference internal auditors encounter related to the scope, performance, or communication of internal audit work and results. The disclosure will include communicating the implications of such interference on the Audit Department's effectiveness and ability to fulfill its mandate.

(h) Communications – The General Auditor will report periodically to the Audit Committee and senior management regarding:

(1) The Audit Department's mandate.

(2) The internal audit plan and performance relative to its plan.

(3) Internal audit budget.

(4) Significant revisions to the internal audit plan and budget.

(5) Potential impairments to independence, including relevant disclosures as applicable.

(6) Results from the quality assurance and improvement program, which include the Audit Department's conformance with the Standards and action plans to address the Audit Department's deficiencies and opportunities for improvement.

(7) Significant risk exposures and control issues, including fraud risks, governance issues, and other areas of focus for the Board of Directors that could interfere with the achievement of Metropolitan's strategic objectives.

(8) Results of assurance and advisory services.

(9) Resource requirements.

(10) Management's responses to risk that the Audit Department determines may be unacceptable or acceptance of a risk that is beyond Metropolitan's risk appetite.

Division VI

PERSONNEL MATTERS

Chapter 4

OFFICERS

Article 4

GENERAL AUDITOR

§ 6451. Audit Department Charter.

(a) Purpose – The purpose of the Audit Department is to strengthen Metropolitan's ability to create, protect, and sustain value by providing the Board of Directors and management with independent, risk-based, and objective assurance, advice, insight, and foresight. The Audit Department enhances Metropolitan's: successful achievement of its objectives; governance, risk management, and control processes; decision-making and oversight; reputation and credibility with its stakeholders; and ability to serve the public interest.

Metropolitan's Audit Department is most effective when: internal auditing is performed by competent professionals in conformance with The Institute of Internal Auditor's Global Internal Audit Standards (Standards), which are set in the public interest; the Audit Department is independently positioned with direct accountability to the Board of Directors; and internal auditors are free from undue influence and committed to making objective assessments.

(b) Accountability – The General Auditor shall be accountable to the Board of Directors and the Audit Committee to:

(1) Advise on the adequacy and effectiveness of the District's processes for controlling its activities and managing its risks;

(2) Report significant issues related to the processes for controlling the activities of the District and managing its risks, including potential improvements to those processes, and provide information concerning such issues through to resolution; and

(3) Coordinate with other District control and monitoring functions (e.g., risk management, legal, finance, ethics, security, environmental).

(c) Professional Standards – The Audit Department shall govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements. These documents constitute the operating procedures for the department and constitute an addendum to the charter. In addition, Audit Department staff shall adhere to Metropolitan's policies and procedures, the California Government Code; and the Audit Department's Policies and Procedures Manual.

Internal auditors will:

(1) Maintain an unbiased mental attitude that allows them to perform engagements objectively such that they believe in their work product, do not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance.

(2) Disclose impairments of independence or objectivity, in fact or appearance, to appropriate parties and at least annually.

(3) Exhibit professional objectivity in gathering, evaluating, and communicating information.

(4) Make balanced assessments of all available and relevant facts and circumstances.

(5) Take necessary precautions to avoid conflicts of interest, bias, and undue influence.

(d) Authority – The Audit Department's authority is created by its direct reporting relationship to the Board of Directors. Such authority allows for unrestricted access to the Board of Directors.

(1) The Board of Directors authorizes the General Auditor and Audit Department staff members to:

(i) Have full and unrestricted access to all functions, data, records, information, physical property, and personnel, pertinent to carrying out internal audit responsibilities, subject to the requirements of safekeeping, confidentiality, and applicable processes;

(ii) Have full and free access to the Audit Committee, subject to applicable law;

(iii) Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue communications to accomplish the function's objectives; and

(iv) Obtain the necessary assistance of District personnel, as well as other specialized services from within or outside the District to complete internal audit services.

(2) Internal auditors will have no direct operational responsibility or authority over any of the activities they review. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, or engage in other activities that may impair their judgment. Accordingly, the General Auditor and Audit Department staff are not authorized to:

(i) Perform any operational duties for the District or member agencies;

(ii) Initiate or approve transactions external to the Audit Department;

(iii) Direct the activities of any District employee not employed by the Audit Department, except to the extent such employees have been appropriately assigned to internal auditing teams or to otherwise assist the internal auditors; or

(iv) Assess specific operations for which they had responsibility within the previous year.

Circumstances may justify a follow-up discussion between the General Auditor, Board of Directors, and senior management on the internal audit mandate or other aspects of the internal audit charter. Such circumstances may include but are not limited to: a significant change in the Standards; a significant reorganization within the District; significant changes in the Direct Report Team, Board of Directors, and/or senior management; significant changes to the District's strategies, objectives, risk profile, or the environment in which the District operates; or new laws or regulations that may affect the nature and/or scope of internal audit services.

This Charter shall be reviewed at least annually by the Audit Committee and Board of Directors.

(e) Role – The primary role of the Audit Department is to conduct internal audit activities and deliver internal audit services. The scope of internal audit services covers the entire breadth of the District, including all of Metropolitan's activities, assets, and personnel. The scope of work of the Audit Department also encompasses but is not limited to objective examinations of evidence to provide independent assurance and advisory services to the Board of Directors and management to determine whether the District's network of governance, risk management, and internal control, as designed and represented by District management, is adequate and functioning in a manner to ensure:

(1) Risks related to the achievement of Metropolitan's strategic objectives are appropriately identified, managed and monitored;

(2) The integrity of information and the means used to identify, measure, analyze, classify, and report such information is reliable;

(3) Actions by Metropolitan's officers, directors, management, employees, contractors, or relevant parties are in compliance with Metropolitan's policies, procedures and applicable laws, regulations, and governance standards;

(4) Resources and assets are acquired economically, used efficiently and sustainably, and adequately protected;

(5) The results of operations and programs are consistent with established goals and objectives;

(6) Quality and continuous improvement are fostered in the District's control process;

(7) Significant legislative or regulatory issues impacting the District are recognized and addressed appropriately;

(8) Information technology is governed and systems and applications are securely deployed and monitored;

(9) Operations and programs are being carried out effectively, efficiently, ethically, and equitably; and

(10) Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact Metropolitan.

The nature and scope of advisory services may be agreed with management requesting the service, provided the Audit Department does not assume management responsibility. Opportunities for improving the efficiency of governance, risk management, and internal control may be identified during advisory engagements, and will be communicated to the appropriate level of District management.

(f) Responsibilities – The Audit Department shall carry out the following responsibilities:

(1) Develop and present a flexible annual audit plan to the Audit Committee and Board of Directors for review and approval. This plan should be developed utilizing a risk-based methodology and should include input and discussion on risks or internal control concerns identified by Management or the Board of Directors. Review and adjust the internal audit plan, as necessary, in response to changes in Metropolitan's business, risks, operations, programs, systems, and controls;

(2) Report periodically to the Audit Committee and District management the status of the current year's audit plan and the resource limitations on the audit plan. Communicate with the Audit Committee and senior management if there are significant interim changes to the internal audit plan;

(3) Submit audit reports to the Audit Committee and District management communicating the General Auditor's opinion regarding the internal control structure, identifying significant control issues, and providing related recommendations;

(4) Evaluate the responsiveness of District management's responses to, and the corrective action taken on, all recommendations noted in audit reports. Conduct follow-up reviews as necessary and periodically report to the Audit Committee and senior management the status of District management's progress. Referrals to the Audit Committee shall be made for recommendations not agreed to by management or determined to be not fully implemented upon secondary follow-up review;

(5) Ensure the selection, development and supervision of competent and professional audit staff. Ensure the Audit Department collectively possesses or obtains the knowledge, skills, and other competencies and qualifications needed to meet the requirements of the Standards and fulfill the internal audit mandate;

(6) Develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the Audit Department.

(i) The program will include external and internal assessments of the Audit Department's conformance with the Standards, as well as performance measurement to assess the Audit Department's progress toward the achievement of its objectives and promotion of continuous improvement. The program also will assess, if applicable, compliance with laws and/or regulations relevant to internal auditing. Also, if applicable, the assessment will include plans to address the Audit Department's deficiencies and opportunities for improvement.

(ii) Annually, the General Auditor will communicate with the Audit Committee and senior management about the Audit Department's quality assurance and improvement program, including the results of internal assessments (ongoing monitoring and periodic self-assessments) and external assessments. External assessments will be conducted at least once every five years by a qualified, independent assessor or assessment team from outside Metropolitan; qualifications must include at least one assessor holding an active Certified Internal Auditor credential.

(7) Perform advisory services to assist District management in meeting its objectives. Examples may include facilitation, process design, training, and assessment services;

(8) Evaluate additions or changes in internal control processes coincident with their development and implementation;

(9) Keep the Audit Committee and senior management informed as appropriate through information items of trends and emerging issues that could impact the District;

(10) Assist in the investigation of significant suspected fraudulent activities within the District. Assure reporting to the Audit Committee on the results, as appropriate;

(11) Coordinate activities and consider relying on the work of other internal and external providers of assurance and advisory services to minimize duplication of effort. Ensure that significant issues raised as a result of their review, are appropriately addressed. If the General Auditor cannot achieve an appropriate level of coordination, the issue must be communicated to senior management and if necessary escalated to the Audit Committee;

(12) Ensure that internal auditors:

(i) Conform with the Standards, including the principles of Ethics and Professionalism: integrity, objectivity, competency, due professional care, and confidentiality.

(ii) Understand, respect, meet, and contribute to the legitimate and ethical expectations of the District and be able to recognize conduct that is contrary to those expectations.

(iii) Encourage and promote an ethics-based culture in the District.

(iv) Report organizational behavior that is inconsistent with the District's ethical expectations, as described in applicable laws, regulations and policies and procedures.

(13) Ensure that the Audit Department remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. If the General Auditor determines that objectivity or independence may be impaired in fact or appearance, the details of the impairment, including the actions or safeguards employed to address the impairment, will be disclosed, to the Audit Committee and/or management as appropriate.

(14) Ensure internal audit engagements are performed, documented, and communicated in accordance with the Standards and laws and/or regulations.

(15) Ensure adherence to Metropolitan's relevant policies and procedures unless such policies and procedures conflict with the internal audit charter or the Standards. Any such conflicts will be resolved or documented and communicated to the Audit Committee and senior management.

(16) Be accountable for confidentiality and safeguarding records and information; and

(17) Consider emerging trends and successful practices in internal auditing.

(g) Independence – The General Auditor will be positioned at a level in the District that enables internal audit services and responsibilities to be performed without interference from management, thereby establishing the independence of the Audit Department. The General Auditor will report functionally to the Board of Directors through the Audit Committee and administratively (e.g., board support, finance, human resources) to the General Manager. This positioning provides the organizational authority and status to bring matters directly to senior management and escalate matters to the Board of Directors, when necessary, without interference and supports the internal auditors' ability to maintain objectivity.

(1) The General Auditor will confirm to the Audit Committee, at least annually, the organizational independence of the Audit Department. If the governance structure does not support organizational independence, the General Auditor will document the characteristics of the governance structure limiting independence and any safeguards employed to achieve the principle of independence.

(2) The General Auditor will disclose to the Audit Committee any interference internal auditors encounter related to the scope, performance, or communication of internal audit work and results. The disclosure will include communicating the implications of such interference on the Audit Department's effectiveness and ability to fulfill its mandate.

(h) Communications – The General Auditor will report periodically to the Audit Committee and senior management regarding:

(1) The Audit Department's mandate.

(2) The internal audit plan and performance relative to its plan.

(3) Internal audit budget.

(4) Significant revisions to the internal audit plan and budget.

(5) Potential impairments to independence, including relevant disclosures as applicable.

(6) Results from the quality assurance and improvement program, which include the Audit Department's conformance with the Standards and action plans to address the Audit Department's deficiencies and opportunities for improvement.

(7) Significant risk exposures and control issues, including fraud risks, governance issues, and other areas of focus for the Board of Directors that could interfere with the achievement of Metropolitan's strategic objectives.

(8) Results of assurance and advisory services.

(9) Resource requirements.

(10) Management's responses to risk that the Audit Department determines may be unacceptable or acceptance of a risk that is beyond Metropolitan's risk appetite.

Audit Committee

Audit Department Charter Revisions

Item 7c

March 9, 2026

Presented by: Scott Suzuki

Item 7c
Audit Department Charter Revisions

Subject
Discussion on amendments to the Metropolitan Water District Administrative Code Section 6451 regarding the Audit Department Charter

Purpose
Review proposed amendments to the Audit Department Charter

Next Steps
Approval will be requested for the amendments at the June 2026 Board/Audit Committee Meetings

Audit Department Charter Section 6451

The Institute of Internal Auditors

- Internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications
- Established in 1941
- Serves more than 200,000 members from more than 170 countries and territories (www.theiia.org)
- Sets the standards for the way internal auditing is practiced around the world

Professional Internal Audit Standards

Audit Department Charter Section 6451

Global Internal Audit Standards

- Effective January 2025
- Standard 6.2

Audit Department Charter Section 6451

Item Overview

- Significant revisions to Section 6451
- Codification of existing practices
- No additional resources required

Audit Department Charter Section 6451

Recommended Charter Updates

1. Subsection (a) Purpose
   - Rename subsection
   - Replace Mission with the Purpose of Internal Auditing
2. Subsection (b) Accountability
   - Minor update
3. Subsection (c) Professional Standards
   - Update to conform to new Standard references
   - Update internal auditor responsibilities to conform to the Standards

Audit Department Charter Section 6451

Recommended Charter Updates (con't)

4. Subsection (d) Authority
   - Move Authority to this section
   - Update to specify express authority granted by the Board
   - Clarify prohibited Audit Department activities

5. Subsection (e) Role
   - New section
   - Clarify existing Scope of Services
   - Add additional items

Audit Department Charter Section 6451

Recommended Charter Updates (con't)

6. <u>Subsection (f) Responsibilities</u>
   - Clarify the existing list
   - Add additional items

7. <u>Subsection (g) Independence</u>
   - New section
   - Affirm direct reporting relationship to the Board
   - Define the General Auditor's functional and administrative reporting

Audit Department Charter Section 6451

Recommended Charter Updates (con't)

8. Subsection (h) Communications
    - New section
    - Define specific instances requiring communication to the Board and management

Administrative Code

Future Updates

- Audit Committee (Section 242l)

Audit Department Charter Review

Questions?

Audit Committee

3/9/2026 Committee Meeting

7d

Subject

Discussion on the results of the Audit Department's internal Quality Assurance & Improvement Program for Fiscal Year 2024/25

Executive Summary

This item provides an overview of the results of our internal Quality Assessment & Improvement Program (QAIP) covering FY 2024/25, as well as the status of the compliance gaps and opportunities for improvement identified during the external quality assessment completed in 2023.

The purpose of the QAIP is to ensure that an internal audit function conforms with the International Standards for the Professional Practice of Internal Auditing. The QAIP is designed to evaluate audit efficiency and effectiveness, and foster continuous improvement. An external assessment is required every five years, with internal assessments conducted in the intervening years. The next external assessment is due in 2028.

Applicable Policy

Metropolitan Water District Administrative Code Section 6451(d)(6)

Details & Background

Standard 1300 of The Institute of Internal Auditors' Global Internal Audit Standards (Standards) requires the chief audit executive (General Auditor) to develop and maintain a QAIP that covers all areas of the internal audit activity. The QAIP assesses the internal audit function's governance, staff, management, and processes. This evaluation includes the review of departmental policies and procedures, the Internal Audit Charter, risk assessments, project work papers, and audit reports, as well as conducting surveys.

Based on the results of these periodic assessments, the General Auditor must develop plans to address instances of nonconformance with the Standards and opportunities for improvement, including a proposed timeline for actions. The General Auditor must also communicate the results of the assessments to the Board and senior management.

In our last external quality assessment, conducted in 2023, we received a "Generally Conforms" rating, the highest possible rating. This means we have policies, procedures, and a charter in place, and the performance and results of these areas were evaluated to be in conformance with the Standards.

QAIP Results for FY 2024/25

In conducting this assessment, the General Auditor utilized the Institute of Internal Auditors' surveys to obtain anonymous feedback from staff, management, and the Board of Directors. Management included all executive leadership and those connected with the audit reports issued during the year.

The General Auditor received responses from six staff, eight managers, and five board members. This year's participation level was slightly higher than last year's. The surveys received identified both positive feedback and opportunities for improvement. In addition to the survey data, the Audit Department evaluated its policies, procedures, and practices, as well as the progress made in the areas identified for improvement during the last external quality assessment. During the assessment period, the General Auditor made progress in the areas identified in 2023, and that progress continued in the current fiscal year.

Metropolitan's Administrative Code Section 6451(d)(6) requires the Audit Department to perform a quality assurance program by which the General Auditor evaluates internal auditing activities against professional standards and obtains an external quality assurance review as required by the Standards.

Audit Committee

Discussion on the results of the Audit Department's internal Quality Assurance & Improvement Program for Fiscal Year 2024/25

Item 7d

March 9, 2026

Presented by: Kathryn Andrus

Item 7d
Results of internal Quality Assurance & Improvement Program for FY 2024/25

Subject

Discussion on the results of the Audit Department's internal Quality Assurance & Improvement Program for Fiscal Year 2024/25

Purpose

- Share the FY 2024/25 internal quality assessment results
- Provide a status update on the compliance gaps and opportunities for improvement identified during the external quality assessment in 2023

QAIP
FY 24/25

Objective

Evaluate conformance to the Institute of Internal Auditors' (IIA) Standards

Scope

Audit Department efficiency and effectiveness in executing its mission, as set forth in the Charter.

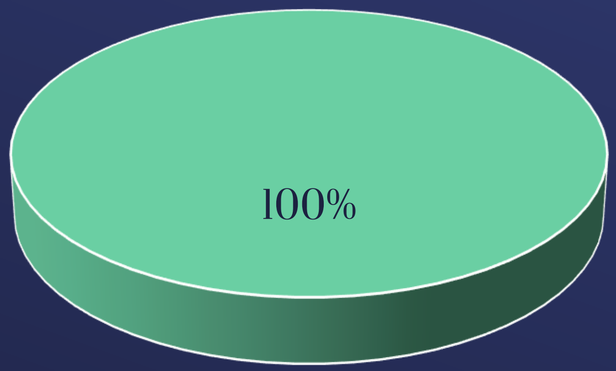
- Internal Audit Governance
- Internal Audit Staff
- Internal Audit Management
- Internal Audit Process

Internal Audit Governance

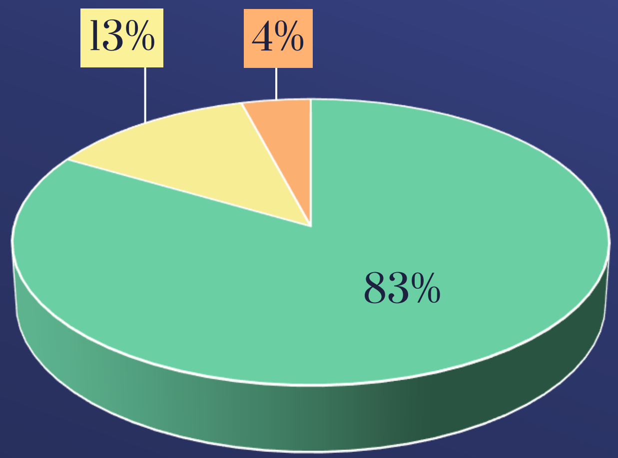
Key

Agree
Disagree
Don't Know

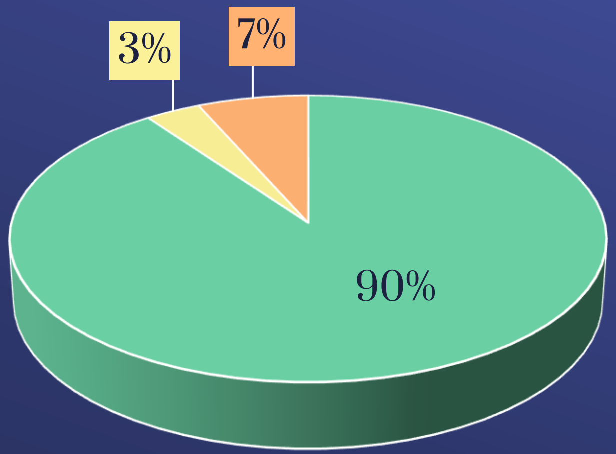
Staff



Management



Board



- Organizational value
- Conforms to the IIA's Standards/Principles and Rules of Conduct
- Unrestricted access to records
- Conflict-of-Interest policy/process

- Organizational value
- Information handling
- Professional objectivity
- Trusted advisor
- Unrestricted access to records
- Organizational independence

Survey Results: Feedback

Internal Audit Governance

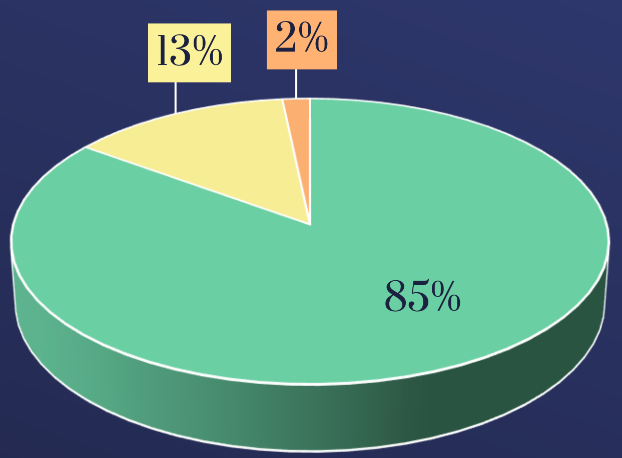
STRENGTHS	OPPORTUNITIES
• Value added • Professional • Integrity • Unrestricted access • Direct report to the Board	• Provide proactive District education – risks, controls, etc.

Internal Audit Staff

Key

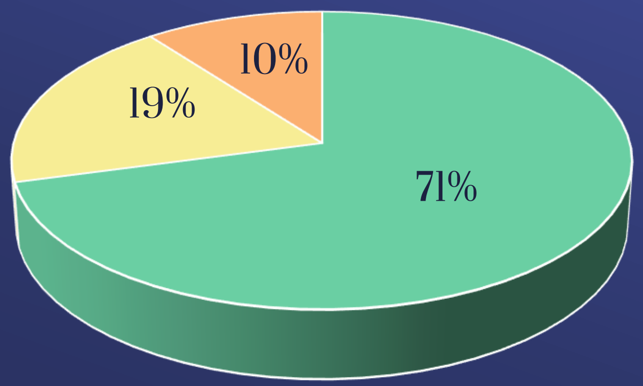
Agree
Disagree
Don't Know

Staff



- Skill/knowledge growth opportunities:
  - Develop professionally/advance career
  - Know key business processes
  - Encourage professional certifications
- Identification of "red flags"
- Performance reviews regular & constructive
- Department – development assignment
- Sufficient IT knowledge

Management



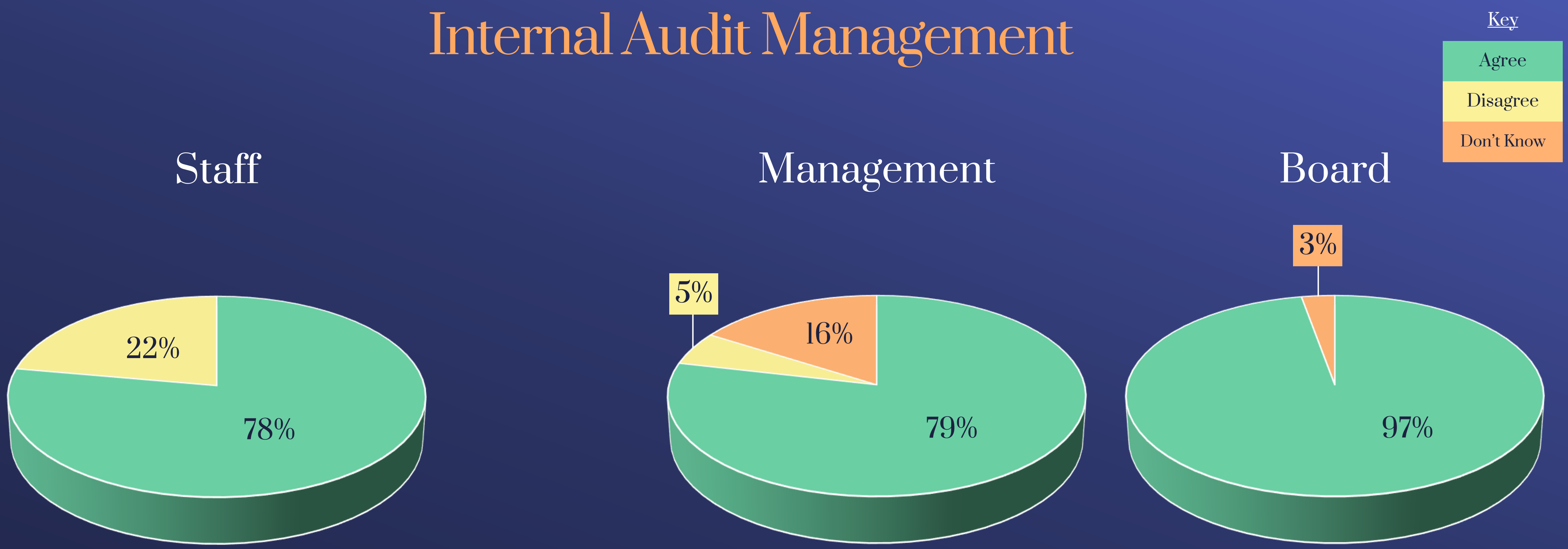
- Communicates effectively
- Keeps current – business/industry
- Adequate knowledge of key business processes
- Effective problem-identification/solution skills
- Effective conflict resolution/negotiation skills
- Viewed as a source of talent for the organization

Survey Results: Feedback

Internal Audit Staff

STRENGTHS	OPPORTUNITIES
• Communicates effectively • Is collaborative/approachable • Has knowledge of District business processes	• Proactive communication • Department career path strategy • Timeliness of management feedback to staff • Obtain training to improve efficiency/effectiveness

Internal Audit Management



- Department policies/procedures in place
- Encourages collaboration – management/staff
- Competently assesses District's:
    - Governance processes
    - Risk management processes
    - Internal controls
- Promotes organizational ethics/values

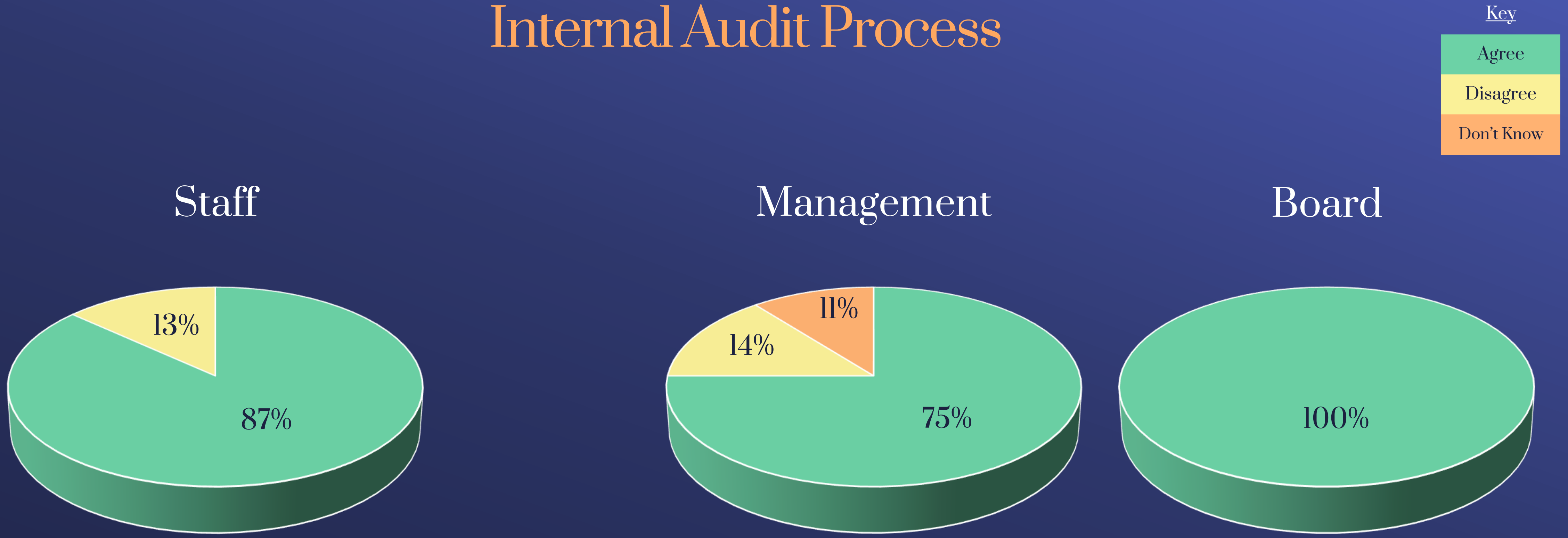
- Establishes risk-based audit plan
- Effectively communicates, including audit plan (scope/objectives)
- Adequately assesses risk management processes/system of internal controls
- Keeps current business/industry
- Promotes organizational ethics/values

Internal Audit Management

Survey Results: Feedback

STRENGTHS	OPPORTUNITIES
• Proactively communicates • Is collaborative/approachable • Uses a risk-based audit plan • Promotes District ethics/values • Provides status updates • Continue management/Board education efforts	• Fill open positions

Internal Audit Process



- Engagement objectives align with risks
- Employ data analytics
- Engagement feedback – timely/constructive
- Proficient project management
- Proficient organization skills
- Timely engagement completion
- Effective conflict/resolution skills

- Timely engagement completion
- Sufficient IT risks/controls knowledge
- Sufficient fraud knowledge
- Reporting – accurate, objective, clear, concise, constructive, and complete

Survey Results: Feedback

Internal Audit Process

STRENGTHS	OPPORTUNITIES
• Engagement planning – scope/objective vs. risks • Constructive feedback – engagement performance • Engagement reporting format/ content	• Increase engagement, completion timeliness & efficiency • Increase use of data analytics • Increase staff IT knowledge • Improve staff project management skills • Improve staff organizational skills • Evaluate District-level risk and governance processes

External Assessment Observations – Compliance Gaps

COMPLETED	IN PROCESS	NOT STARTED
Internal Assessment	Engagement Review	Ethics-Related Objectives, Programs, and Activities
External Assessment	Reporting Timelines	
Engagement Level Risk Assessments		
Final Engagement Communications		
Condition Causes		

External Assessment Observations – Improvement Opportunities

COMPLETED	IN PROCESS	NOT STARTED
IA Charter	Talent Management	Department Manual Update
	IT-Related Credentials	Key Performance Indicators
	Data Analytics	Enterprise Risk Framework
	Internal Audit Strategic Plan	
	District Fraud Investigations	
	Risk Reporting	

Quality Assurance & Improvement Program for FY 2024/25

Questions?

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

1928

Audit Committee

3/9/2026 Committee Meeting

7e

Subject

Overview of the Institute of Internal Auditors' Three Lines Model

Executive Summary

This item provides a general overview of the Three Lines Model (Model) published by the Institute of Internal Auditors (IIA). The Model is a principle-based framework that aligns governance (the Board), management, and independent assurance (e.g., Internal Audit) to improve organizational oversight, risk management, and performance. The framework is designed to provide an adaptable structure for risk management, internal control, and governance, including clarifying organizational roles at each line.

Applicable Policy

Metropolitan Water District Administrative Code Section 6451(d)(9)

Details and Background

This is an educational item. Education topics aim to inform Board members on contemporary subjects, including governance, risk management, internal controls, fraud, emerging threats, and other areas of interest.

Administrative Code Section 6451(d)(9) requires the General Auditor to keep the Audit Committee informed of significant emerging trends and best practices in internal auditing and governance.

Attachment 1 – The IIA's Three Lines Model

POSITION PAPER

The IIA's Three Lines Model

An Update of the Three Lines of Defense

The Institute of Internal Auditors

Contents

Introduction

Organizations are human undertakings operating in an increasingly uncertain, complex, interconnected, and volatile world. They often have multiple stakeholders with diverse, changeable, and sometimes competing interests. Stakeholders entrust organizational oversight to a governing body, which in turn delegates resources and authority to management to take appropriate actions, including managing risk.

For these reasons and more, organizations need effective structures and processes to enable the achievement of objectives while supporting strong governance and risk management. As the governing body receives reports from management on activities, outcomes, and forecasts, both the governing body and management rely on the internal audit function to provide independent, objective assurance and advisory services on all matters and to promote and facilitate innovation and improvement. The governing body is ultimately accountable for governance, which is achieved through the actions and behaviors of the governing body as well as management and internal audit.

The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.

Key terms

- organization – An organized group of activities, resources, and people working toward shared goals.
- stakeholder* – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers, vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.
- governing body – The highest-level body charged with governance, termed "board" in the Global Internal Audit Standards™. In an organization that has more than one governing body, board refers to the body/bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.
- management – Those individuals, teams, and support functions assigned to provide products and/or services to the organization's clients.
- internal auditing* – An independent, objective assurance and advisory service designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.
- internal audit function* – A professional individual or group responsible for providing an organization with assurance and advisory services.
- control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary.

The model applies to all organizations and is optimized by:

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of “defense” and protecting value.
- Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

Principles of the Three Lines Model

Principle 1: Governance

The governance of an organization requires appropriate structures and processes that enable:

- Accountability by a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- Actions (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.
- Assurance and advice by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

Principle 2: Governing body roles

The governing body ensures:

- Appropriate structures and processes are in place for effective governance.
- Organizational objectives and activities are aligned with the prioritized interests of stakeholders.

Key terms

- risk-based decision-making – A considered process that includes analysis, planning, action, monitoring, and review, and takes account of potential impacts of uncertainty on objectives.
- assurance* – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.
- governance* – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.
- advisory services* – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."
- assurance services* – Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational/performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary.

The governing body:

- Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.
- Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

Principle 3: Management and first and second line roles

Management's responsibility to achieve organizational objectives comprises both first and second line roles.[1] First line roles are most directly aligned with the delivery of products and/or services to clients of the organization and include the roles of support functions[2]. Second line roles assist with managing risk.

First and second line roles may be blended or separated. Some second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles. Second line roles can focus on specific objectives of risk management, such as: compliance with laws, regulations, and acceptable ethical behavior; controls; information and technology security; sustainability; and quality assurance. Alternatively, second line roles may span a broader responsibility for risk management, such as enterprise risk management (ERM). However, responsibility for managing risk remains a part of first line roles and within the scope of management.

Principle 4: Third line roles

The internal audit function provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.[3] It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

Principle 5: Third line independence

Internal audit's independence from the responsibilities of management is critical to its objectivity, authority, and credibility. It is established through accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

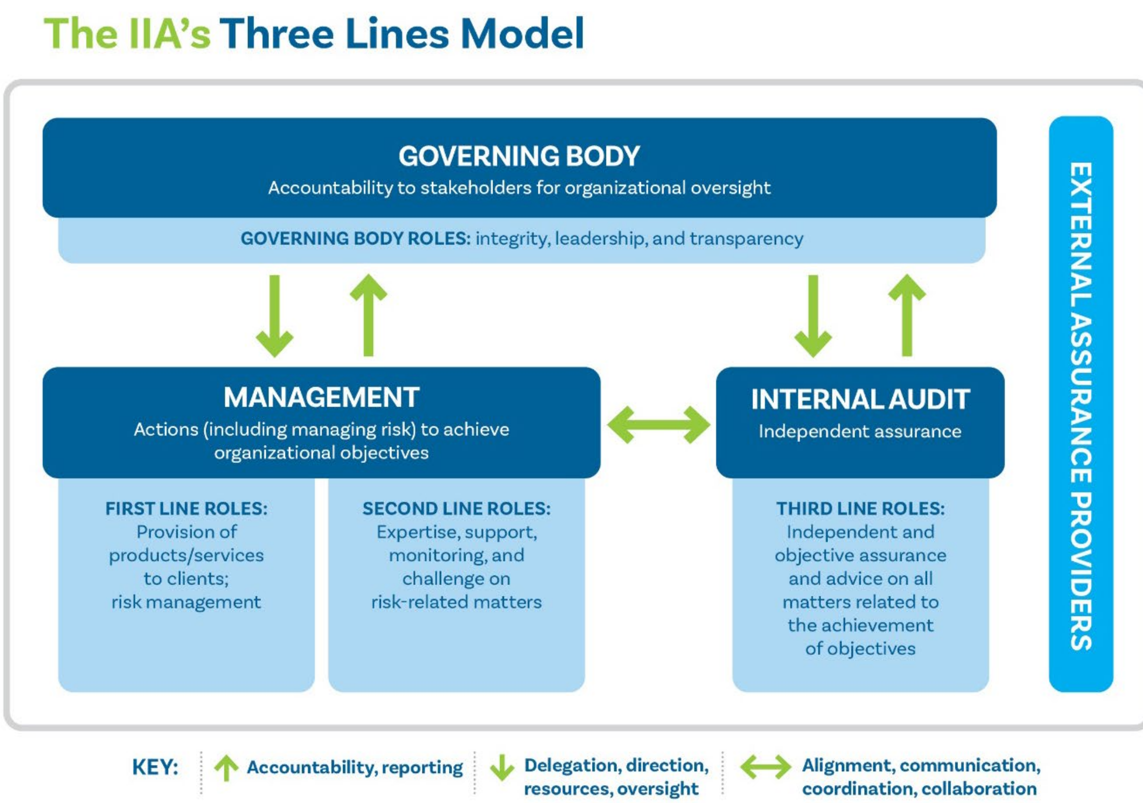
1. The language of "first line," "second line," and "third line" is retained from the original model in the interests of familiarity. However, the "lines" are not intended to denote structural elements but a useful differentiation in roles. Logically, governing body roles also constitute a "line" but this convention has not been adopted to avoid confusion. The numbering (first, second, third) should not be taken to imply sequential operations. Instead, all roles operate concurrently.

2. Some consider the roles of support functions (such as HR, administration, and building services) to be second line roles. For clarity, the Three Lines Model regards first line roles to include both "front of house" and "back office" activities, and second line roles to comprise those complementary activities focused on risk-related matters.

3. In some organizations, other third line roles are identified, such as oversight, inspection, investigation, evaluation, and remediation, which may be part of the internal audit function or operate separately.

Principle 6: Creating and protecting value

All roles working together collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritized interests of stakeholders. Alignment of activities is achieved through communication, cooperation, and collaboration. This ensures the reliability, coherence, and transparency of information needed for risk-based decision-making.



Key Roles in the Three Lines Model

Organizations differ considerably in their distribution of responsibilities. However, the following high-level roles serve to amplify the Principles of the Three Lines Model.

Governing body

- Accepts accountability to stakeholders for oversight of the organization.
- Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.
- Nurtures a culture promoting ethical behavior and accountability.
- Establishes structures and processes for governance, including auxiliary committees as required.
- Delegates responsibility and provides resources to management for achieving the objectives of the organization.
- Determines organizational appetite for risk and exercises oversight of risk management (including controls).
- Maintains oversight of compliance with legal, regulatory, and ethical expectations.
- Establishes and oversees an independent, objective, and competent internal audit function.

Management

First line roles

- Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization.
- Maintains a continuous dialogue with the governing body, and reports on planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including controls).
- Ensures compliance with legal, regulatory, and ethical expectations.

Second line roles

- Provides complementary expertise, support, monitoring, and challenge related to the management of risk, including:
    - The development, implementation, and continuous improvement of risk management practices (including controls) at a process, systems, and entity level.
    - The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior; controls; information and technology security; sustainability; and quality assurance.
- Provides analysis and reports on the adequacy and effectiveness of risk management (including controls).

Internal audit function

- Maintains primary accountability to the governing body and independence from the responsibilities of management.
- Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including controls) to support the achievement of organizational objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required.

External assurance providers

- Provide additional assurance to:
  - Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
  - Satisfy requests by management and the governing body to complement internal sources of assurance.

Relationships Among Core Roles

Between the governing body and management (both first and second line roles)

The governing body typically sets the direction of the organization by defining the vision, mission, values, and organizational appetite for risk. It then delegates responsibility for the achievement of the organization's objectives to management, along with the necessary resources. The governing body receives reports from management on planned, actual, and expected outcomes, as well as reports on risk and the management of risk.

Key term

chief executive officer (CEO) – The most senior individual in the organization with responsibility over operations.

Organizations vary as to the degree of overlap and separation between the roles of the governing body and management. The governing body can be more or less "hands on" with respect to strategic and operational matters. Either the governing body or management may take the lead in developing the strategic plan, or it may be a shared undertaking. In some jurisdictions, the CEO may be a member of the governing body and may even be its chair. In all cases, there needs to be strong communication between management and the governing body. The CEO is typically the focal point for this communication, but other senior managers may have frequent interactions with the governing body. Organizations may wish, and their regulators may require, leaders of second line roles such as a chief risk officer and a chief compliance officer to have a direct reporting line to the governing body. This is fully consistent with the Principles of the Three Lines Model.

Between management (both first and second line roles) and the internal audit function

Internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the carrying out of its work, enjoying unfettered access to the people, resources, and information it requires. It is accountable to the governing body. However, independence does not imply isolation. There must be regular interaction between the internal audit function and management to ensure internal audit work is relevant and aligned with the strategic and operational needs of the organization. Through all its activities, the internal audit function builds its knowledge and understanding of the organization, which contributes to the assurance and advisory services it delivers as a trusted advisor and strategic partner. There is a need for collaboration and communication across both the first and second line roles of management and the internal audit function to ensure there is no unnecessary duplication, overlap, or gaps.

Between the internal audit function and the governing body

The internal audit function is accountable to, and sometimes described as being the "eyes and ears" of, the governing body.

The governing body is responsible for oversight of internal audit, which requires: ensuring an independent internal audit function is established, including the hiring and firing of the chief audit executive; serving as the primary reporting line for the CAE;[4] approving and resourcing the audit plan; receiving and considering reports from the CAE; and enabling free access by the CAE to the governing body, including private sessions without the presence of management.

Key term

chief audit executive (CAE)* – The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

*Terms with asterisks come from the Global Internal Audit Standards™ glossary

Among all roles

The governing body, management, and the internal audit function have their distinct responsibilities, but all activities need to be aligned with the objectives of the organization. The basis for successful coherence is regular and effective coordination, collaboration, and communication.

4. For administrative purposes, the CAE may also report to an appropriately senior level of management.

Applying the Model

Structure, roles, and responsibilities

The Three Lines Model is most effective when it is adapted to align with the objectives and circumstances of the organization. How an organization is structured and how roles are assigned are matters for management and the governing body to determine. The governing body may establish committees to provide additional oversight for particular aspects of its responsibility, such as audit, risk, finance, planning, and compensation. Within management, there are likely to be functional and hierarchical arrangements and an increasing tendency toward specialization as organizations grow in size and complexity.

Functions, teams, and even individuals may have responsibilities that include both first and second line roles. However, direction and oversight of second line roles may be designed to secure a degree of independence from those with first line roles — and even from the most senior levels of management — by establishing primary accountability and reporting lines to the governing body. The Three Lines Model allows for as many reporting lines between management and the governing body as required. In some organizations, most notably regulated financial institutions, there is a statutory requirement for such arrangements to ensure sufficient independence. Even in these situations, those in management with first line roles remain responsible for managing risk.

Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk. Insofar as these provide support and challenge to those with first line roles and are integral to management decisions and actions, second line roles are part of management's responsibilities and are never fully independent from management, regardless of reporting lines and accountabilities.

A defining characteristic of third line roles is independence from management. The Principles of the Three Lines Model describe the importance and nature of internal audit independence, setting the internal audit function apart from other functions and enabling the distinctive value of its assurance and advisory services. The internal audit function's independence is safeguarded by not making decisions or taking actions that are part of management's responsibilities (including risk management) and by declining to provide assurance on activities for which the function has current, or has had recent, responsibility. For example, in some organizations, the CAE is asked to assume additional decision-making responsibilities over activities utilizing similar competencies, such as aspects of statutory compliance or ERM. In such circumstances, the internal audit function is not independent of these activities or of their results, and therefore, when the governing body seeks independent and objective assurance and advice relating to those areas, it is necessary for its provision to be undertaken by a qualified third party.

Oversight and assurance

The governing body relies on reports from management (comprising those with first and second line roles), internal audit, and others in order to exercise oversight and achievement of its objectives, for which it is accountable to stakeholders. Management provides valuable assurance (also referred to as attestations) on planned, actual, and forecast outcomes, on risk, and on risk management by drawing upon direct experience and expertise. Those with second line roles provide additional assurance on risk-related matters. Because of internal audit's independence from management, the assurance it provides carries the highest degree of objectivity and confidence beyond that which those with first and second line roles can provide to the governing body, irrespective of reporting lines. Further assurance may also be drawn from external providers.

Coordination and alignment

Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration, and communication. The governing body seeks confirmation through the internal audit function that governance structures and processes are appropriately designed and operating as intended.

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 245,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance.

For more information, visit theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Updated September 2024

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101

Audit Committee

Overview of the Institute of Internal Auditors' Three Lines Model

Item 7e

March 9, 2026

Presented by: Andrew Lin

Item 7e

Overview of the Three Lines Model

Subject

Overview of the Institute of Internal Auditors' Three Lines Model

Purpose

Provide an overview of the Three Lines Model, which helps organizations improve oversight, risk management, and performance.

Overview

What is the Three Lines Model?

- Risk, governance, and value
- Roles and accountability
- Collaboration

Three Lines Model

Core Principles and Key Roles

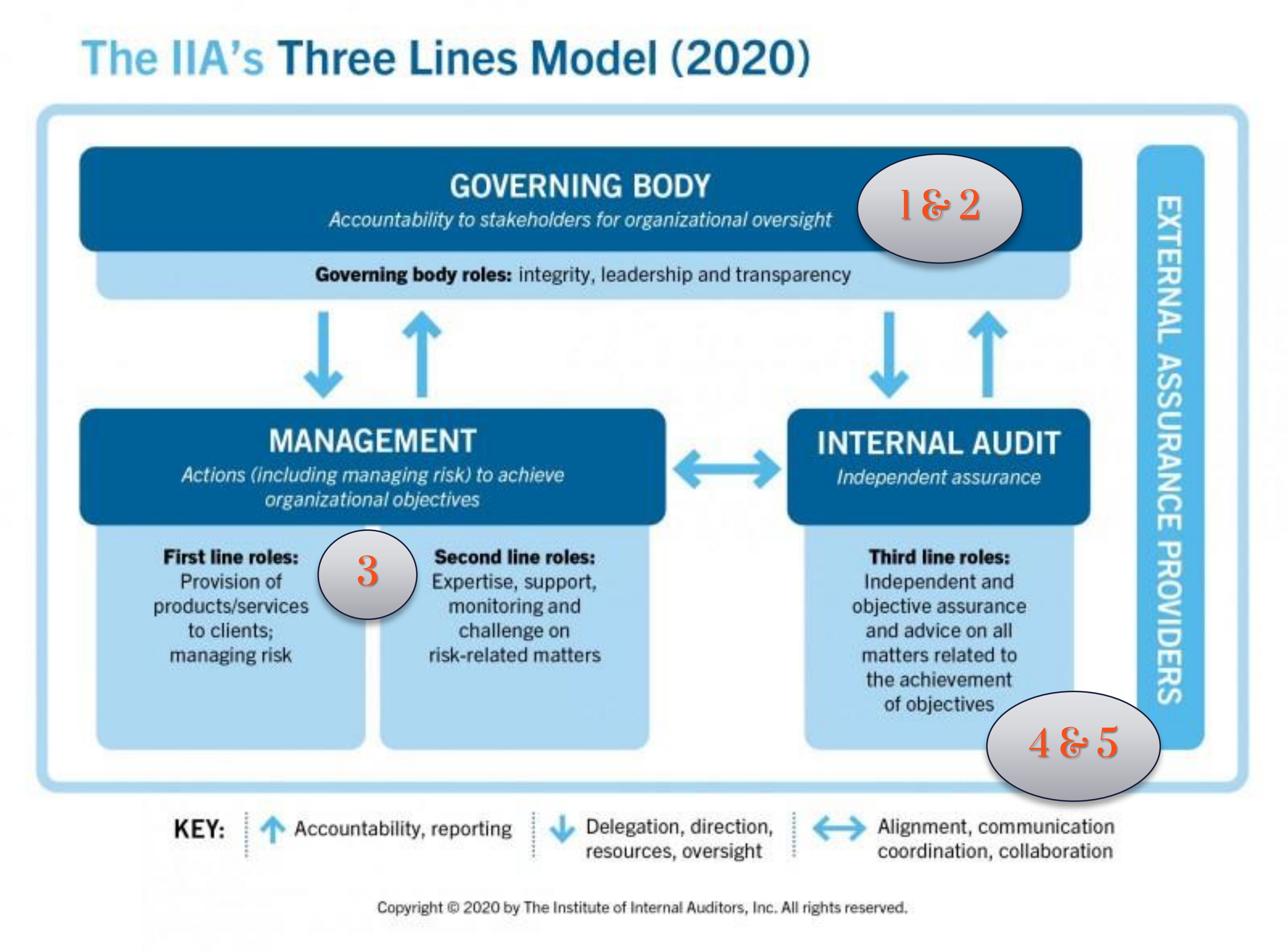
1. Governance
2. Governing Body Roles
3. Management Roles
4. Third Line Roles
5. Third Line Independence
6. Creating & Protecting Value

Governing Body

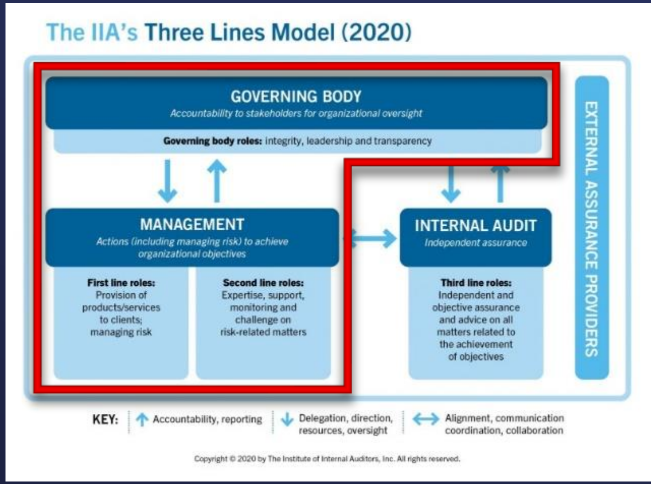
Management

Internal Audit

Source: The IIA's Three Lines Model


The IIA's Three Lines Model (2020)
GOVERNING BODY
Accountability to stakeholders for organizational oversight
1 & 2
Governing body roles: integrity, leadership and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
3
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
4 & 5
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration
Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

Three Lines Model



Source: The IIA's Three Lines Model

Key Roles and Relationships

GOVERNING BODY
Accountability to stakeholders for organizational oversight

GOVERNING BODY ROLES: integrity, leadership, and transparency

Direction
Responsibility & resources
Strategic planning
Communication

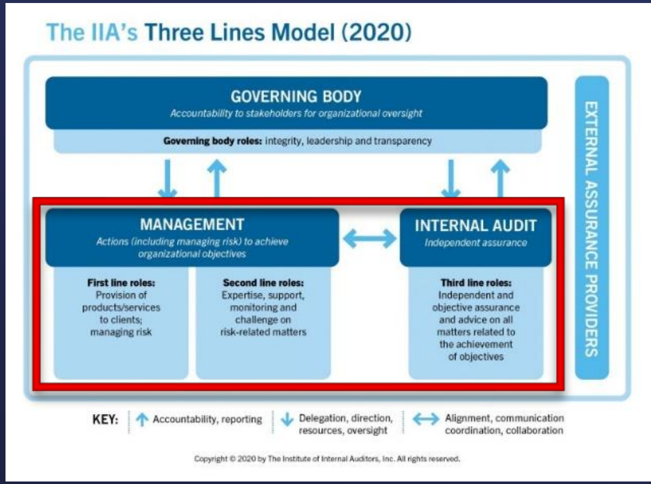
Organizational objectives
Outcomes & risk
Strategic planning
Communication

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives

FIRST LINE ROLES:	SECOND LINE ROLES:
Provision of products/services to clients; risk management	Expertise, support, monitoring, and challenge on risk-related matters

Key Roles and Relationships - Continued

Three Lines Model

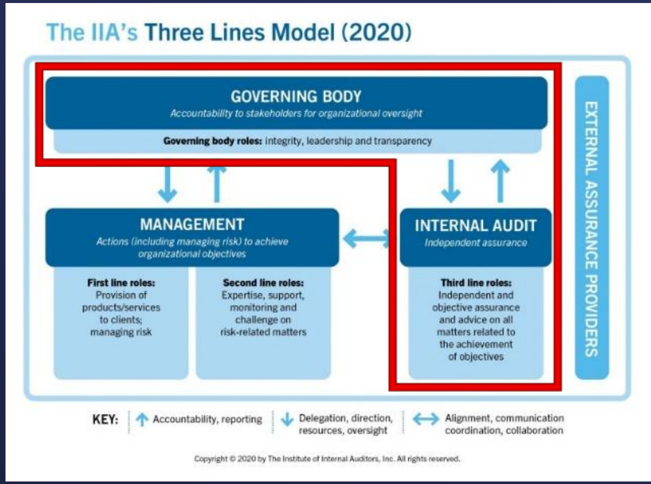


- Independent
- Interaction
- Strategic & operational
- Assurance & advice
- Collaboration & communication

Source: The IIA's Three Lines Model

Key Roles and Relationships - Continued

Three Lines Model



Source: The IIA's Three Lines Model

Key Roles and Relationships - Continued

Three Lines Model

INTERNAL AUDIT
Independent assurance

THIRD LINE ROLES:
Independent and objective assurance and advice on all matters related to the achievement of objectives

Three Lines Model

Applying the Model

Three Lines Model

Conclusion

- Strengthens governance
- Improves risk management & accountability
- Supports the achievement of goals
- Creates and protects value

Three Lines Model

Questions?

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

1928

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Committee Item
INFORMATION

Audit Committee

3/9/2026 Committee Meeting

7f

Subject

Annual Internal Audit Plan and Risk & Control Discussion

Executive Summary

This item provides a general overview of how the Office of the General Auditor creates the annual risk-based internal audit plan, presents an overview of internal controls, and provides current risk information. The purpose of this item is to provide a formal platform for board-level discussion and input regarding the District's internal control environment and current risk profile to be considered in the development of the annual General Auditor's Internal Audit Plan.

Applicable Policy

Metropolitan Water District Administrative Code Sections 2416(b)(4), 6451(a)(1), and 6451(d)(1)

Related Board Action(s)/Future Action(s)

In June 2026, we will present our Internal Audit Plan for FY 2026/27 to the Board for approval.

Details and Background

General Auditor's Internal Audit Plan

Developing an annual audit plan involves creating a risk-based strategic roadmap that aligns Audit Department activities with Metropolitan's goals. Key steps include defining the audit universe, performing risk assessments, engaging stakeholders, and setting the scope, timing, and resources for audits. The final approved document ensures resources focus on high-risk, critical areas of the District.

Standard 9.4 of The Institute of Internal Auditors' Global Internal Audit Standards (Standards) requires the chief audit executive (General Auditor) to create an internal audit plan that supports the achievement of an organization's objectives, and must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be performed annually and be informed by input from the Board and senior management, as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes.

Additionally, the Standards recommend that the Board communicate its perspective on the organization's strategies, objectives, and risks to assist the General Auditor with determining internal audit priorities (Standard 8.1).

Internal Control

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides internal control guidance in its *Internal Control – Integrated Framework*, which consists of 17 principles organized under the five components of internal control: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring Activities.

The Comptroller General of the United States created the Standards for Internal Control in the Federal Government (the Green Book), which adapts the COSO principles for government entities to establish and maintain an effective internal control system. Entity management determines, in accordance with applicable laws and regulations, how to adapt the Green Book framework appropriately.

The Office of the General Auditor has future initiatives to provide internal control training to District employees and to officially recognize the Green Book as the District's internal control framework.

Risk

Risk is the possibility that an event will occur and impact the achievement of objectives. As noted above, Standard 9.4 requires the chief audit executive to base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks, and to ensure the plan is responsive to organizational changes and emerging risks. As part of the risk assessment process, emerging risks are identified during the development of the annual audit plan and reassessed throughout the year. The risk assessment process also includes issues raised by the organization's board and senior management. This identification supports the evaluation of potential impacts to the District and contributes to the audit plan's development.

Various organizations gather and publish annual information on national emerging risks (**Attachment 1** and **Attachment 2**). The General Auditor uses this data to stay informed about the significant risks impacting organizations, which may include the District.

Metropolitan's Administrative Code Section 2416(b)(4) requires the Executive Committee to consider the effectiveness of the District's internal control system, including information technology security and control.

Metropolitan's Administrative Code Section 6451(a)(1) requires the scope of work of the Audit Department to determine whether the District's network of governance, risk management, and internal control, as designed and represented by District management, is adequate and functioning in a manner to ensure risks are appropriately identified, managed, and monitored.

Metropolitan's Administrative Code Section 6451(d)(1) requires the Audit Department to develop and present a flexible annual audit plan to the Audit Committee for review and approval. This plan should be developed utilizing a risk-based methodology and should include risks or internal control concerns identified by Management or the Board of Directors.

Attachment 1 – Internal Audit Foundation – 2026 Risk in Focus-Hot Topics for Internal Auditors

Attachment 2 – Protiviti – 2026 Edition – Unlocking Opportunity Executive Perspectives on Top Risks and Opportunities

2026 RISK IN FOCUS

Hot topics for internal auditors

NORTH AMERICA

Internal Audit FOUNDATION

ABOUT GLOBAL RISK IN FOCUS

Know Your Risks. Plan Strategically.

Risk in Focus is the Internal Audit's Foundation's premier annual initiative to identify the five most significant risks impacting organizations around the world.

Learn what internal auditors are saying about the:

- Five highest risks in their region
- Five top priorities for internal audit effort
- Key considerations for boards and audit committees

Risk in Focus uses survey results, regional roundtables, and interviews with local experts to reveal key insights about regional risks along with perspective on risks worldwide.

The Internal Audit Foundation gratefully acknowledges the work of IIA Institutes and IIA regional bodies who make this research possible: African Federation of Institutes of Internal Auditors (AFIIA), Arab Confederation of Institutes of Internal Auditors (ARABCIIA), Asian Confederation of Institutes of Internal Auditors (ACIIA), European Confederation of Institutes of Internal Auditing (ECIIA), and Fundación Latinoamericana de Auditing Internos (FLAI).

Special appreciation goes to the European Institutes Research Group (EIRG), who developed the Risk in Focus research approach in 2016 and continues to publish the report for Europe through the ECIIA.

Reports and board briefings are free to the public for:

- Africa
- Asia Pacific
- Europe
- Latin America
- Middle East
- North America
- Global Summary

Visit the Risk in Focus Knowledge Center for reports and more information.

Internal Audit FOUNDATION

Visit the **Risk in Focus Knowledge Center** for free reports and board briefings (**theiia.org/RiskInFocus**).

WORLDWIDE RESEARCH PARTICIPATION

131 countries/territories

4,073 survey responses

18 roundtables with **182** participants

24 in-depth interviews

CONTENTS

EXECUTIVE SUMMARY

Geopolitical Risks Increase Dramatically

The percentage of respondents in North America who ranked geopolitical uncertainty as one of their five highest risks spiked dramatically in North America, while cybersecurity and digital disruption remained high, according to the most recent Risk in Focus survey results.

In North America, 45% of survey respondents said geopolitical uncertainty was one of the five highest risks at their organization (up from 26% in the prior year) (Exhibit 3). North America tied with Europe and Latin America this year for geopolitical uncertainty risk levels (Appendix D). Rapid changes in U.S. policies initiated by the Trump administration are the likely drivers for this change, particularly tariffs and changes in federal funding.

At the same time, cybersecurity and digital disruption topped the risk rankings in North America, with 86% citing cybersecurity as one of the five highest risks, and 53% citing digital disruption (Exhibit 1). Risk ratings for regulatory change and business resilience increased moderately, keeping them on the list of highest risks.

Internal auditors are responding to geopolitical uncertainty with expanded advisory services and participation in broader strategic planning. They are joining cross-functional teams to proactively address new risks related to supply chain disruptions and changes in federal funding for the public sector, nonprofit organizations, and other industries.

The major driver for digital disruption risks in North America is generative artificial intelligence (AI), with cybercriminals taking advantage of it to increase their attacks. Organizations are forming AI governance teams to manage deployment and risks. At the same time, internal audit is increasing use of AI to automate routine tasks, increase efficiency, and provide data for stakeholders.

Continued volatility in geopolitics and technology is almost guaranteed, so internal auditors must prepare to provide support and direction. The North America Risk in Focus 2026 report features practical ways to address this unprecedented risk environment, using insights from roundtables and interviews conducted with internal audit leaders throughout the region.

Key Points

- Geopolitical risks spiked dramatically in North America, with 45% of survey respondents saying it was one of the five highest risks at their organization (up from 26% in the prior year) (Exhibit 3).
- Digital disruption risk, including AI, continues to increase and is now a Top 5 risk for 53% in North America (Exhibit 3).
- Cybersecurity remains the highest-rated risk in North America (86%) (Exhibit 1).
- Internal auditors are joining cross-functional teams to address supply chain issues and changes in federal funding.
- Strong IT governance is essential to prevent problems and take advantage of opportunities presented by generative AI and new technology.

NORTH AMERICA RESEARCH PARTICIPATION

- **271** survey responses
- **3** roundtables with **59** participants
- **3** interviews

NORTH AMERICA REPORT SPONSOR

AuditBoard

SECTION 1. NORTH AMERICA'S RISK ENVIRONMENT

Heightened Geopolitical Tensions Alter Risk Landscape

The percentage of respondents in North America who ranked geopolitical/macroeconomic uncertainty as one of their five highest risks spiked dramatically, rising 19 percentage points from the prior year (Exhibit 3). Two other areas – business resilience and regulatory change – saw smaller but notable increases that could be linked to the geopolitical change.

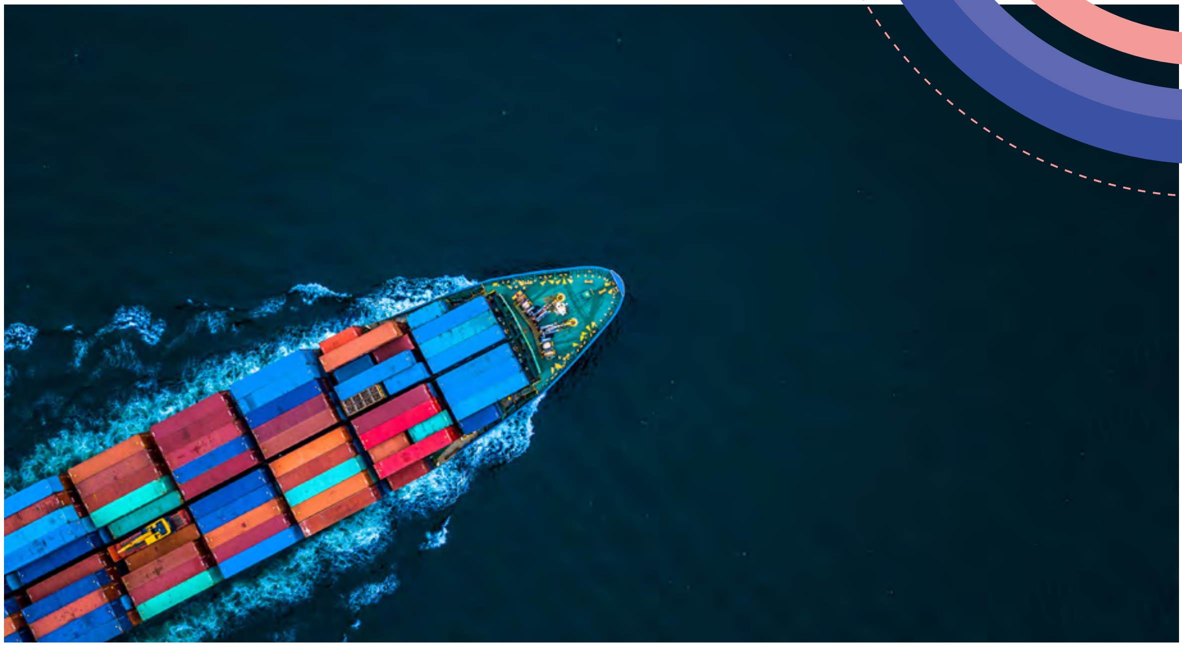
Geopolitical risks hit North America

In a dramatic shift from the previous two years of survey results, North America tied Europe and Latin America this year for the highest geopolitical risk levels in the world. In these three regions, 45% of survey respondents said geopolitical uncertainty was one of the five highest risks at their organizations (Appendix D). This stands in stark contrast to North America's survey results in the prior year, where geopolitical uncertainty was ranked ninth, with only 26% saying it was one of their Top 5 risks (Exhibit 3).

Rapid changes in U.S. policies initiated by the Trump administration are the likely drivers for this change, particularly tariffs and changes in federal funding policies.

As macroeconomic and geopolitical concerns are increasing, cybersecurity and digital disruption (including AI) remain the two top-rated risks in North America. Digital disruption continued its climb up the risk rankings from sixth to third to second. Cybersecurity remained entrenched as the highest ranked risk (Exhibit 3).

Risk in Focus survey results closely mirrored the World Economic Forum's assessment of global challenges, which were described as a "time of extraordinary volatility and uncertainty" in the Chief Economist's Outlook: May 2025. The same report noted that the rapid advance of AI has created additional complexity and opportunity in the global economic landscape.



NORTH AMERICA'S RISK ENVIRONMENT

During the North America Risk in Focus roundtables, internal audit leaders described active involvement in these two risk areas, including expanded advisory services. Additionally, interviews with internal audit thought leaders emphasized that volatility and uncertainty create important opportunities that internal auditors must embrace.

North American industries with the highest risk ratings for geopolitical uncertainty were manufacturing and mining/energy/water. These industries also showed high audit priority for supply chains. (Appendix C).

Risk levels compared to global

While geopolitical uncertainty risk went up 10 percentage points at the global level (Exhibit 4), it increased nearly twice as much for North America (19 percentage points) (Exhibit 3). The uptick for North America was the largest increase for a single risk area of any region in this year's survey results.

North America rated technology risks as higher than the global average. As in previous years, North American respondents cited cybersecurity as a high risk more often than the global average, with 86% listing it as a Top 5 risk, 13 percentage points higher than the global average. Digital disruption also was cited more often by North American respondents; 53% compared to 48% globally (Exhibit 2).

On the other hand, North America was lower than the global average for risk related to fraud (12 percentage points lower), climate change (11 percentage points lower), and governance/corporate reporting (9 percentage points lower) (Exhibit 2). Because so much fraud risk in North America is related to cybersecurity, the lower fraud risk rating for North America may be offset by the higher rating for cybersecurity.

In last year's Risk in Focus survey, North American respondents expected climate change risk ratings to increase in the next three years. However, the dramatic changes in the geopolitical landscape led more people to choose geopolitical uncertainty as one of their Top 5 risks, and climate change risk ratings dropped 6 percentage points in North America, tying for the lowest rated risk on the list (Exhibit 3).

Audit priorities

Audit priorities shifted in response to risk level changes but to a lesser extent. (Audit priorities are defined as the five areas where internal audit spends the most time and effort.)

In North America, audit priority ratings for geopolitical uncertainty grew by 8 percentage points over the prior year (Exhibit 7). Nevertheless, the audit priority ratings for geopolitical uncertainty in North America were still much lower than the risk level ratings. Roundtable participants explained that geopolitical uncertainty is not a typical audit area with identifiable processes and controls. Therefore, to address geopolitical risks, audit priority increases in related areas, for example, business resilience, which increased 6 percentage points, or market changes/competition, which increased 4 percentage points (Exhibit 7).

Risk ratings for geopolitical uncertainty in North America increased 19 percentage points – nearly double the global increase, which was 10 percentage points (Exhibits 3 and 4).

NORTH AMERICA'S RISK ENVIRONMENT

Audit priorities compared to global

North America and the global average were fully aligned for the five highest audit priority areas: cybersecurity, business resilience, governance/corporate reporting, regulatory change, and financial/liquidity (although with slightly different rankings) (Exhibit 6).

Audit priority for digital disruption increased the most, both for North America and global – 11 percentage points for North America and 7 percentage points for global. The second highest increase was for geopolitical/macroeconomic uncertainty – up 8 percentage points for North America and 3 percentage points for global (Exhibits 7 and 8).

One notable difference between North America and global audit priority was for business resilience – increasing 6 percentage points for North America compared to a decrease of 2 percentage points for global (Exhibits 7 and 8). North America's uptick was likely a way of responding to increased geopolitical uncertainty, according to roundtable participants.

Risk compared to audit priority

For both North America and global, three out of the five highest risks were also high audit priorities – cybersecurity, regulatory change, and business resilience.

At the same time, several risks showed large gaps between risk levels and audit priority, in particular, geopolitical uncertainty, human capital, and digital disruption. Geopolitical risk ratings exceeded audit priority ratings by 35 percentage points in North America and 27 percentage points globally. Similarly, human capital risk ratings exceeded audit priority ratings by 27 percentage points in North America, but a more modest 14 percentage points globally. Digital disruption had a smaller gap, but it was still notable: 10 percentage points for North America and 16 percentage points for global (Exhibits 9 and 10).

As noted earlier, some gaps may be explained by difficulty in directly auditing an area, for example, geopolitical uncertainty. Or the issue may be a lack of processes in place or a lack of audit skills in an area, for example, digital disruption.

A closer look at urgent risks

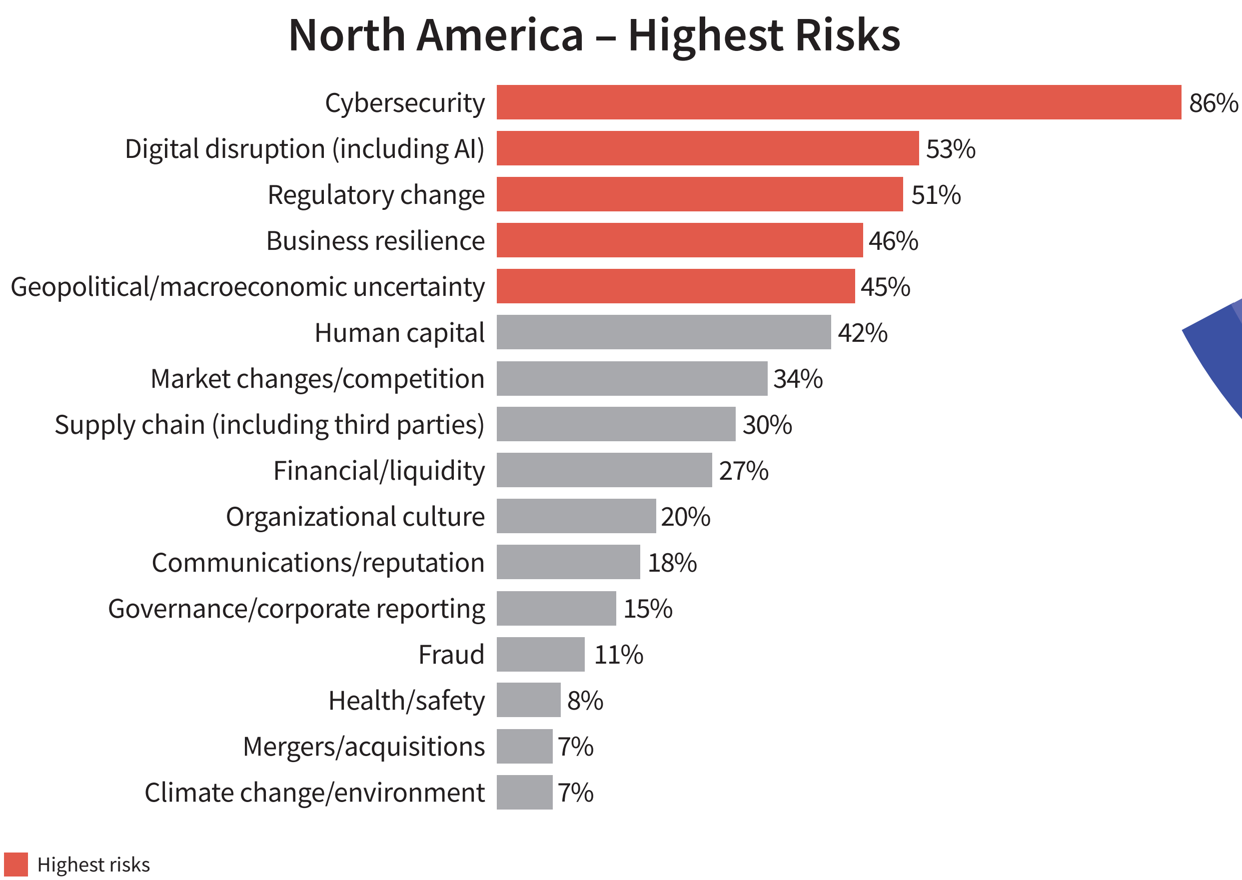
Based on survey results and roundtables, the featured topics for this year's Risk in Focus report are geopolitical uncertainty and digital disruption. See Section 3 for insights into how internal audit and their organizations are meeting challenges in these high-risk areas.

Based on survey results and round tables, the featured topics for this year's Risk in Focus report are geopolitical uncertainty and digital disruption.

SECTION 2. RISK LEVELS

Exhibit 1. North America – Highest Risks

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

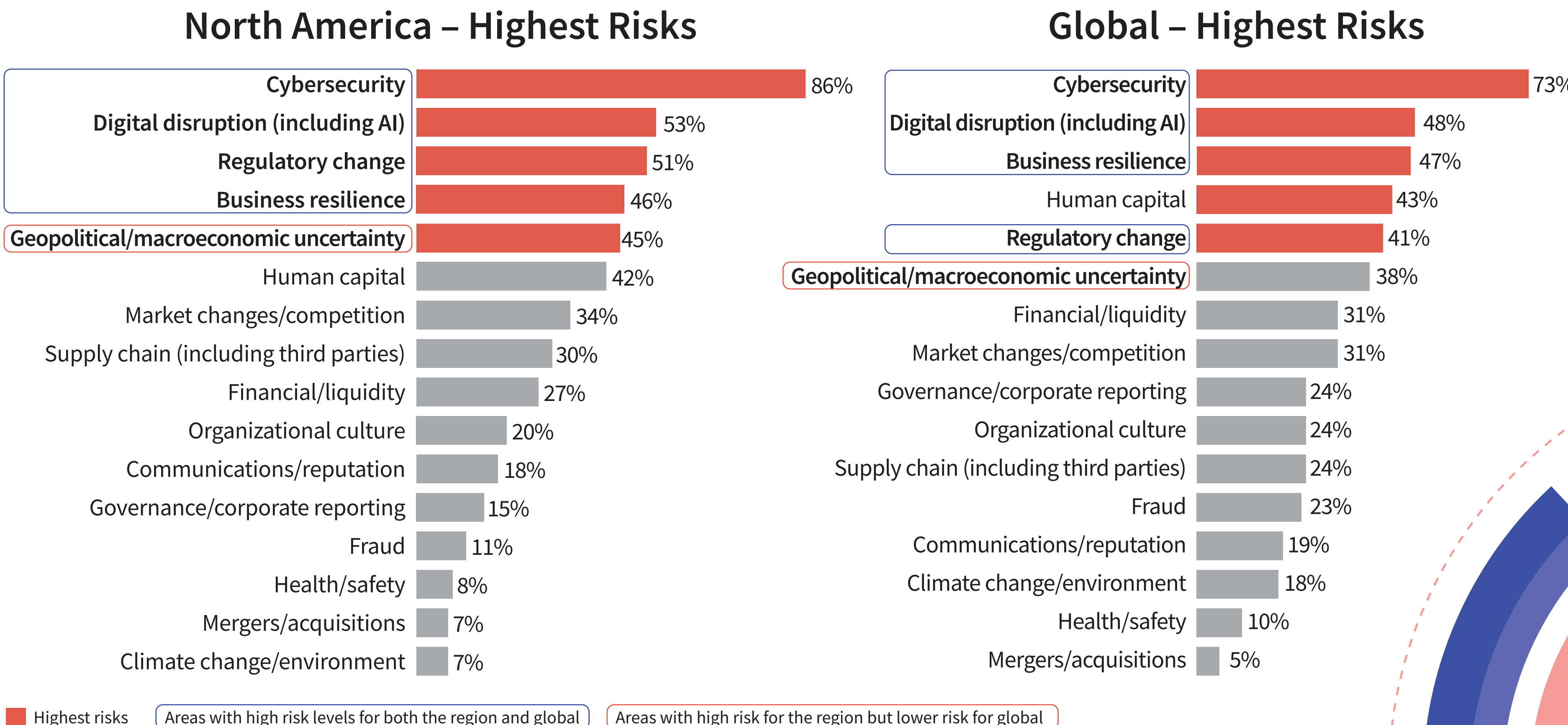


Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.

RISK LEVELS

Exhibit 2. North America vs. Global – Highest Risks

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**



Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America. *n* = 4,073 for global.

RISK LEVELS

Exhibit 3. North America – Risk Level Trend

***Survey question:* What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	Change from 2024 to 2025	Change	Risk area
85%	87%	86%		-1	Cybersecurity
36%	48%	53%		+5	Digital disruption (including AI)
43%	47%	51%		+4	Regulatory change
36%	41%	46%		+5	Business resilience
28%	26%	45%		+19	Geopolitical/macroeconomic uncertainty
65%	54%	42%		-12	Human capital
41%	41%	34%		-7	Market changes/competition
36%	29%	30%		+1	Supply chain (including third parties)
28%	28%	27%		-1	Financial/liquidity
21%	20%	20%		0	Organizational culture
21%	20%	18%		-2	Communications/reputation
16%	16%	15%		-1	Governance/corporate reporting
9%	9%	11%		+2	Fraud
17%	13%	8%		-5	Health/safety
8%	8%	7%		-1	Mergers/acquisitions
12%	13%	7%		-6	Climate change/environment

Increased risk level compared to prior year   Decreased risk level compared to prior year

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.
Note 2: The orange and blue bars show the difference in risk level ratings from 2024 to 2025. The column labeled "change" shows the percentage point difference between 2024 and 2025. The areas are listed from the highest to lowest risk level rating for 2025. The years indicate the year the survey was conducted.

RISK LEVELS

Exhibit 4. Global – Risk Level Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	Change from 2024 to 2025	Change	Risk area
73%	71%	73%		+2	Cybersecurity
34%	39%	48%		+9	Digital disruption (including AI)
47%	54%	47%		-7	Business resilience
51%	49%	43%		-6	Human capital
39%	37%	41%		+4	Regulatory change
30%	28%	38%		+10	Geopolitical/macroeconomic uncertainty
32%	32%	31%		-1	Financial/liquidity
32%	32%	31%		-1	Market changes/competition
27%	26%	24%		-2	Governance/corporate reporting
26%	25%	24%		-1	Organizational culture
26%	22%	24%		+2	Supply chain (including third parties)
24%	27%	23%		-4	Fraud
21%	21%	19%		-2	Communications/reputation
19%	21%	18%		-3	Climate change/environment
11%	11%	10%		-1	Health/safety
6%	6%	5%		-1	Mergers/acquisitions

Increased risk level compared to prior year   Decreased risk level compared to prior year

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 4,073 for global.
Note 2: The orange and blue bars show the difference in risk level ratings from 2024 to 2025. The column labeled "change" shows the percentage point difference between 2024 and 2025. The areas are listed from the highest to lowest risk level rating for 2025. The years indicate the year the survey was conducted.

SECTION 3. AUDIT PRIORITIES

Exhibit 5: North America – Highest Audit Priorities

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

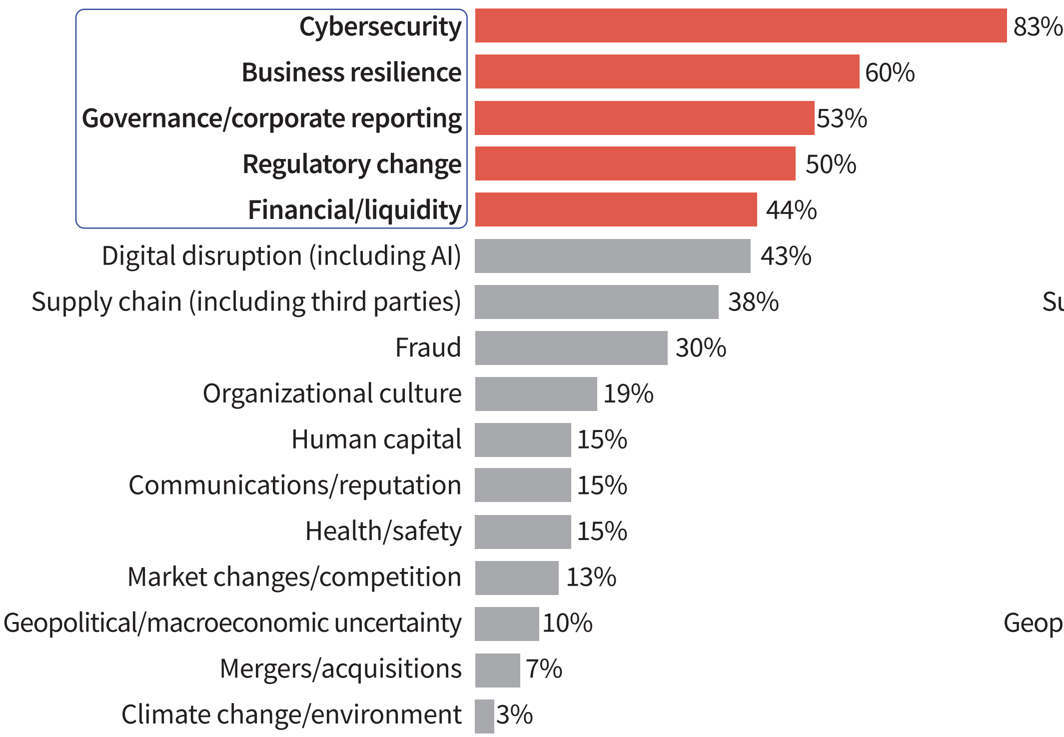
Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.

AUDIT PRIORITIES

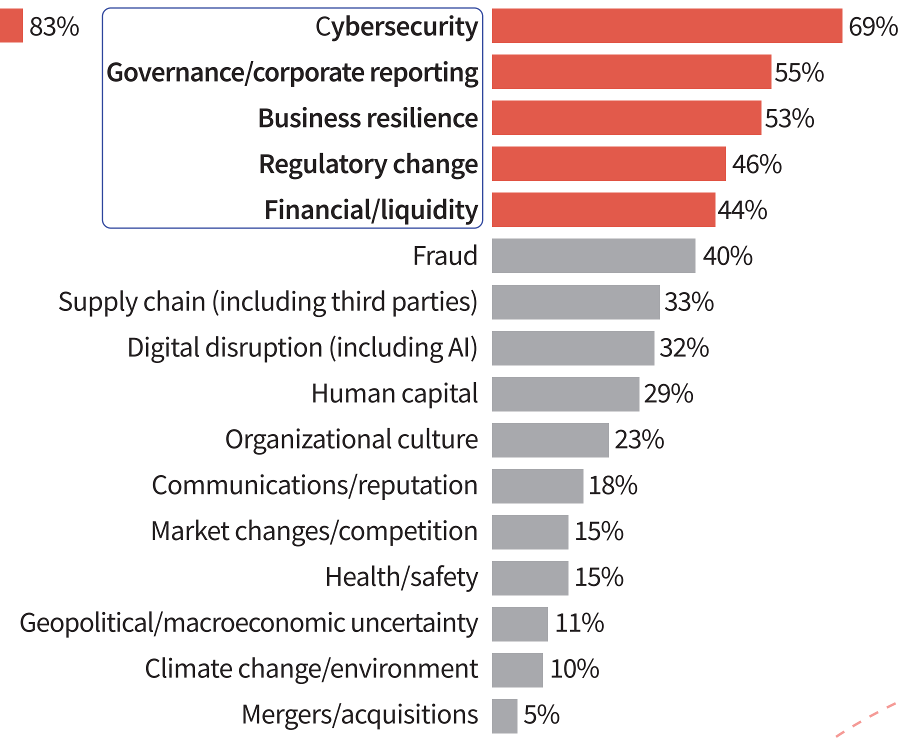
Exhibit 6.North America vs. Global – Highest Audit Priorities

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

North America – Highest Audit Priorities



Global – Highest Audit Priorities



Highest audit priorities | Areas with high audit priority for both the region and global | Areas with high audit priority for the region but lower audit priority for global

Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America. *n* = 4,073 for global.

AUDIT PRIORITIES

Exhibit 7. North America – Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	Change from 2024 to 2025	Change	Risk area
84%	87%	84%		-3	Cybersecurity
53%	54%	60%		+6	Business resilience
55%	58%	52%		-6	Governance/corporate reporting
53%	54%	51%		-3	Regulatory change
25%	33%	44%		+11	Digital disruption (including AI)
46%	46%	44%		-2	Financial/liquidity
38%	34%	37%		+3	Supply chain (including third parties)
26%	29%	30%		+1	Fraud
17%	15%	18%		+3	Organizational culture
21%	16%	15%		-1	Health/safety
26%	27%	15%		-12	Human capital
20%	17%	14%		-3	Communications/reputation
14%	10%	14%		+4	Market changes/competition
4%	3%	11%		+8	Geopolitical/macroeconomic uncertainty
10%	10%	7%		-3	Mergers/acquisitions
9%	9%	3%		-6	Climate change/environment

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.
Note 2: The orange and blue bars show the difference in audit priority ratings from 2024 to 2025. The column labeled "change" shows the percentage point difference between 2024 and 2025. The areas are listed from the highest to lowest audit priority rating for 2025. The years indicate the year the survey was conducted.

AUDIT PRIORITIES

Exhibit 8. Global – Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	Change from 2024 to 2025	Change	Risk area
68%	69%	69%		0	Cybersecurity
55%	56%	55%		-1	Governance/corporate reporting
54%	55%	53%		-2	Business resilience
46%	46%	46%		0	Regulatory change
45%	45%	44%		-1	Financial/liquidity
42%	41%	40%		-1	Fraud
34%	**31%**	**33%**		**+2**	**Supply chain (including third parties)**
22%	**25%**	**32%**		**+7**	**Digital disruption (including AI)**
30%	31%	29%		-2	Human capital
24%	23%	23%		0	Organizational culture
20%	20%	18%		-2	Communications/reputation
16%	16%	15%		-1	Market changes/competition
17%	16%	15%		-1	Health/safety
9%	**8%**	**11%**		**+3**	**Geopolitical/macroeconomic uncertainty**
11%	12%	10%		-2	Climate change/environment
6%	6%	5%		-1	Mergers/acquisitions

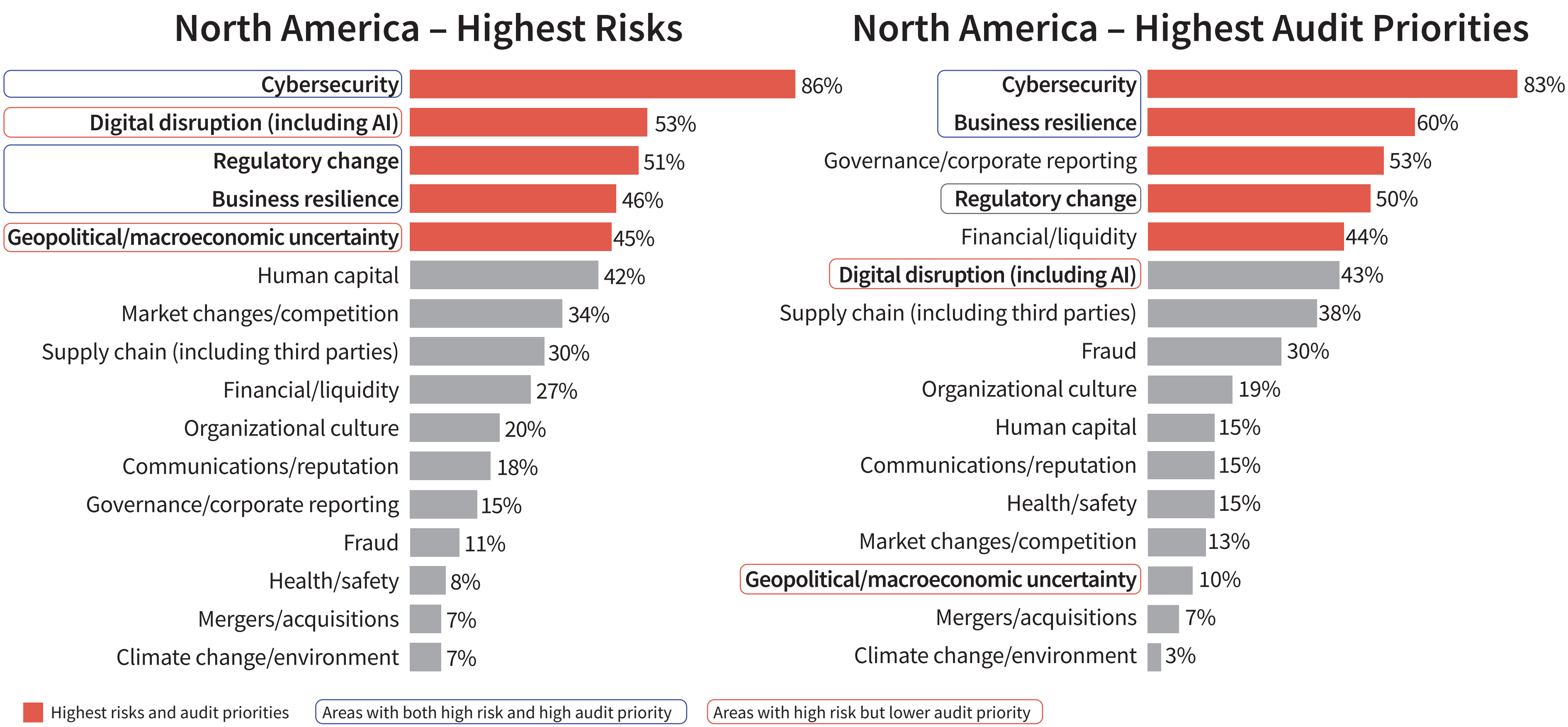
Increased audit priority compared to prior year   Decreased audit priority compared to prior year

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 4,073 for global.
Note 2: The orange and blue bars show the difference in audit priority ratings from 2024 to 2025. The column labeled "change" shows the percentage point difference between 2024 and 2025. The areas are listed from the highest to lowest audit priority rating for 2025. The years indicate the year the survey was conducted.

SECTION 4. RISK VS. AUDIT PRIORITIES

Exhibit 9. North America – Risk vs. Audit Priorities

Survey questions: **What are the Top 5 risks your organization currently faces? (Choose 5.)**
What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)

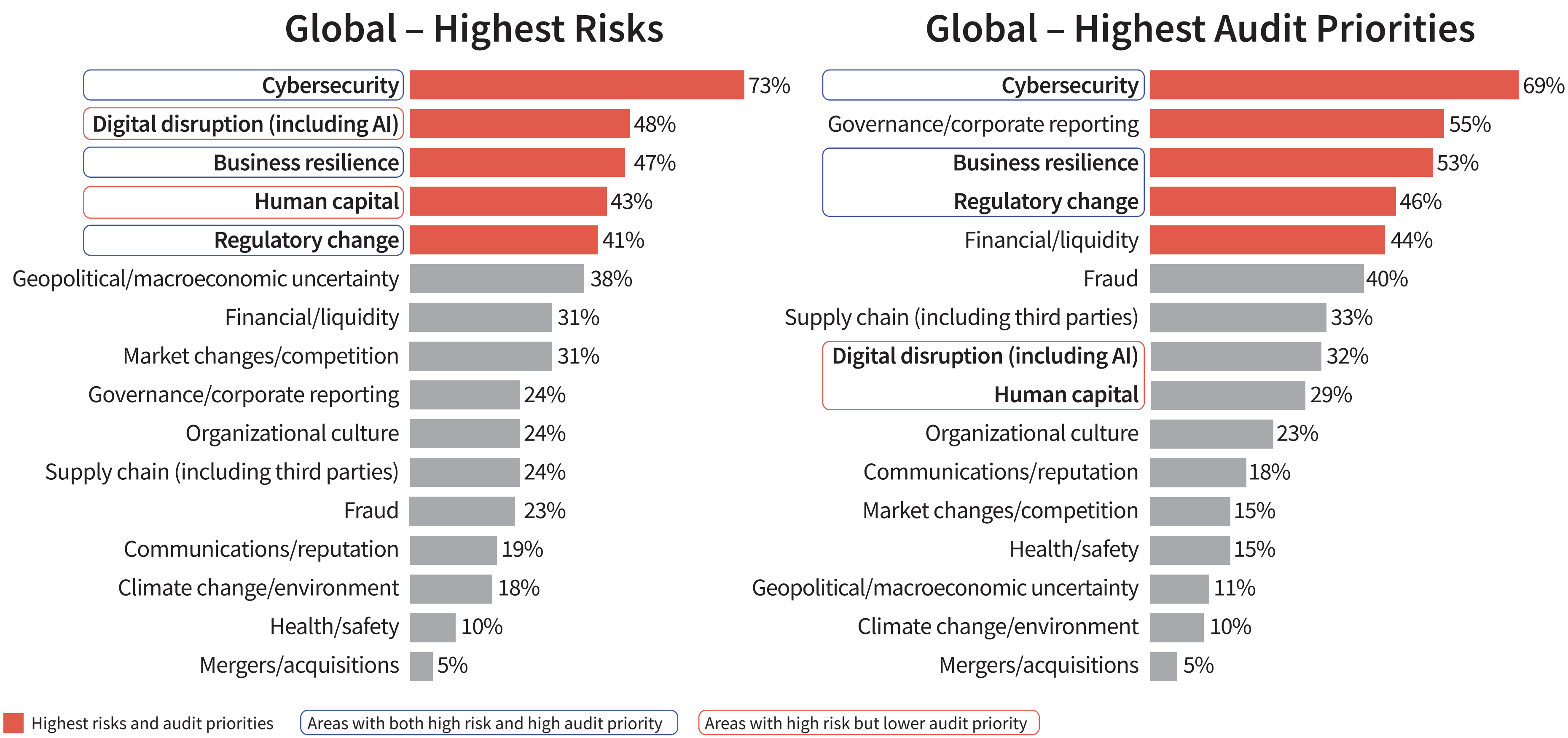


Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.

RISK VS. AUDIT PRIORITIES

Exhibit 10. Global – Risk vs. Audit Priorities

Survey questions: **What are the Top 5 risks your organization currently faces? (Choose 5.)**
What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)



Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 4,073 for global.

SECTION 5. HOT TOPICS

GEOPOLITICAL UNCERTAINTY

New U.S. Policies Drive Up Risk

North American internal audit leaders are responding to uncertainty by pivoting to expanded advisory services and participating in broader strategic planning.

The U.S. policy shifts were announced by the Trump administration as the Risk in Focus survey was in progress, making it likely that this risk continued to increase after the survey ended.

Geopolitical/macroeconomic uncertainty is peaking at levels not seen since the COVID crisis. Less than five years removed from that global emergency, organizations are struggling to cope with new volatility and uncertainty from policy changes implemented by U.S. President Donald Trump.

For example, the potential impact on domestic policies and spending drove one internal audit leader at an agri-business lending organization to rank geopolitical/macroeconomic uncertainty as his top risk. Uncertainty about the annual Congressional Farm Bill, which often includes provisions related to agricultural trade, such as export subsidies and international food assistance programs, is driving volatility in the sector, he said.

“We have some big winners some days in the direction that things are headed and some big losers. So, it tends to balance out a bit across our portfolio,” he said. “But we have very significant clients that are dealing with crazy input costs and volatility in the markets. That’s definitely why I placed it as number one for us.”

GEOPOLITICAL UNCERTAINTY

Widespread impacts

Supply chain risk is one of the driving factors behind many organizations' concerns. Whether it's sourcing ingredients for a global restaurant chain or getting healthcare supplies that can only be obtained from China, organizations are scrambling for alternatives and financially viable solutions.

Another looming obstacle is the widespread cuts in federal funding, initiated by the Department of Government Efficiency (DOGE) formed by the Trump administration. The CAE at a not-for-profit company that operates in more than 20 countries said federal funding cuts have prompted reexamination of budgets, called into question the viability of foreign offices, and may trigger a reorganization. An internal auditor working in state government expressed concerns about the ban on programs for DEI (diversity, equity, and inclusion) and how that could affect funding for a variety of programs that rely on federal support.

Delivering value to boards and management

Internal auditors should be key allies in helping organizations to be resilient and deal with evolving risks, said Richard Chambers, senior internal audit advisor for AuditBoard. But boards and executive management need to be educated about what internal audit offers.

"We [internal auditors] need to have frank and candid conversations with executive management and the board about the environment in which we live, and we need to educate them on what our potential is to help navigate that environment," said Chambers. "Very few board members or executive management members are going to naturally think, 'Oh, tariffs are changing three times a day. What I need to do is call the internal auditors and see what they're thinking.'"

"We have to influence the change we want to see," Chambers said. "We want our stakeholders to see our capabilities in a broader light or in a different light. Then we have to deliver."

Benito Ybarra, IIA executive vice president of global standards, guidance, and certifications, added, "Leading internal auditors like the challenge of making their organizations better. Internal auditors have a huge opportunity to engage board members and senior leaders to make sure that they understand what internal audit can do to help organizations thrive."

> "Supply change risk is one of the driving factors behind many organizations' concerns."

GEOPOLITICAL UNCERTAINTY

Advisory services across industries

The new geopolitical reality is driving an all-hands-on-deck mentality in organizations, which is expanding use of internal audit for advisory services across industries. Internal auditors are using their expertise in organizational operations to help develop new strategies.

Increasing inventory (Utilities)

For one Midwestern utility, the changing risk landscape brought together leaders from IT, ERM, executive management, and internal audit to identify and mitigate evolving risks. The utility explored how tariffs announced by the Trump administration affected supply chain strategies. For example, inventory of critical and long-lead-time products was dramatically expanded.

"We use a lot of steel poles and transformers, things that have heavily tariffed materials," said Andrea Klubertanz, audit manager at ATC, a Wisconsin-based utility company. "We are increasing our inventory by forty- to sixty-fold in the course of a few years and to an amount that is material to our financial statements. The pace at which we're growing, the long lead times, and the lack of suppliers in that space make it particularly challenging for us."

Beyond expanding inventory, the utility is reexamining its vendor list and looking for alternative suppliers who might not be impacted by tariffs. They also are examining whether there may be engineering solutions to support growing load demand. Since the pandemic, the utility has looked at better aligning audit services with company strategy, and internal audit has adopted the same mindset.

"We're really trying to think more strategically," Klubertanz said. Her team shifted away from routine audits and started to review the risks for key areas such as construction, procurement, and strategic resource alliances. "These are the kinds of things that our stakeholders, our audit committee, want to see," Klubertanz explained.

Board communications (Clothing retailer)

At an international clothing retailer based in North America, geopolitical uncertainty has become one of the organization's top enterprise risks. The internal audit function has stepped up its risk advisory work, keeping management informed about tariffs and military actions that affect suppliers.

The new geopolitical reality is driving an all-hands-on-deck mentality in organizations, which is expanding use of internal audit for advisory services across industries.

GEOPOLITICAL UNCERTAINTY

Counting costs (Manufacturing)

The audit leader of a global professional services company said she realized her organization needed to do an advisory review of the supply chain process when they tried to find alternate manufacturing locations to ease reliance on Asia. "Unfortunately…a lot of those (alternative) countries are also now impacted by high tariffs," she said. Internal audit conducted a detailed review of the supplier award process and supplier performance to determine if the mix remained beneficial to the organization. Their review also looked at supply chain decision-making and whether short-term and long-term impacts were being considered. From a financial perspective, internal audit also explored whether business units were considering tariff impacts, inventory costs, and how costs would be reflected on income statements.

Reconsidering marketing (Software technology)

For a software technology company, the uncertainty has prompted an examination of risk concentration in some of the regions in which it operates. "We're looking at the footprint and saying, 'Can we really rationalize the number of countries we operate in without necessarily increasing our risks?'" said its vice president of internal audit, adding that such risks include compliance with sovereign data rules, privacy, and sustainability, as well as the potential for increased fraud.

> Ultimately, the aim is to have a clear view of risks and the effectiveness of risk mitigation, and to provide assurance and support to the areas of highest risk.

Conclusion

The complexity of the business environment can seem overwhelming at some organizations, said Ybarra, but internal auditors can help bring clarity by reexamining risk assessments and understanding where the organization's critical assets lie. Having a clear idea of who provides assurance over risk mitigation efforts in key areas through risk mapping and second-line collaborations also is vital. Ultimately, the aim is to have a clear view of risks and the effectiveness of risk mitigation, and to provide assurance and support to the areas of highest risk. This presents a holistic view of risk management that boards and senior management want and need to hear, Ybarra said.

GEOPOLITICAL UNCERTAINTY

Key Points

Survey findings

- Geopolitical/macroeconomic uncertainty as a Top 5 risk spiked dramatically, rising 19 percentage points year over year (Exhibit 3).
- As a result, North America risk in this area was higher than the global average for the first time for the Risk in Focus project.
- Geopolitical/macroeconomic uncertainty saw the second highest increase – 8 percentage points – in the number of survey respondents who listed it as a Top 5 area where internal audit spends most time and effort (Exhibit 7).

Internal audit strategies

- Pivot to changing geopolitical uncertainty by reviewing materials sourcing.
- Monitor federal funding cutbacks for direct impacts on budgets and projects and implications for third-party contractors.
- Explore implications of new tariffs on supplier contracts.
- Examine new and existing regulations for impacts on existing contracts and supplier relationships.
- Seek greater involvement in broader strategic planning through expanded meetings with key C-suite and department leaders.
- Educate boards and executive management about internal audit's potential to help navigate the current risk environment.

DIGITAL DISRUPTION

Generative AI Causes Paradigm Shift

Less than three years after the introduction of ChatGPT, generative AI is creating profound impacts on business. From improving efficiency, competitiveness, and resilience to fundamentally altering how the C-suite views human capital, generative AI meets the definition of a paradigm shift.

Over the past two years, the percentage of North American survey respondents listing digital disruption as a Top 5 risk grew 17 percentage points (Exhibit 3). Much of that growth is likely driven by North America's rapid adoption of generative AI products. Since the first practical generative AI products were introduced in late 2022, AI use has exploded.

Stanford's 2025 AI Index Report stated that AI business usage in the U.S. is accelerating rapidly, with 78% of organizations reporting using AI in 2024, up from 55% the year before. In addition, a report from the National Bureau of Economic Research stated that nearly 4 in 10 of the U.S. population age 18 to 64 were using generative AI at work or at home in 2024, with 9.2% saying they used it every day.

Against this dramatic backdrop, internal auditors are striving to understand AI's impact on business strategies and risks (including cybersecurity) while simultaneously leveraging the technology to improve their own efficiency, relevance, and value.

Cybercriminals take advantage of AI

Cybercriminals are also using AI as a powerful tool to increase the frequency and sophistication of attacks. One of the most troubling data points is the sheer volume of attacks organizations face, with the number exploding globally from 579 attacks per second in 2021 to a staggering 7,000 password attacks per second in 2024, according to the Microsoft Digital Defense Report 2024. In addition, spammers save 95% on campaign costs using large language models (LLMs) to generate phishing emails, according to a Harvard Business Review article.

Over the past two years, the percentage of North American survey respondents listing digital disruption as a Top 5 risk grew 17 percentage points (Exhibit 3).

DIGITAL DISRUPTION

Risk in Focus roundtable participants cited a variety of personal experiences with AI-assisted cyberattacks. For example, a public sector CAE discovered that people were using AI to generate fake IDs and bills in attempts to get paid for fraudulent benefits claims.

AI's impact on the workforce

In its State of AI report (March 2025), McKinsey noted that companies are starting to implement new structures and processes designed to extract value from AI. Increasingly, this includes redesigning workflows to integrate generative AI, with 21% reporting fundamental redesigns. Larger organizations are adapting more rapidly, particularly in AI governance and risk management.

Some CEOs are insisting that employees use AI. Shopify CEO Tobias Lütke not only announced the expectation that everyone in the organization would use AI, but he also said that any request for additional resources would have to demonstrate why AI couldn't be used instead. Additionally, Lütke stated AI use would become an explicit part of employee performance evaluations.

A CAE at the roundtable said his organization has the same perspective: "Our CEO put out something very similar," he said. "Before recruiting across the organization, including for internal audit, there's a drive to make sure that AI can't do what we're trying to recruit for."

RESOURCE: The IIA's Cybersecurity Topical Requirement

The new IIA Cybersecurity Topical Requirement (February 2025) provides guidance for internal auditors to follow when auditing cybersecurity. Available free to download from The IIA global headquarters website.

The Cybersecurity Topical Requirement directs those working on cybersecurity audits to assess at minimum:

Governance	Risk Management	Controls
Strategy/objectives	Cyber risk assessment/risk management	Internal/vendor controls
Policies/procedures	RM scope	Talent management controls
Roles/responsibilities	Accountability/responsibility	Monitoring controls
Stakeholder engagement	Escalation process	Lifecycle inclusion
	Risk awareness process	Continuous improvement
	Incident response/recovery	Network controls
		Endpoint communications

Topical Requirements are available to download for free from The IIA global headquarters website.

Ford CEO Jim Farley recently predicted AI will replace "literally half of all white-collar workers in the U.S.," while Marianne Lake, CEO of Consumer & Community Banking at JPMorgan Chase, told investors she could see the massive firm's headcount falling by 10% in the future because of AI, according to an article in the Wall Street Journal.

DIGITAL DISRUPTION

Multiple roundtable participants said they are turning to external service providers and consultants to support their AI journey. A bank CAE at the roundtables wants to explore where AI fits in across all levels of the organization. "What are the questions we should be asking? I'm talking all the way up at the oversight level, at the board level," he said.

More cautious approaches

Although AI implementation is mandated by some large organizations, anecdotal evidence from roundtables suggests that smaller organizations are relatively cautious about using AI (as also noted in the McKinsey report). A CAE at a smaller community bank in Texas said she finds the current governance very restrictive at her organization. She lamented that her team cannot use AI as they'd like. A CAE from the insurance industry said that Microsoft Copilot is the only generative AI their organization allows. This organization primarily sees AI as an efficiency booster and urges users to closely review AI outputs for accuracy. The internal audit function at this organization therefore uses AI primarily to support report drafting.

A public sector auditor in Canada said that her province is slow in developing a governance framework for AI, so she has few options for implementing it in her audit function. Despite this, she is trying to leverage AI where she can safely do so to improve efficiency within her function.

AI governance teams

Whether AI implementation is conservative or aggressive, many organizations are assembling AI governance teams to manage deployment, and CAEs are being included. For example, a roundtable participant said their global professional services firm created an AI council focused on leveraging AI to interact with customers. The council is led by the CIO, CAE, and other senior management.

A CAE from financial services said his organization uses a governance council that evaluates AI use cases both internally and eventually for customers as a service. The council's work so far has focused on evaluating vendors who use AI and are providing services to customers or for clients seeking to add AI products to existing services.

"The governing council evaluates security and privacy, among other things, to see whether we can move forward with those use cases," he said. "I think the committee itself is still learning what the real risks are and what types of services we can allow."

Even when an AI governing council is in place, auditing AI governance is proving to be a challenge. A CAE in financial services said his team conducted a search for governance frameworks in 2024 that they could use for AI evaluation, but they found no blueprint at the time that described what good AI governance looks like. A second financial services CAE agreed, describing the area of AI frameworks as a "greenfield."

"Many organizations are assembling AI governance teams to manage deployment, and CAEs are being included."

DIGITAL DISRUPTION

Auditing AI automation

Tammy Valvo, CAE at Gate City Bank, said the bank is using AI and robotic process automation (RPA) to automate where possible, estimating that business process improvement automations have already delivered the equivalent of more than 66,000 hours of time saved in the past three years.

"It doesn't mean we've reduced people, because we haven't laid people off to do it," Valvo said. "It just means that we're using people to do things that only people can do and using systems to do more routine things that, quite frankly, people often get bored doing and then don't do well."

As processes throughout the organization are automated using AI and RPA, Valvo is reviewing workflows to ensure leaders remain aware of what is happening within those processes. Additionally, with the growing reliance on business intelligence and tools such as Tableau, internal audit is working to ensure there is an understanding of where the data originates, where it is going, and what it is informing, she said.

Similarly, Klubertanz said her internal audit team is working on ways to help ensure that data integrity, access management, and other aspects of automation are appropriately handled from a security perspective.

Hidden risks of automation

Valvo's experience with auditing automated systems brings to light various potential pitfalls that effective assurance can help deter, and one of the biggest is the idea that once systems or processes are automated, they can be left alone.

"It's out of sight, out of mind once you don't have to do it anymore," she said. "There's basically no human interaction in that step. It's easy to forget that that step even happens. You assume that step is still working the way that it should, but you don't know."

This is particularly relevant if changes are made in systems that feed data to automated systems, she said. "If there's a downstream change in another system, you may not know that it didn't work. Eventually you'll probably figure it out because you'll start to have errors, or you'll start to see issues. But you may not even make the connection," she said. "You may put band-aids on them without realizing that it's a systemic thing that's happening."

From a first-line perspective, those types of risks need to be identified, and automated processes need to be fully understood so that when changes are considered, all implications of the changes are understood. From an audit perspective, Valvo and her team look at source codes for automated processes to ensure they are designed to do what leadership thinks they are doing, she said.

RESOURCE: Auditing IT Governance and IT Management

This Global Technology Audit Guide (GTAG) from The IIA helps internal auditors:

- Identify gaps in IT governance
- Evaluate alignment with organizational objectives
- Provide recommendations to bolster IT oversight and resilience

Updated in August 2025 and aligned with the latest IIA Standards, this GTAG is available to IIA members for free from The IIA global headquarters website.

DIGITAL DISRUPTION

The other risk to consider is decidedly human focused – individual knowledge of what's been automated.

"For example, I'm the leader, and I know all the processes that I automated," Valvo said. "But when I change roles, and someone else comes in, they're going to have no idea what was automated, and no one's going to even think to tell them because no one's thinking about it anymore because it's automated."

Auditing AI at a technology company

An audit leader at a Canadian information management company said AI is significant at their organization for two key reasons: first, it has incorporated AI into information management software it retails, and second, AI provides a unique competitive advantage for the business.

"We're no different from Salesforce and Oracle, where we see it [AI] as a way to really digitize operations; the way you interact with products and with customers through chatbots; the way you fulfill products; the way you go to market; the way you price solutions," he said.

The challenge for internal audit is to provide assurance over a rapidly growing number of business cases across the organization, all aimed at accelerating customer response times, he said. "I want to really make sure that the governance, the policies, the expectations are well laid out and they're followed through," he said. "There's an aspect around the efficiency of AI models that we haven't got around to auditing yet, but it's very front and center."

Auditing AI models in financial services

An audit leader at a California insurance group noted that regulators are concerned about bias in AI models, privacy issues, and more. Similarly, an internal audit leader at a fintech startup in the Northeast, which has AI built into its service model, said her team is focused on identifying independent model validation processes to ensure AI models are working as intended. The organization will most likely use an external firm to validate this model to ensure operational accuracy.

Internal audit finds new ways to use AI

AI is an effective tool to increase efficiency for routine internal audit tasks, according to roundtable participants. Several describe using AI to generate emails, review draft reports for clarity and tone, and improve internal work processes. Several CAEs touted AI as the equivalent of adding a part-time junior staff auditor or intern. A CAE at a nonprofit said her organization is encouraging AI's use specifically because of limited funding.

AI can also help internal auditors improve their process analysis and communication skills. "We use AI to improve how we are doing things from an analysis standpoint, improving our work with procedures, and writing reports in a different way to make sure we're getting the right points across to stakeholders," said another CAE, repeating the views of several roundtable participants.

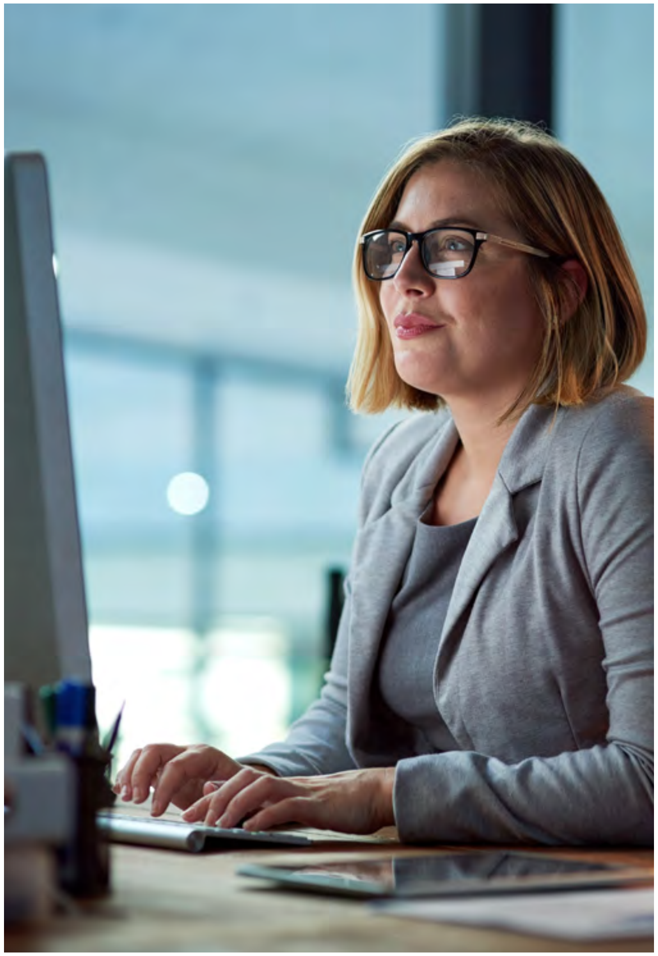
DIGITAL DISRUPTION

In contrast, one senior manager at a bank expressed concern that younger auditors accept AI output without question, "no matter how much training we have regarding using skepticism." As a precaution, AI use in his internal audit function is separated from all assurance activities, he said.

"If AI can help summarize a report, for instance, or perhaps make a process narrative more concise, that would be one permissible use, provided it still had certain precautions in place," he said. "But we would distinguish that use of AI from using it to develop assurance conclusions or observations."

Testing AI can have a playful side. A CAE at a Texas insurance company found a creative way to use her organization's internal AI chatbot to answer internal audit questions and promote the internal audit function during Internal Audit Month in May.

"We did little [video] snippets about what our company values are and how internal audit is using the bot to pave the way for the organization," she said. "We're kind of just dipping our toe into the water right now, playing with work papers and risk assessments, editing reports, and dumping data behind our firewall to see what analysis and insights that [data] can give us. We're trying to do it in a fun way where it's not intimidating or scary or unknown."



RESOURCE: Internal Audit Use Cases for AI

Read about insights and use cases from internal audit leaders who have integrated or explored AI within their teams in two new reports from the Internal Audit Foundation:

- Solving the Riddle: Harnessing Generative AI for Internal Audit Activities (in partnership with Wolters Kluwer)
- Demystifying AI: Internal Audit Use Cases for Applying New Technology (in partnership with AuditBoard)

> "We use AI to improve how we are doing things from an analysis standpoint, improving our work with procedures, and writing reports."

DIGITAL DISRUPTION

Key Points

Survey findings

- Fifty-three percent of North American respondents listed digital disruption (including AI) as a Top 5 risk, which was 5 percentage points higher than the global average of 48% (Exhibit 2).
- Since 2023, the percentage of North American survey respondents listing digital disruption as a Top 5 risk grew 17 percentage points (Exhibit 3).
- Much of that growth is likely driven by North America’s rapid adoption of generative AI products. Since the first practical generative AI products were introduced in late 2022, AI use has exploded.

Internal audit strategies

- Monitor and understand the risk implications of the organization’s tone on AI usage, whether aggressive or conservative.
- Push for inclusion on AI governance teams that manage deployment of AI.
- Watch for hidden risks related to AI-converted systems becoming “out of sight and out of mind.”
- Review AI workflows to ensure program leaders remain aware of what is happening within those processes.
- Ensure program leaders understand where the data fed to AI originates, where it is going, and what it is informing.
- Stay on top of all AI use cases across the organization and provide timely and relevant assurance.
- Be aware of regulations, particularly in financial services, that require independent model validation processes to ensure AI models are working as intended.
- Be bold in experimenting with AI usage to improve internal audit efficiency, and share work programs and processes where appropriate.

CONCLUSION

Rising to the Challenge

The risk landscape for 2026 is as uncertain and volatile as in the first year of the COVID crisis.

The key difference is that business and industry have not been slowed by quarantines and shifts in work patterns as they were with COVID. While geopolitical and macroeconomic disruptions have spooked markets and raised questions about inflation and slowing economic growth, new technology solutions, such as AI, offer enticing opportunities. Business leaders will need to leverage the organizational resilience and agility that are the pandemic's legacy to rise to the challenge.

"This dynamic risk landscape will undoubtedly prove challenging for many organizations, but it also presents a significant opportunity for internal auditors to demonstrate their value as objective assurance providers and insightful trusted advisors," said IIA president and CEO Anthony Pugliese. "These challenges are precisely the kinds of scenarios envisioned in The IIA's Vision 2035 report, and they highlight why it is essential for every internal auditor to embrace the responsibility of enhancing their organization's ability to create, protect, and sustain value."

In this environment, internal auditors face the twin tasks of supporting effective risk management while providing insightful advisory services that position their organizations for success. Finding the right balance will be as challenging as anything the profession has faced in a generation.

Data from the Risk in Focus survey, along with insights and observations from North American internal audit leaders, show promise for meeting these challenges. But just as C-suites and boards are emboldened to act in this time of uncertainty, so must internal audit. Digital disruption and geopolitical uncertainty allow internal audit to showcase its value and position itself as an integral player in risk management, and a trusted strategic advisor.

The coming year provides a unique opportunity to change how stakeholders think about internal audit. CAEs can seize that opportunity by thinking strategically, anticipating stakeholder needs, and delivering risk assurance and advice that is relevant, timely, and bold.

APPENDIX A: METHODOLOGY

Survey, Roundtables, and Interviews

The survey was conducted by the Internal Audit Foundation and the European Institutes Research Group (EIRG) from April 28 to June 6, 2025, and received 4,073 responses. The survey was conducted online through contacts associated with IIA Institutes and regional bodies.

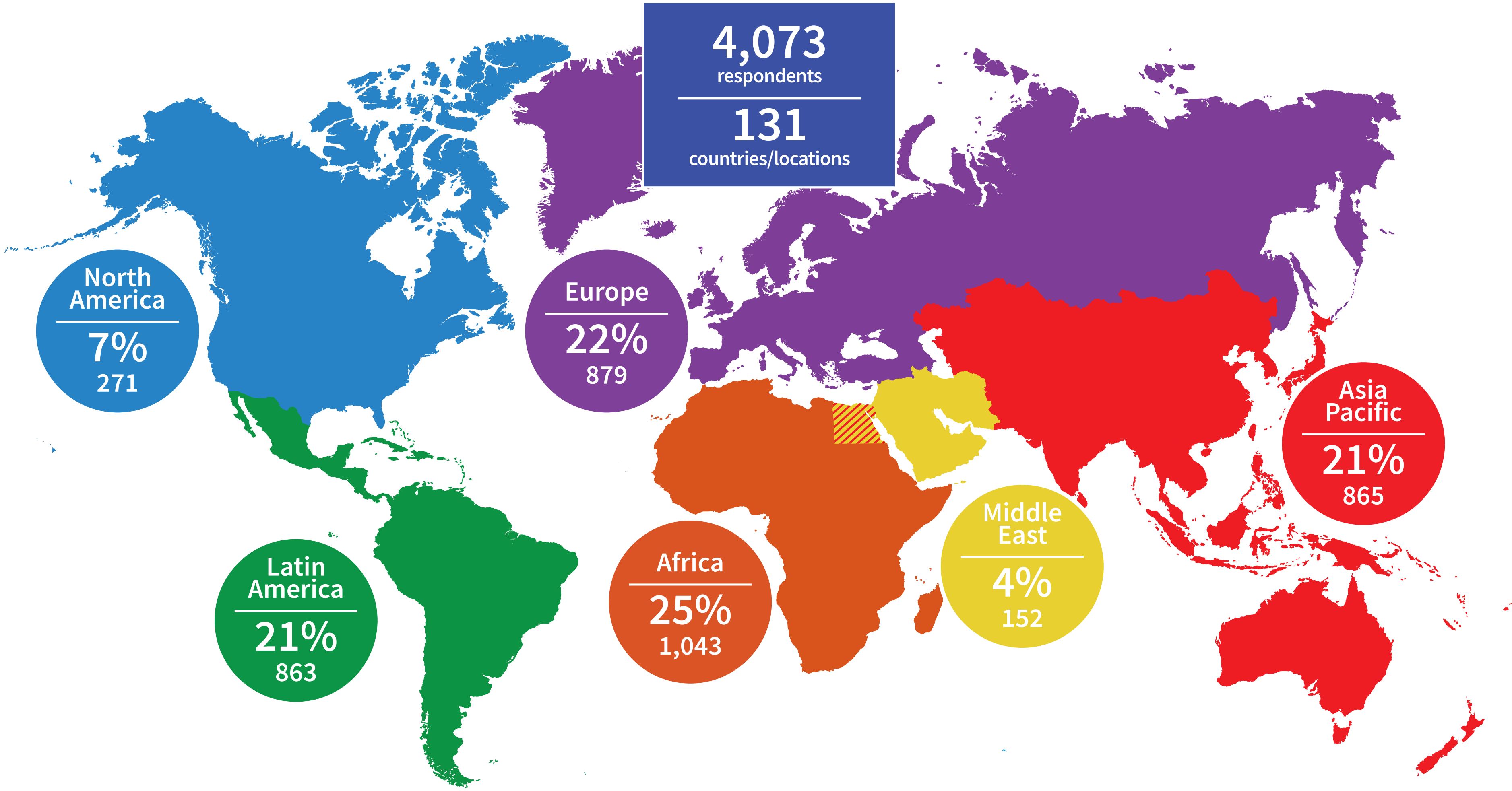
The 16 risk areas used in the survey are shown below. Respondents were asked two key questions related to these areas: What are your five highest risks, and what are the five areas where internal audit spends the most time and effort? The survey research was enhanced by roundtables and interviews with internal audit leaders in each region.

Risk areas used in the survey

Risk Name	Risk Description Used in the Survey
Business resilience	Business continuity, operational resilience, crisis management, and disaster response
Climate change/environment	Climate change, biodiversity, and environmental sustainability
Communications/reputation	Communications, reputation, and stakeholder relationships
Cybersecurity	Cybersecurity and data security
Digital disruption (including AI)	Digital disruption, new technology, and AI (artificial intelligence)
Financial/liquidity	Financial, liquidity, and insolvency risks
Fraud	Fraud, bribery, and the criminal exploitation of disruption
Geopolitical/macroeconomic uncertainty	Macroeconomic, social, and geopolitical uncertainty
Governance/corporate reporting	Organizational governance and corporate reporting
Health/safety	Health, safety, and security
Human capital	Human capital, diversity, and talent management and retention
Market changes/competition	Market changes/competition and customer behavior
Mergers/acquisitions	Mergers/acquisitions
Organizational culture	Organizational culture
Regulatory change	Change in laws and regulations
Supply chain (including third parties)	Supply chain, outsourcing, and ‘n^{th}’ party risk

APPENDIX B: DEMOGRAPHICS

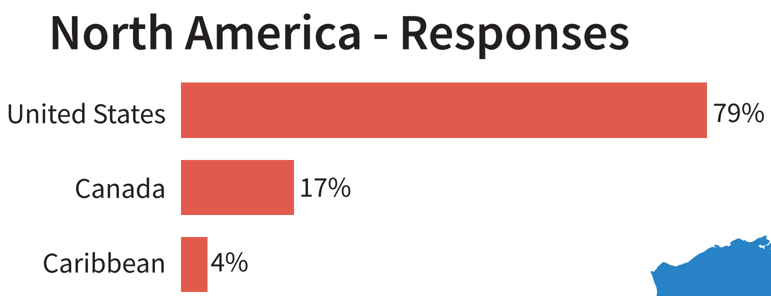
Exhibit 1. Global – Response Rate

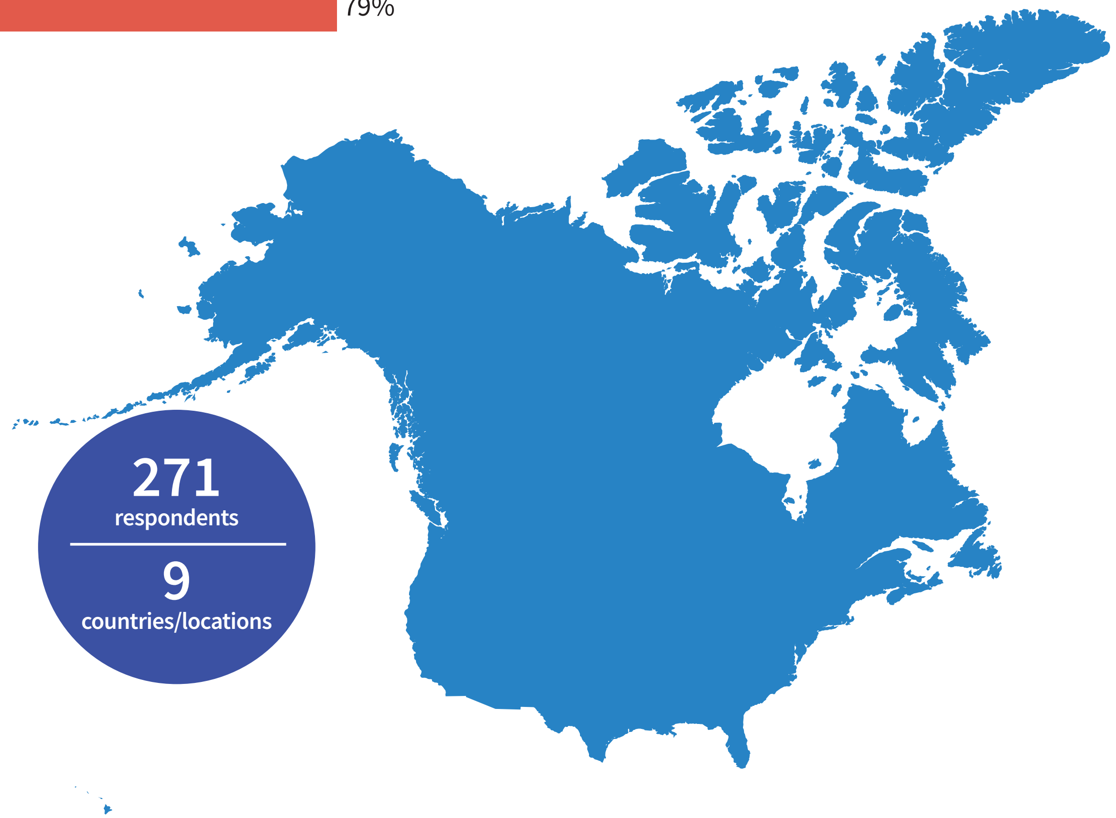


Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. n = 4,073.
Note 2: The map shows regional groups used by The IIA for operational purposes. The regional groups do not represent any political position for The IIA or IIA Institutes.
Note 3: Egypt is shaded orange and gold to show its respondents are divided between Africa and the Middle East.

DEMOGRAPHICS

Exhibit 2. North America – Responses per Country/Location





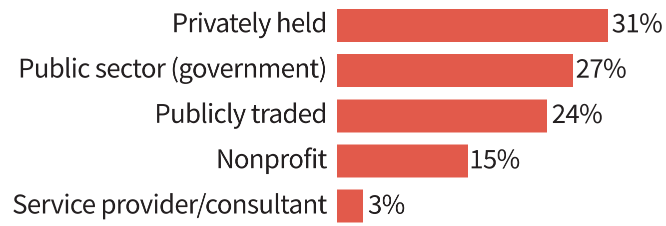
Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.
Note 2: Caribbean countries that speak English or Dutch are included with North America (including Anguilla, Antigua and Barbuda, Bahamas, Bermuda, Curaçao, Jamaica, Trinidad and Tobago. Caribbean countries that speak Spanish are included with Latin America).

DEMOGRAPHICS

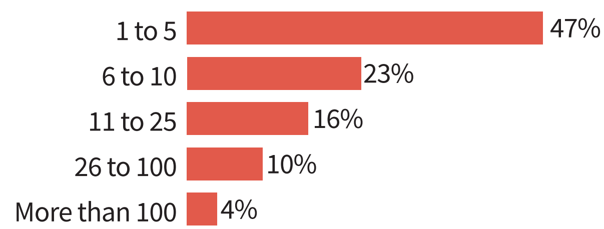
Industry, Organization Type, Size

North America – Industry

North America – Organization Type



North America – Function Size



Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.

APPENDIX C: NORTH AMERICA INDUSTRY ANALYSIS

North America – Highest Risks per Industry

Survey question: **What are the top 5 risks your organization currently faces? (Choose 5.)**

Risk area	All	Financial services	Public sector (government)	Health/social work	Education	Manufacturing	Mining/ energy/water	Professional/ technical
Cybersecurity	**86%**	**93%**	**82%**	**92%**	**87%**	**77%**	**71%**	**90%**
Digital disruption (including AI)	**53%**	**60%**	**48%**	**46%**	**48%**	**55%**	24%	**70%**
Regulatory change	**51%**	**53%**	**48%**	**62%**	**74%**	27%	**57%**	**45%**
Business resilience	**46%**	**44%**	**52%**	31%	**48%**	32%	**62%**	**65%**
Geopolitical/macroeconomic uncertainty	**45%**	37%	33%	**42%**	39%	**64%**	**48%**	**45%**
Human capital	42%	**52%**	**67%**	**42%**	35%	36%	29%	30%
Market changes/competition	34%	37%	0%	27%	26%	**59%**	**52%**	**45%**
Supply chain (including third parties)	30%	21%	18%	**62%**	9%	**55%**	**48%**	25%
Financial/liquidity	27%	36%	12%	31%	**43%**	14%	24%	25%
Organizational culture	20%	23%	39%	8%	26%	23%	14%	10%
Communications/reputation	18%	11%	45%	19%	26%	9%	5%	10%
Governance/corporate reporting	15%	15%	30%	15%	13%	9%	5%	10%
Fraud	11%	11%	12%	0%	9%	9%	5%	10%
Health/safety	8%	0%	6%	8%	17%	9%	29%	10%
Mergers/acquisitions	7%	6%	0%	12%	0%	9%	10%	10%
Climate change/environment	7%	2%	6%	4%	0%	14%	19%	0%

Highest risks per industry

If there is a tie for the fifth highest percentage, the tied percentages are highlighted in a lighter color

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.
Note 2: Industries with the highest response rates are shown. The column labeled "All" shows the average of all respondents.

NORTH AMERICA INDUSTRY ANALYSIS

North America – Highest Audit Priorities per Industry

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

Audit area	All	Financial services	Public sector (government)	Health/social work	Education	Manufacturing	Mining/ energy/water	Professional/ technical
Cybersecurity	**83%**	**86%**	**73%**	**81%**	**91%**	**82%**	**81%**	**85%**
Business resilience	**60%**	**60%**	**64%**	**50%**	**57%**	**55%**	**62%**	**65%**
Governance/corporate reporting	**53%**	**68%**	**61%**	23%	**35%**	**59%**	**62%**	**45%**
Regulatory change	**50%**	**61%**	**45%**	**58%**	**74%**	**41%**	14%	**50%**
Financial/liquidity	**44%**	**57%**	24%	**50%**	**57%**	27%	**52%**	40%
Digital disruption (including AI)	43%	**45%**	**48%**	**50%**	30%	23%	33%	**50%**
Supply chain (including third parties)	38%	32%	21%	**62%**	17%	**68%**	**67%**	30%
Fraud	30%	22%	36%	15%	30%	36%	33%	20%
Organizational culture	19%	14%	36%	19%	22%	18%	5%	20%
Human capital	15%	17%	15%	15%	13%	5%	14%	25%
Communications/reputation	15%	15%	30%	19%	9%	5%	0%	15%
Health/safety	15%	2%	27%	31%	**35%**	18%	38%	0%
Market changes/competition	13%	11%	3%	15%	9%	23%	10%	20%
Geopolitical/macroeconomic uncertainty	10%	5%	6%	4%	17%	9%	5%	30%
Mergers/acquisitions	7%	5%	0%	4%	0%	18%	14%	0%
Climate change/environment	3%	0%	0%	4%	4%	14%	10%	5%

Highest audit priorities per industry

If there is a tie for the fifth highest percentage, the tied percentages are highlighted in a lighter color

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.
Note 2: Industries with the highest response rates are shown. The column labeled "All" shows the average of all respondents.

APPENDIX D: GLOBAL REGION ANALYSIS

Highest Risks per Region

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

Risk area	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	**73%**	**62%**	**62%**	**82%**	**76%**	**72%**	**86%**
Digital disruption (including AI)	**48%**	**44%**	**39%**	**47%**	**54%**	**50%**	**53%**
Business resilience	**47%**	**49%**	**58%**	39%	35%	**58%**	**46%**
Human capital	**43%**	35%	**56%**	**48%**	**40%**	**38%**	42%
Regulatory change	**41%**	34%	38%	**45%**	**49%**	28%	**51%**
Geopolitical/macroeconomic uncertainty	38%	27%	35%	**45%**	**45%**	29%	**45%**
Financial/liquidity	31%	**43%**	19%	27%	32%	**38%**	27%
Market changes/competition	31%	19%	**49%**	32%	24%	29%	34%
Governance/corporate reporting	24%	33%	23%	20%	16%	**38%**	15%
Organizational culture	24%	29%	21%	19%	28%	26%	20%
Supply chain (including third parties)	24%	17%	28%	29%	15%	23%	30%
Fraud	23%	**43%**	20%	16%	32%	19%	11%
Communications/reputation	19%	25%	19%	12%	19%	19%	18%
Climate change/environment	18%	24%	17%	23%	25%	13%	7%
Health/safety	10%	11%	11%	12%	6%	11%	8%
Mergers/acquisitions	5%	3%	6%	5%	5%	6%	7%

Highest risks per region

If there is a tie for the fifth highest percentage, the tied percentages are highlighted in a lighter color

Note 1: The global average is calculated by summing the average from each region and dividing by the number of regions.
Note 2: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 4,073 for global.

GLOBAL REGION ANALYSIS

Highest Audit Priorities per Region

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

Audit area	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	**69%**	**60%**	**63%**	**72%**	**69%**	**69%**	**83%**
Governance/corporate reporting	**55%**	**51%**	**55%**	**58%**	**48%**	**64%**	**53%**
Business resilience	**53%**	**54%**	**57%**	**50%**	40%	**59%**	**60%**
Regulatory change	**46%**	37%	**58%**	**49%**	**53%**	30%	**50%**
Financial/liquidity	**44%**	**47%**	30%	**43%**	**51%**	**47%**	**44%**
Fraud	40%	**49%**	**42%**	37%	**51%**	30%	30%
Supply chain (including third parties)	33%	31%	32%	39%	24%	35%	37%
Digital disruption (including AI)	32%	30%	25%	29%	30%	**36%**	43%
Human capital	29%	32%	36%	27%	27%	35%	15%
Organizational culture	23%	26%	23%	21%	29%	19%	19%
Communications/reputation	18%	23%	18%	14%	21%	19%	14%
Market changes/competition	15%	13%	19%	13%	16%	14%	13%
Health/safety	15%	13%	17%	17%	12%	14%	15%
Geopolitical/macroeconomic uncertainty	11%	12%	8%	8%	16%	13%	10%
Climate change/environment	10%	14%	10%	16%	9%	8%	4%
Mergers/acquisitions	5%	3%	4%	5%	6%	4%	7%

Highest audit priorities per region

If there is a tie for the fifth highest percentage, the tied percentages are highlighted in a lighter color

Note 1: The global average is calculated by summing the average from each region and dividing by the number of regions.
Note 2: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 4,073 for global.

ACKNOWLEDGMENTS

Internal Audit Foundation Board of Trustees, 2025–26

President: Glenn Ho, CIA, CRMA
Senior Vice President: Shirley Machaba, CCSA, CRMA
Vice President, Finance and Development: Michael A. Smith, CIA
Vice President, Content: Nora Zeid Kelani, CIA, CRMA

- Subramanian Bhaskar
- Jose Gabriel Calderon, CIA, CRMA
- Hossam El Shaffei, CCSA, CRMA
- Susan Haseley, CIA
- Dawn Jones, CIA, CRMA
- Reyes Fuentes Ortea, CIA, CCSA, CRMA
- Anthony J. Pugliese, CIA

Staff liaison: Laura LeBlanc, Senior Director, Internal Audit Foundation

Committee of Research and Education Advisors, 2025–26

Chair: Nora Zeid Kelani, CIA, CRMA

- Tonya Arnold-Tornquist, CIA, CRMA
- Christopher Calvin, CIA
- Joseph Ian Canlas, CIA, CRMA
- Andrew Dahle, CIA, CRMA
- Andre Domingos
- Christina Duquette, CRMA
- Marc Eulerich, CIA
- Dagmar Flores, CIA, CCSA, CRMA
- Ivony Kudzayi Katsande, CIA, CRMA
- Ayaka Mitsunari
- Ahmed Mohammed, CIA
- Grace Mubako, CIA
- Emmanuel Pascal, CIA, CRMA
- Brad Schafer, CIA
- Brian Tremblay, CIA
- Koji Watanabe
- Stacy Wright, CIA

Staff liaison: Nicole Narkiewicz, Director, Academic and Research Strategy, Internal Audit Foundation

North America Risk in Focus Project Team

Research lead: Deborah Poulalion, Senior Manager, Research and Insights, The IIA

Project manager: Candace Sacher

Writer: Robert Perez

Graphic designers: Sergio Analco, Cathy Watanabe

North America regional liaison: Benito Ybarra, Senior Vice President, Standards and Guidance, The IIA

INTERNAL AUDIT FOUNDATION PARTNERS

DIAMOND PARTNERS

ARABCIIA
الاتحاد العربي لجمعيات المراجعين الداخليين
Arab Confederation for Institutes of Internal Auditors

AuditBoard

bakertilly

Deloitte.

The Institute of Internal Auditors

The Institute of Internal Auditors Chicago

Wolters Kluwer

Platinum Partners

African Federation of Institutes of Internal Auditors

Grant Thornton

Gold Partners

- Fundación Latinoamericana de Auditores Internos
- IIA–Houston
- IIA–Japan
- IIA–New York
- IIA–San Francisco

President's Circle (Individual Donors)

- Larry Harrington, CIA, QIAL, CRMA
- Keith Kahl, CIA, CRMA
- Doug Mims, CIA, CRMA
- Stacey Schabel, CIA
- Michael A. Smith, CIA
- Warren Stippich, CIA, CRMA

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

About the Internal Audit Foundation

The Internal Audit Foundation is the preeminent global resource, in strategic partnership with The IIA, dedicated to elevating and empowering the internal audit profession by developing cutting-edge research and programs. The Foundation helps current and future internal auditors stay relevant by building and enhancing their skills and knowledge, ensuring organizations are equipped to create, protect, and sustain long-term value. For more information, visit theiia.org/Foundation.

Disclaimer and Copyright

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Internal Audit FOUNDATION

Global Headquarters | The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, USA
Phone: +1-407-937-1111 | Fax: +1-407-937-1101
Web: theiia.org/Foundation

Office of the General Auditor note:
The original IIA document contained only 41 pages, not 42 as indicated on the previous page.

2026 EDITION

UNLOCKING OPPORTUNITY

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

NC STATE Poole College of Management
Enterprise Risk Management Initiative

Table of contents

Introduction

Successful companies view even challenging times as catalysts for innovation and growth, actively seeking opportunities where others see obstacles.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organizations balancing risk management with a strong focus on seeking growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity. Accordingly, our discussions of risks are framed contextually with a high-level focus on opportunity with the intention to enhance the discussion of risk by linking it to value-creating initiatives.

This report — our **14th annual edition** — contains insights from 1,540 board members and C-suite executives around the world regarding their perspectives on:

- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organizations;
- The top risks on the horizon for the near-term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long-term (a decade from now) related to 12 risk themes that consider the strategic and operational near-term risks; and
- A discussion of their organizations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. As in the past, the report provides analyses across organizations of different sizes, industries, geographic regions, as well as the executive positions held by the respondents (board members, CEOs, CFOs, etc.).

The key findings in this report provide useful insights for board members and senior executives to benchmark their organization's opportunities and risks against those on the minds of other executive leaders around the world. Our hope is that this report will foster meaningful dialogue and discussion among an organization's leaders as they seek to create strategic value in these challenging times.

Executive summary

Notwithstanding several years of uncertainty and shifting geopolitical and economic dynamics, our results indicate that business leaders are ready to act and are embracing innovation, strategic partnerships and long-term planning to drive transformation and realize growth opportunities. The biggest risk organizations face today is doing nothing.

In brief: what you need to know

There is strong optimism for revenue growth over the next two to three years. Nearly seven in 10 board members and executives (69%) agree somewhat to completely that, considering current conditions, there are significant opportunities to increase revenues over the next two to three years.

Ecosystem expansion is a strategic priority. More than six in 10 leaders (62%) indicate their organizations plan to expand their strategic alliances and partnerships over the next two to three years.

AI is both a transformative growth driver and a complex challenge. AI is a long-term strategic priority, with 31% of leaders focused on integrating it into current technologies and business processes. AI ranks sixth among near-term global risks, while concerns about IT infrastructure performance have risen to the fourth-rated risk this year versus 13th last year. Thus, while AI is seen as a transformative growth enabler, IT infrastructure and talent readiness present major barriers to its effective deployment and realizing its full benefits. Cybersecurity risks linked to AI also remain top of mind.

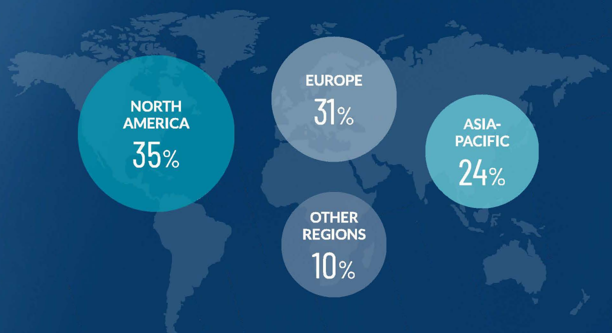
Cybersecurity is the top global risk and investment priority. Not only are cyber threats ranked as the top global near-term risk, but third-party risks (which are linked to cyber concerns) rank second. Cybersecurity also stands out as the top investment priority for organizations to address near-term risk issues. Interestingly, there are geographical distinctions in rating these risks.

Talent challenges are evolving but not disappearing. Talent risks continue to be at the forefront among board members and C-suite leaders globally, with issues surrounding workforce upskilling and the availability of skilled labor remaining significant, particularly given the expected impact of AI on job roles and workforce transformation.

Concerns about the economy and trade-related challenges and their impact on global markets are top 10 near-term risk concerns. Trade-related challenges entered the top 10 list as the 10th-rated risk for this year, while uncertainties linked to interest rates and inflation continue to create reason for pause among respondents.

Customer experience, cyber and AI are top long-term strategic focus areas. Organizations are prioritizing customer and competition dynamics, security and privacy, and AI deployments in their long-term strategies, indicating a shift toward integrated decision-making that encompasses both immediate and future opportunities and risks.

Snapshot of key findings



Number of respondents = 1,540

Top global near-term risks

2026 rank	Risk issue	Average*	2025 rank
1	Cyber threats	3.39	2
2	Third-party risks	3.16	7
3	Adopting new/emerging technologies elevates need to upskill/reskill workforce	3.06	9
4	Operations/legacy IT unable to meet expectations	3.05	13
5	Economic conditions	3.05	1

** Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."*

There is optimism for potential growth opportunities

- 69% Revenue potential
- 62% Ecosystem development
- 52% Geographic expansion

Based on a five-point scale assessing agreement/disagreement.
Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

Top 3 priorities – impact of AI

- Data for AI use/cyber exposure: 31%
- Integrating AI in enterprise: 31%
- Equipping workforce to realize AI's value proposition: 29%

Top 3 investment areas

- Cybersecurity: 43%
- Business process improvements: 35%
- Infrastructure modernization: 33%

Top 3 long-term challenges

- Customers and competition: 42%
- Security and privacy: 40%
- AI deployments: 39%

Differences across respondent groups

In the following pages, we offer analysis and insights based on subsets of the full survey sample, including breakdowns by executive position, industry group, geographic region and organization size. These subsets are defined below.

Executive position

Position	Number of respondents	Percentage of sample
Board Member (Board)	94	6%
Chief Executive Officer (CEO)	62	4%
Chief Financial Officer (CFO)	314	20%
Chief Operating Officer (COO)	236	15%
Chief Information/Technology Officer (CIO/CTO)	211	14%
Chief Information Security Officer (CISO)	115	7%
Chief Human Resources Officer (CHRO)	24	2%
Chief Risk Officer (CRO)	159	10%
Chief Audit Executive (CAE)	168	11%
Chief Strategy/Innovation Officer (CSO)	18	1%
Chief Data/Digital Officer (CDO)	10	1%
Chief Legal Officer/General Counsel (CLO)	12	1%
Other C-Suite (OCS)	44	3%
All other	73	5%

Industry group

Industry	Number of respondents	Percentage of sample
Financial Services (FS)	325	21%
Consumer Products and Services (CPS)	241	16%
Manufacturing and Distribution (MD)	216	14%
Technology, Media and Telecommunications (TMT)	167	11%
Aerospace and Defense (AD)	125	8%
Healthcare (HC)	142	9%
Energy and Utilities (EU)	117	8%
Government (GOVT)	127	8%
Not-for-Profit/Higher Education (NFP/HE)	59	4%
Other industries (not separately reported)	21	1%

Geographic region

Region	Number of respondents	Percentage of sample
North America	536	35%
Latin America	87	6%
Europe	479	31%
Middle East and Africa	68	4%
India	87	6%
Asia	207	13%
Australia and New Zealand	76	5%

Organization size

Organization size	Number of respondents	Percentage of sample
Largest organizations: Revenues of $10 billion or greater; assets or budget under management $50 billion or more	363	24%
Medium-to-large organizations: Revenues $1 billion to $9.99 billion; assets under management $10 billion to $49.99 billion; budget under management $5 billion to $49.99 billion	586	38%
Small-to-medium organizations: Revenues $100 million to $999.99 million; assets under management $1 billion to $9.99 billion; or budget under management $500 million to $4.99 billion	406	26%
Smallest organizations: Revenues less than $100 million; assets under management less than $1 billion; budget under management less than $500 million	185	12%

03

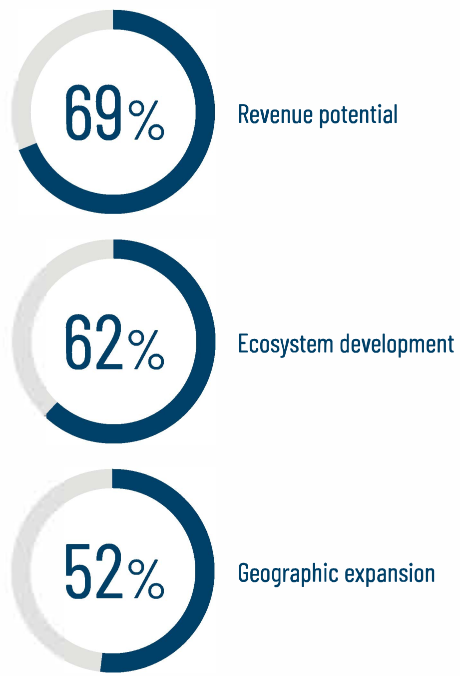
Opportunities for enterprise growth

We asked respondents to rate the level of their agreement with the following three statements about strategic growth opportunities over the next two to three years using a five-point Likert scale ranging from 1=Disagree completely to 5=Agree completely.

- **Revenue potential:** Current macroeconomic conditions notwithstanding, there are significant opportunities to grow our revenues.
- **Ecosystem development:** There are significant opportunities to expand our ecosystem of strategic alliances and partnerships to enhance how we go to market.
- **Geographic expansion:** There are significant opportunities to grow our business in markets other than our headquarters' domestic market.

Figure 1 summarizes the overall level of agreement with each of these statements from the full sample of 1,540 respondents:

Figure 1: Views about opportunities for growth



Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

There is **strong confidence in revenue growth potential,** with 69% of respondents expressing agreement ("Agree completely" or "Agree somewhat") with this statement, the highest among the three statements. Respondents express a strong belief that **revenue growth opportunities exist despite the headwinds their organizations face,** whether it be the economy, geopolitical developments or other matters. This suggests that many organizations are maintaining a forward-looking posture, unlocking opportunities to innovate, expand offerings or capture market share even in uncertain environments. These findings highlight the importance of exploring growth avenues while ensuring that risk-adjusted returns are considered when making capital allocation decisions.

Ecosystem development is seen as a means of unlocking opportunity, with it receiving the second-highest response, 62%. Ecosystems are powerful enablers to helping organizations outperform traditional, isolated business models by fostering interconnected networks that drive innovation and value. Collaboration among ecosystem participants facilitates the sharing of ideas, technologies, capabilities and access that support rapid co-innovation, expanded market reach, and operational efficiency and agility, allowing participants to achieve revenue growth and other outcomes that would be difficult or impossible for any single organization to accomplish alone. Our survey findings reflect optimism about **expanding strategic alliances and partnerships**, indicating that many organizations view the development of these relationships as a key enabler of success. Leaders should assess whether they are fully leveraging external relationships for co-innovation, data sharing and platform integration, among other opportunities.

Geographic expansion is viewed with more caution given there was a lower level of agreement — 52% — among respondents. This finding suggests **more tempered enthusiasm for international or cross-border growth.** This may reflect concerns about trade policies, geopolitical instability, regulatory complexity or uneven recovery across global markets. Directors and executives should probe whether strategies for growth in foreign markets are being pursued with consideration of the opportunities and risks, especially in light of shifting trade policies and regional dynamics, and are supported by robust digital platforms.

Overall implications

These findings suggest that while executives are generally optimistic about growth, they are prioritizing **strategic partnerships and core market expansion** over aggressive geographic moves as they look over the near-term horizon to enhance operational readiness, strategic clarity and competitive advantage. Furthermore, a digital world minimizes the importance of a physical footprint due to the efficiencies, capabilities and flexibility offered by virtual tools, cloud infrastructure and digital platforms. That said, half of the survey respondents overall expressed a priority to grow business in foreign markets.

The following tables summarize respondent views about opportunities for growth across different executive positions and across organizations of different sizes, industries and geographies.[1]

Table 1: Views about opportunities for growth — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Revenue potential	81%	68%	71%	68%	73%	71%	46%	62%	66%
Ecosystem development	65%	55%	65%	61%	67%	68%	67%	60%	59%
Geographic expansion	63%	61%	50%	49%	55%	56%	46%	51%	51%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

[1] In Tables 1-4, we have highlighted in darker blue those statements for which 66% or more of respondents are in agreement that they represent strategic growth opportunities for their organizations; statements for which 50%-65% of respondents are in agreement are highlighted in medium blue, while those for which less than half of respondents are in agreement are highlighted in turquoise.

Board members have the highest level of optimism regarding revenue potential. This may be due to the board's role to challenge management to pursue ambitious goals and think expansively. Boards receive summarized, high-level reports that emphasize strategic wins and growth initiatives. Accordingly, board members may not have the same level of transparency into the operational realities that executives manage day-to-day. In addition, directors serving on multiple boards may be positioned to bring a broader perspective to strategic conversations in the boardroom.

The focus on opportunities to expand the ecosystem of strategic alliances and partnerships to enhance go-to-market strategies is relatively consistent in the boardroom and across the C-suite. The higher interest of directors and CEOs than anyone else in the C-suite in pursuing significant opportunities to grow in foreign markets suggests a sharper focus on their respective roles as stewards of the company's vision, growth and long-term value.

In viewing the results across organization size, the two largest groups of organizations show the most optimism, though all see positive signs and opportunities, particularly in terms of revenue potential and ecosystem development.

Table 2: Views about opportunities for growth – by organization size

	Largest organizations	Medium-to-large organizations	Small-to-medium organizations	Smallest organizations
Revenue potential	74%	72%	62%	65%
Ecosystem development	66%	63%	60%	60%
Geographic expansion	60%	54%	44%	48%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

Regarding the different views on growth opportunities across geographies (see Table 3), organizations in Australia and New Zealand are less bullish than other regions, likely because this year's respondents from the region have a markedly different mix, including government and mining. That said, the top 10 near-term risks overall are largely the same and the long-term risks overall are identical, with and without inclusion of the respondents from this region.

The focus on revenue potential is typically higher in North America, Latin America and India than in Europe and Asia due to a combination of factors — market growth opportunities, economic conditions, favorable consumer demographics, evolving regulatory environments and competitive opportunities. These factors generally contrast with the greater maturity and saturation in many parts of Europe and some developed parts of Asia, particularly Japan. To illustrate:

- India is projected to be the fastest-growing major economy, outpacing China, the U.S. and the EU.
- Latin America has a predominantly young and skilled labor force with a rapidly expanding middle class, driving increased consumption. In contrast, many European and some Asian nations face challenges with aging populations.
- In North American companies, the higher level of revenue growth optimism than, say, Europe and Asia likely stems, at least in part, from a more risk-embracing corporate culture, a more dynamic market-based financial system

that encourages investment, and investor expectations that prioritize growth and innovation. The U.S. market is a magnet for global investment, including substantial capital from European and other foreign investors, which drives high valuations and provides ample funding for growth.

- While markets in Europe are often considered mature and highly competitive, regions like Latin America and India offer a wide range of untapped opportunities in sectors such as digital services, infrastructure and financial services.

The heightened interest in ecosystem development in North America and Latin America is driven by dynamic market growth, innovation-friendly environments, generally supportive policies and the need for collaborative solutions to address complex challenges. While some of these factors exist in other regions, their combination creates an ideal landscape for ecosystem models to flourish, enabling organizations to unlock new opportunities, drive innovation and achieve sustainable growth.

Table 3: Views about opportunities for growth – by geographic region

	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Revenue potential	75%	79%	65%	71%	83%	67%	34%
Ecosystem development	67%	75%	60%	63%	58%	63%	34%
Geographic expansion	58%	52%	51%	56%	56%	49%	16%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

As for growing business in foreign markets, we continue to point out that in a digital world, the need for physical expansion is reduced. The emphasis on pursuing opportunities in foreign markets is generally consistent across geographies, with a slight uptick in North America, where the focus on foreign markets has always been strong. Developed markets in North America and Europe have been the traditional centers of innovation and revenue. However, these markets are now often described as more mature, with higher saturation and complexity, pushing companies to look to new epicenters of growth in emerging regions for significant expansion. As emerging markets liberalize investment laws and actively create favorable environments to stimulate international trade and investments, they become more attractive for foreign companies.

The heightened interest in ecosystem development in North America and Latin America is driven by dynamic market growth, innovation-friendly environments, generally supportive policies and the need for collaborative solutions to address complex challenges.

The emphasis on revenue growth remains largely uniform across industry groups, with the exception of Energy and Utilities and Government. While a reduced focus in the Government sector may be anticipated, the pattern observed within Energy and Utilities is notable, considering the growth prospects associated with increased energy demand driven by data centers. Differences in attention to ecosystem development across industry groups can be attributed to various factors, particularly the view that sustainable growth, ongoing innovation and competitive advantage are increasingly reliant on collaboration and interdependence. Sectors that adopt an ecosystem-oriented approach are generally more equipped to respond to disruption, enhance customer value and secure long-term success. This context may explain the comparatively lower focus observed within Government and Energy and Utilities, as these organizations face less exposure on these fronts.

The focus on growing foreign business is relatively consistent across industry groups, with two exceptions. Understandably, these exceptions are Government and Energy and Utilities.

Table 4: Views about opportunities for growth – by industry group

	AD	CPS	EU	FS	GOVT	HC	MD	NFPHE	TMT
Revenue potential	79%	71%	61%	72%	50%	76%	68%	41%	76%
Ecosystem development	72%	63%	58%	66%	53%	60%	62%	62%	63%
Geographic expansion	59%	56%	40%	55%	31%	58%	55%	34%	57%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

> Differences in attention to ecosystem development across industry groups can be attributed to various factors, particularly the view that sustainable growth, ongoing innovation and competitive advantage are increasingly reliant on collaboration and interdependence.

04

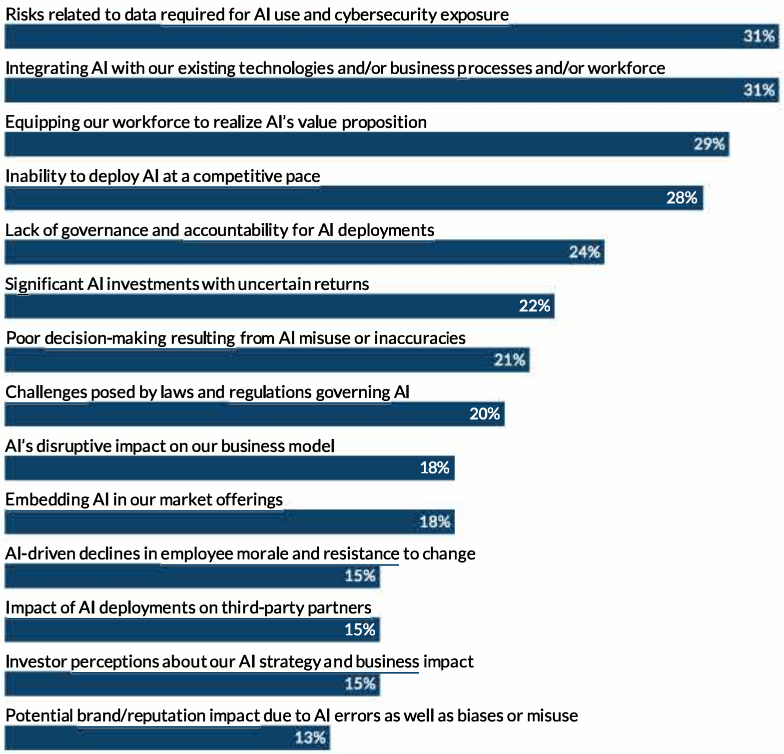
Transformative impact of AI

AI is a critical component to unlocking efficiency, personalization, new innovations and the ability to scale — all drivers of new revenue streams and expansion. As organizations increasingly integrate AI into their core strategies, they are discovering new ways to optimize operations, enhance customer engagement and stay ahead of competitors in a rapidly evolving marketplace. But AI also introduces governance challenges.

The impact of AI is interwoven throughout a number of the top risks on the minds of executives for both near-term and long-term risk horizons. Given the importance of AI capabilities to enabling growth strategies and their rapid deployment, we asked respondents to provide their perspectives about the impact of AI on their organizations over the next two to three years. Specifically, we asked them to select their three most important priorities from a list of 14 potential AI risk issues.

Figure 2 summarizes the percentage of times each AI risk was included as one of the respondents' top three AI risk concerns. As shown, "Risks related to data required for AI use and cybersecurity exposure" and "Integrating AI with our existing technologies and/or business processes and/or workforce" were included most often among the top three AI risk issues for respondents (31%).

Figure 2: Which of the following issues reflect your organization's most significant priorities regarding the impact of AI on your business over the next 2-3 years?



Percentages reflect frequency with which each area was selected among the top three.

These results reveal a unified, yet complex, perception of AI deployment risk over the next two to three years. The primary focus is not on existential threats but on **foundational organizational and operational risk.** The collective consensus points to an overwhelming prioritization of three core challenges:

- Security and data integrity
- Seamless operational integration
- Talent and skills readiness

These concerns underscore a critical tension in the current enterprise AI adoption cycle: The risk of failing to integrate AI effectively and responsibly into existing processes, technologies and workflows is seen as equally pressing as the risk of fundamental security failure. Executives are concerned that poor integration, combined with an ill-equipped workforce, will neutralize any value proposition and competitive advantage that can be gained from AI investments, all while exposing the organization to heightened data and cyber threats.

While risks associated with making "significant AI investments with uncertain returns" and "poor decision-making resulting from AI misuse or inaccuracies" are also high-ranking, our analysis of key findings across executive positions, industry groups and regions reveals that the current risk agenda is dominated by product/service delivery and enterprise defense, signaling a transition from experimental AI investment to operational necessity. A tailored, integrated strategy addressing technology, talent and cyber governance simultaneously will be the defining characteristic of high-performing organizations in the AI era.

Overall implications

The full sample results provide a definitive baseline, grouping the most pressing AI risks into three strategic focus areas that occupy the executive agenda: operationalization of AI, playing defense, and the pace of adoption and utilization. With a near-unanimous focus, C-suite leaders acknowledge that the primary hurdle for AI is not technological capability but organizational change.

- **AI integration** being tied for the top spot highlights a shift away from pilot projects toward embedding AI into the fabric of the enterprise. This risk is intrinsically a complex challenge, involving the fusion of new algorithmic logic with legacy systems and deeply entrenched human workflows. Failure to address the integration challenge means AI investments become "shelf-ware," creating fragmented, difficult-to-scale solutions that defeat the purpose of deploying AI.

- **Talent readiness** closely follows, recognizing that AI's return on investment (ROI) is contingent on human capability. This risk is a stark acknowledgment that simply purchasing AI tools is insufficient; organizations must invest in upskilling, new roles and a cultural shift where AI is a collaborative co-worker, not merely a tool. The bottom line: Properly implemented, AI becomes an extension of the workforce.

Playing defense represents security, ethical and compliance non-negotiables that must underpin any AI initiative.

- **Security and data** (31%) is the most-cited risk, signaling executives' understanding that AI models are fundamentally new attack surfaces. This risk extends beyond traditional cybersecurity to encompass model poisoning, data leakage during training and inference, and the ethical use of massive, sensitive datasets. No AI deployment can succeed without addressing the data lifecycle from acquisition to decommissioning.

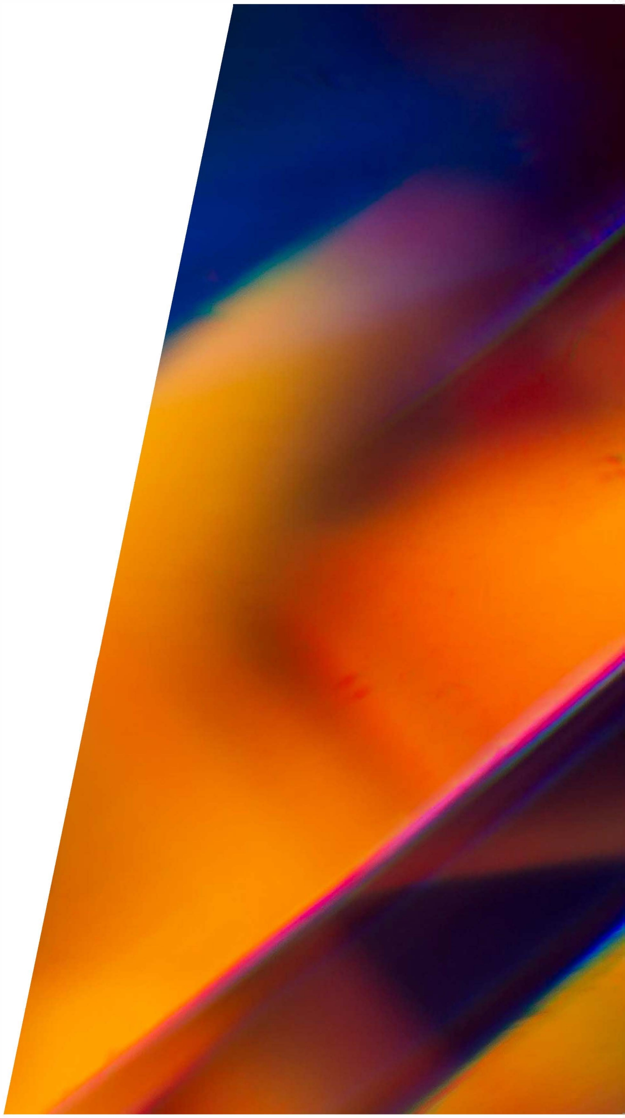
- **Governance and accountability** (24%) indicates that a quarter of all respondents foresee the risk of a direct failure of organizational control. This risk speaks to the difficulty of establishing clear ownership for AI outputs, ensuring traceability and transparency, and providing appropriate human oversight, especially as systems' decision-making and actions become more autonomous.
- The **evolving regulatory landscape** (20%) reveals that the challenges posed, as new laws and regulations governing AI emerge, are of significant concern to executives as they continue down the path to AI implementation and reliance on outputs from AI deployment.

The risks related to competitive speed and financial efficacy reflect market pressures.

- **Competitive pace** (28%) shows a strong fear of falling behind competitors, treating AI deployment as a strategic race. This gives rise to FOMO (fear of missing out) because proprietary AI deployments are not easily replicated capabilities when they involve unique, protected technologies and processes owned by an organization, giving them exclusive rights and competitive advantage.
- **Uncertain returns** (22%) serve as the counterpoint: A significant portion of leaders fear that this rapid race **will** result in expensive failures, leading to stranded assets and a loss of confidence from the board and investors. This concern suggests a need to proceed with clear objectives, quality data sources, the right technology, pilots and testing, and continuous evaluation and monitoring to keep implementations on track.

The overall full sample picture is one of practical, immediate concern: Executives are focused on **execution risks** first and **existential risks** second, as governance and controls struggle to keep pace with the dual demands of implementation speed and seamless integration.

No AI deployment can succeed without addressing the data lifecycle from acquisition to decommissioning.



Perspectives on impact of AI across selected respondent groups

Table 5: Top three AI risk issues — by executive position*

Risk	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Risks related to data required for AI use and cybersecurity exposure	35%	29%	25%	27%	23%	32%	17%	40%	42%
Equipping our workforce to realize AI's value proposition	45%	42%	21%	25%	22%	21%	42%	33%	36%
Integrating AI with our existing technologies and/or business processes and/or workforce	33%	52%	22%	18%	20%	15%	33%	53%	48%
Inability to deploy AI at a competitive pace	25%	27%	29%	23%	30%	19%	33%	40%	31%
Significant AI investments with uncertain returns	18%	19%	28%	24%	23%	23%	4%	18%	16%
Lack of governance and accountability for AI deployments	17%	29%	20%	20%	19%	23%	17%	30%	42%
Challenges posed by laws and regulations governing AI	12%	19%	21%	23%	26%	25%	38%	14%	12%
AI-driven declines in employee morale and resistance to change	15%	6%	17%	20%	23%	24%	38%	7%	5%
Embedding AI in our market offerings	18%	21%	21%	25%	17%	21%	0%	7%	12%
Impact of AI deployments on third-party partners	12%	5%	25%	18%	18%	24%	12%	7%	9%
Investor perceptions about our AI strategy and business impact	16%	5%	18%	22%	24%	20%	29%	4%	3%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

A deeper dive into the data reveals that executive perception of AI risk is heavily modulated by functional accountability, resulting in distinct risk profiles across the C-suite.

CEOs, board members and COOs — the roles most responsible for overall strategic outcomes and operational delivery — demonstrate a strong consensus around the **operationalization imperative**.

- **CEOs** prioritize **integration**, followed by **workforce** and then **governance**. This profile reflects the three pillars of executive focus: ensuring the system works to make the business operate better, smarter and faster; ensuring people can use it; and ensuring it is managed, controlled and secured.

- **COOs** mirror this concern with **cyber/data risk** being their top concern, followed by the emerging risk of **embedding AI in market offerings**, and then **workforce**. This indicates that operational leaders are on the front lines focusing on data security as AI is implemented and how the deployment will translate into new products.

Both CFOs and CIOs/CTOs are focused on the financial physics of AI: speed versus investment risk.

- **CFOs** prioritize **competitive pace** and **uncertain returns** as their top two concerns. The CFO's primary mandate is capital stewardship, and the data reflects their concern about the uncertain duration of AI investments. The third risk, **impact of AI on third-party partners**, underscores concern over extended enterprise risk and supply chain financial liability. **Cyber/data**, the exposure to security threats, closely follows third-party risk concerns.

- **CIOs/CTOs** exhibit a hybrid profile, prioritizing **competitive pace** but immediately followed by **legal and regulatory challenges related to governing AI.** Technology leaders recognize that the pressure to deploy quickly heightens the exposure to risk. Their focus on **regulations** as a concern indicates the need to future-proof technology deployments against evolving compliance frameworks.

The CRO and CAE roles focus on systemic control matters.

- Interestingly, **CROs** and **CAEs** rank **integration** as their top concern, recognizing that a poorly integrated system falls short of realizing the expected value. CROs' subsequent concerns are **competitive pace** and **cyber/data**, highlighting a triple threat: a rush to implement, poor organizational integration and the resulting exposure to security threats. CAEs are also concerned with **cyber/data** and, to no surprise, governance.

> Executive perception of AI risk is heavily modulated by functional accountability, resulting in distinct risk profiles across the C-suite.

Table 6: Top three AI risk issues — by industry group

Risk	AD	CPS	EU	FS	GOVT	HC	MD	NFPHE	TMT
Risks related to data required for AI use and cybersecurity exposure	21%	39%	32%	24%	27%	41%	31%	41%	38%
Integrating AI with our existing technologies and/or business processes and/or workforce	15%	42%	42%	24%	16%	38%	34%	44%	42%
Equipping our workforce to realize AI's value proposition	23%	38%	37%	22%	19%	33%	33%	34%	44%
Inability to deploy AI at a competitive pace	29%	29%	29%	30%	28%	24%	30%	42%	29%
Significant AI investments with uncertain returns	29%	18%	19%	27%	17%	20%	23%	19%	18%
Impact of AI deployments on third-party partners	27%	11%	8%	24%	19%	11%	12%	10%	5%
Challenges posed by laws and regulations governing AI	20%	12%	20%	23%	29%	18%	18%	15%	14%
AI-driven declines in employee morale and resistance to change	20%	9%	8%	18%	28%	13%	15%	7%	10%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each industry group are highlighted in blue (ties included).

AI risk perception is sharply defined by the regulatory, trust and business model characteristics of each industry group. In industries where data sensitivity and public trust are paramount, **data and security** often dominate the risk agenda. In industries focused on high-volume transactions, product development and supply chain efficiencies, the **organizational agility** theme often emerges.

- Four industry groups — **Consumer Products and Services, Energy and Utilities, Healthcare,** and **Technology, Media and Telecommunications** — rank the same risks in their top three AI-related concerns: **integration, cyber/data** and **workforce**, with **integration** the top issue for three of the four groups.

- **Cyber/data** is a top three concern overall for the above four industry groups as well as **Financial Services** and **Manufacturing and Distribution.** This is a clear reflection of the catastrophic potential of a data breach or a cyber attack involving critical national infrastructure, sensitive operations or highly protected personally identifiable information. For these sectors, while AI is viewed as a *value creator*, it is also viewed as an *enabler of risk*.

- In addition to **cyber/data, Manufacturing and Distribution** ranks **workforce** and **competitive pace** as significant concerns. For the creators and primary users of AI in these companies, the focus is on fast, controlled and secure deployment through skilling employees expected to leverage AI-powered agents and tools.

- In addition to **cyber/data, Financial Services** reports **competitive pace, uncertain returns, integration** and **impact of AI on third-party partners.** This suggests that financial institutions have accepted the risks related to data required for AI use and cybersecurity exposure as a baseline cost of doing business and are now primarily focused on how quickly and effectively they can realize value by replacing human-driven processes with AI-optimized ones.

- Both **Aerospace and Defense** and **Government** rank **competitive pace** among their top three concerns. Aerospace and Defense also lists **uncertain returns** and **impact of AI on third-party partners** in their concerns, with Government listing **regulations** and AI's **impact on organizational culture**. These industries are heavily reliant on large, decentralized operational workforces (e.g., retail, factory floors, logistics) and recognize that the success of AI hinges on empowering, not alienating, their human capital through targeted upskilling and seamless system integration.

The **Not-for-Profit/Higher Education** sector leads with **integration,** followed by **competitive pace** and **cyber/data** as their top AI risk concerns. For mission-driven organizations that face ongoing challenges for talent and resources, AI integration with existing systems and deployment at a competitive pace are understandable concerns.

> In industries where data sensitivity and public trust are paramount, data and security often dominate the risk agenda. In industries focused on high-volume transactions, product development and supply chain efficiencies, the organizational agility theme often emerges.

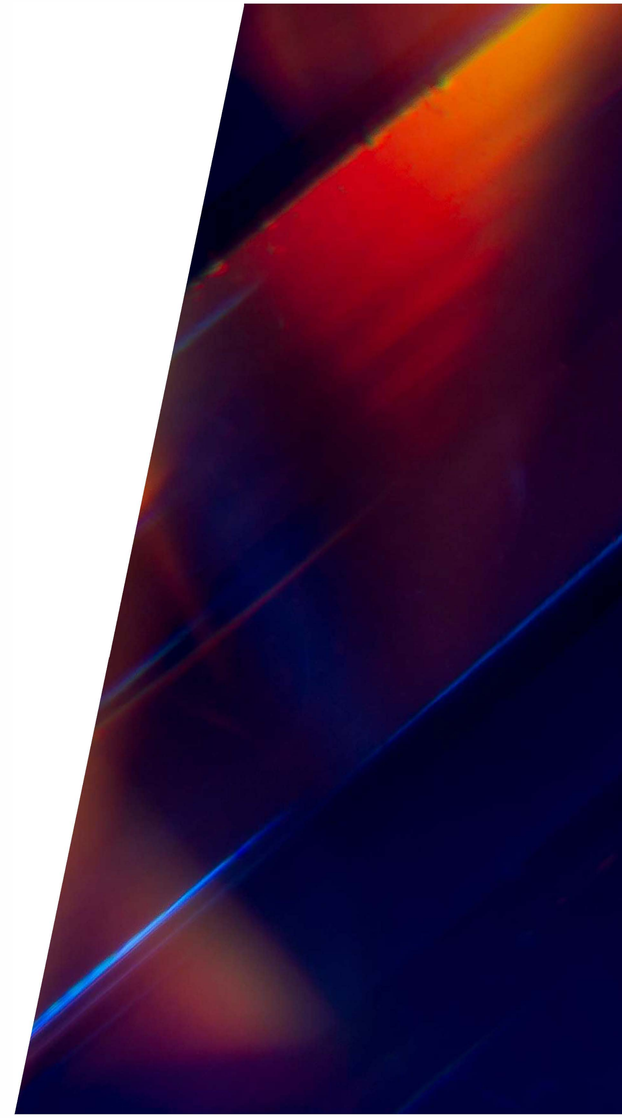


Table 7: Top three AI risk issues — by geographic region

Risk	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Risks related to data required for AI use and cybersecurity exposure	34%	29%	26%	26%	44%	34%	22%
Integrating AI with our existing technologies and/or business processes and/or workforce	38%	30%	26%	34%	28%	29%	15%
Inability to deploy AI at a competitive pace	28%	38%	28%	31%	21%	30%	29%
Equipping our workforce to realize AI's value proposition	32%	32%	23%	25%	20%	43%	26%
Significant AI investments with uncertain returns	19%	17%	26%	25%	23%	17%	30%
Poor decision-making resulting from AI misuse or inaccuracies	22%	8%	23%	15%	29%	13%	29%
Embedding AI in our market offerings	16%	25%	15%	26%	15%	21%	25%
Lack of governance and accountability for AI deployments	24%	25%	22%	25%	19%	30%	22%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each region are highlighted in blue (ties included).

AI risk is also perceived through a regional, geographic lens, reflecting local economic development, regulatory environments, and political and labor market characteristics.

In **North America** and the **Middle East and Africa (MEA)**, the top priority is **integration**.

- **North America** reflects a sophisticated, rapidly adopting market where the focus has moved beyond *whether* to use AI to *how* to assimilate it into complex corporate structures and make its deployment effective and responsible via talent and security measures.
- **MEA** shows a focus on rapid **integration** combined with a high fear of being outpaced, suggesting these countries view AI as a critical enabler of immediate competitive growth and are willing to take on deployment risk to achieve it.

Europe and **Australia and New Zealand (ANZ)** show a distinct focus on the financial and strategic value of AI.

- **Europe** and **ANZ** both place **competitive pace** and **uncertain returns** high on their list. This is likely driven by a combination of high regulatory oversight (especially in Europe) and a cultural focus on strategic, controlled investment, where the financial justification of technology is scrutinized rigorously. The recognition of the risk of **poor decision-making** in ANZ suggests a greater concern with the reliability and output quality of deployed AI systems.

India and **Asia** present a profile defined by large populations, rapid digital transformation and a high sensitivity to systemic failures.

- **India** is the only region to prioritize **cyber/data** and **poor decision-making** as its top two concerns. This unique pairing suggests a deep concern over the integrity and reliability of AI systems handling massive volumes of new digital data, where errors can have immediate, cascading effects across large-scale services.

Asia prioritizes **workforce**, recognizing that the scale of AI adoption demands an enormous and rapidly trained talent base. The combination of this region's top three issues underpins a struggle to train people rapidly and secure data while keeping up with the competitive pace of the region.

Additional subgroup analyses

For brevity, we have omitted tabulation of AI risk concerns for our two remaining subgroups: organization size and type.

The size and organizational maturity of the enterprise significantly shape the risk outlook, distinguishing between organizations focused on managing immense complexity and those focused on securing competitive viability.

The largest organizations are defined by complexity and scale. Their top AI risk concern is **cyber/data**. The sheer volume and sensitivity of data managed by these global giants make the risk related to AI use and cybersecurity exposure an exponentially increasing one, meaning the widespread impact of AI systems and their potential for errors and omissions can accumulate over time without a human in the loop. Their second and third concerns, **workforce** and **integration**, reflect the challenge of driving massive, systemic change across global divisions and legacy IT systems.

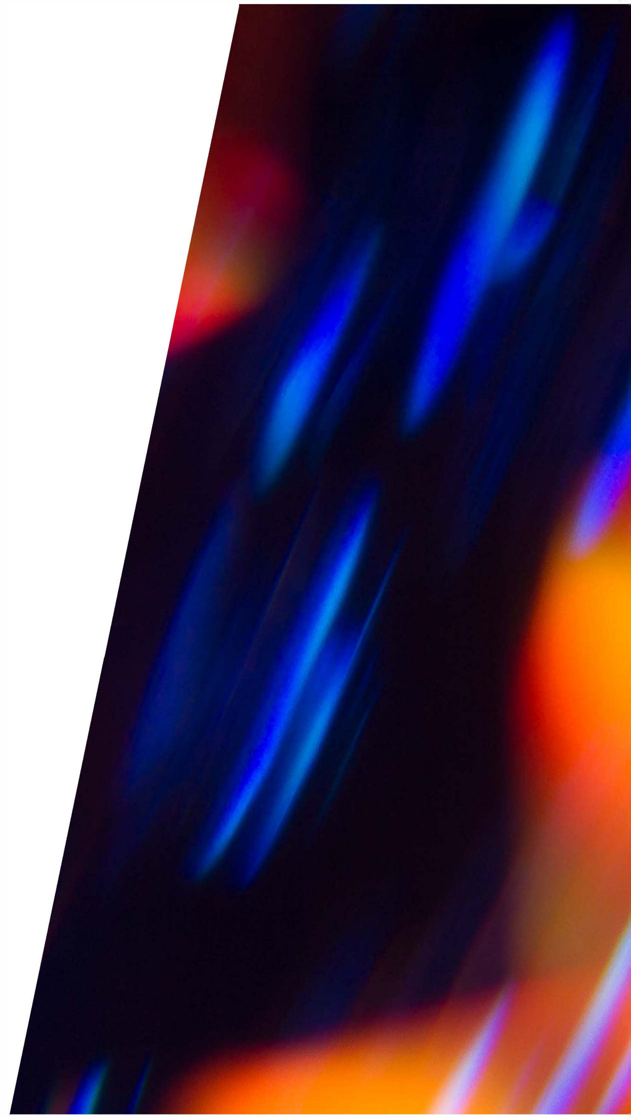
By contrast, **the smallest organizations** are driven by existential urgency. Their top concern is **competitive pace**. For smaller players, the failure to adopt AI quickly is seen as an immediate threat to market survival. Their focus then shifts to the practicalities of deployment — **cyber/data** and **integration** — as they lack the resource buffers of larger firms to absorb implementation failures. For the smallest firms, risk is rooted in their **limited AI agility** and **resource scarcity**.

> The sheer volume and sensitivity of data managed by these global giants make the risk related to AI use and cybersecurity exposure an exponentially increasing one.

We also examined variation in AI risk exposure based on organization type.

- **Public organizations** prioritize **workforce**, then **cyber/data** and **integration.** This is a balanced, operational profile reflecting the need to maximize ROI from publicly scrutinized investments by seamlessly integrating AI deployments with core business processes and upskilling employees to make the new business model work.
- **Private organizations (planning an IPO)** exhibit a unique, high-growth risk profile: **competitive pace, uncertain returns** and **embedding AI in market offerings.** This group is laser-focused on rapid validation of their business model for public markets. Their risks are predominantly **market-facing and financial,** prioritizing speed and demonstrable value over internal systemic concerns. Their focus on the market is particularly telling, indicating that AI is not just a tool but also a core, sellable feature of their valuation story.
- **Private organizations with no current plans for an IPO** identify the difficulty of integrating AI with existing technologies and business processes as the most problematic AI risk issue. They also have concerns with cyber-related risks associated with AI data needs and with their ability to deploy AI at a competitive pace.
- **Organizations owned in whole or part by a private equity firm** express the greatest concerns about the inability to deploy AI at a competitive pace, and risks related to data required for AI use and cybersecurity exposure. These challenges are understandable given the private equity market's focus on competitive positioning and growth, as well as on protecting the enterprise, including but not limited to its intellectual property.
- **Governmental and not-for-profit** organizations share a risk foundation of **integration and cyber/data.** These organizations, which often serve critical societal functions, are highly attuned to the risk of poor service delivery and the compromise of sensitive citizen/beneficiary data. Their risk profile is fundamentally about **mission continuity and public trust.**

> The size and organizational maturity of the enterprise significantly shape the risk outlook, distinguishing between organizations focused on managing immense complexity and those focused on securing competitive viability.



Summary

Our results show that AI risks are interconnected and require a broad, coordinated approach. The co-dominance of **cyber/data, integration** and **workforce** issues converge to a single potential failure point. Focusing only on data security without proper workforce training leaves systems unusable, while investing in integration without effective governance may facilitate speed and interconnectedness but can also breed uncontrolled risks.

Insights:

- **From a siloed to an integrated focus:** Given the theme emphasizing AI integration in our survey findings, organizations may find value in **shifting investments from sequential, siloed projects (cyber, HR, IT) to a more holistic approach**. For example, a cross-functional AI program office, reporting to a senior executive, could be empowered to evaluate opportunity and risk in the context of the three aforementioned core risks.
- **From deployment to realization:** The strong showing of **competitive pace** and **uncertain returns**, particularly among the CFO and private organizations, suggests a need to consider recalibrating the deployment narrative. The question is: Should the strategic calculus shift from **speed of deployment** to **speed of realization**?
- **From broad mandates to targeted outcomes:** Organizations can gain advantages by ensuring that each AI initiative is directly linked to clear, measurable business results associated with a proven financial benchmark, instead of following a wide-reaching technological mandate. The control functions (CRO and CAE) should participate in the initial idea phase, consistent with a **governance-for-value approach** in which control systems facilitate responsible and effective deployment, not simply restricting progress.
- **From prioritizing technology and systems to embracing the human component:** Concerns about core **workforce** issues and a related risk, **AI-driven morale declines and resistance to change** (a CHRO concern), highlight human capital's role in successful AI deployment. Employees should be trained not only to use AI, but also to assess its performance, spot errors, decide when to intervene and adapt their roles accordingly. AI should be supervised like human staff, with clear expectations, training to meet expectations, measuring and monitoring against expectations, and corrective actions taken to improve performance when necessary. Companies that prepare employees to work alongside and oversee AI agents are more likely to maximize the technology's potential.

The variance in industry-specific risk priorities necessitates the development of customized security frameworks. Our findings indicate that executive leadership recognizes that AI risk is an operational reality and competitive advantage will be achieved not by organizations deploying the greatest number of AI models, but by those offering solutions that are **safest, most integrated** and **highly trusted**. A unified strategy led by senior management is needed to achieve this focus.

05

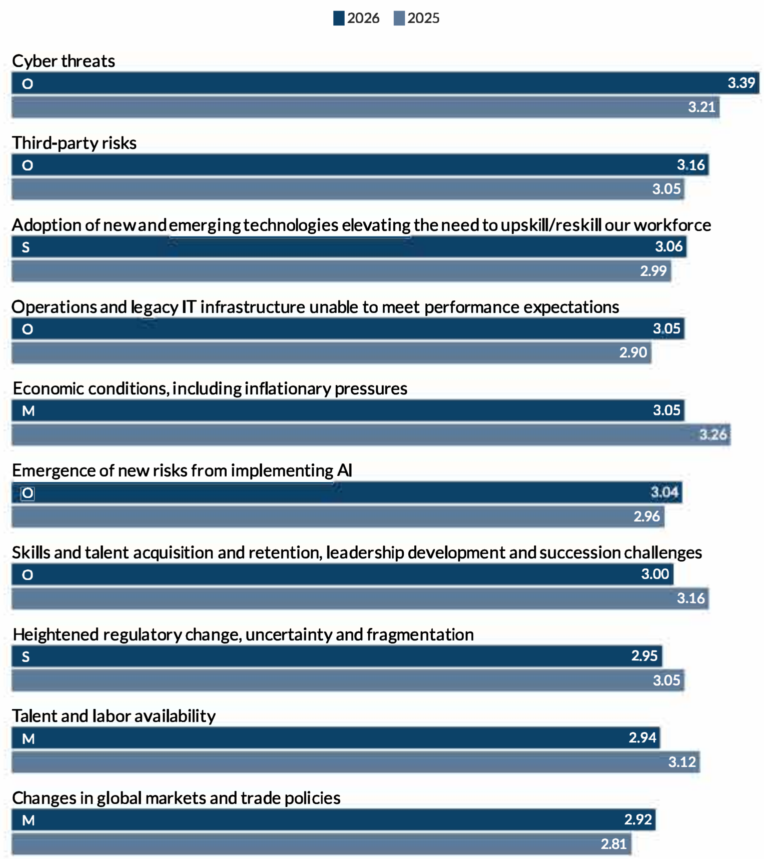
Navigating the near-term risk landscape

Relative to the prior year, the overall impression among the 1,540 respondents is that the magnitude and severity of the overall risk environment their organizations will face in executing their strategy and achieving their performance goals over the next two to three years is higher compared to last year. Using a 5-point Likert scale where 1=extremely low and 5=extremely high, the average risk score is 3.30 relative to 3.13 one year ago. This signals an overarching impression among respondents that the overall risk environment seems more challenging than views expressed in our prior year survey.

The top 10 near-term risk results from our study offer insights as to why the risk environment is slightly elevated. Figure 3 summarizes the rank-ordered list of top 10 risks over the next two to three years for the full sample of 1,540 C-suite executive and board member respondents, compared to the prior year. These risks, while dominated by operational risks, span macroeconomic, operational and strategic categories and are ranked based on their average Likert scores. The findings reveal a strong emphasis on operational vulnerabilities, talent challenges and the disruptive potential of emerging technologies.

Overall, 11 of the 28 risks rated by respondents are operational in nature, while nine are macroeconomic and eight are strategic.

Figure 3: Top 10 risks for the near-term



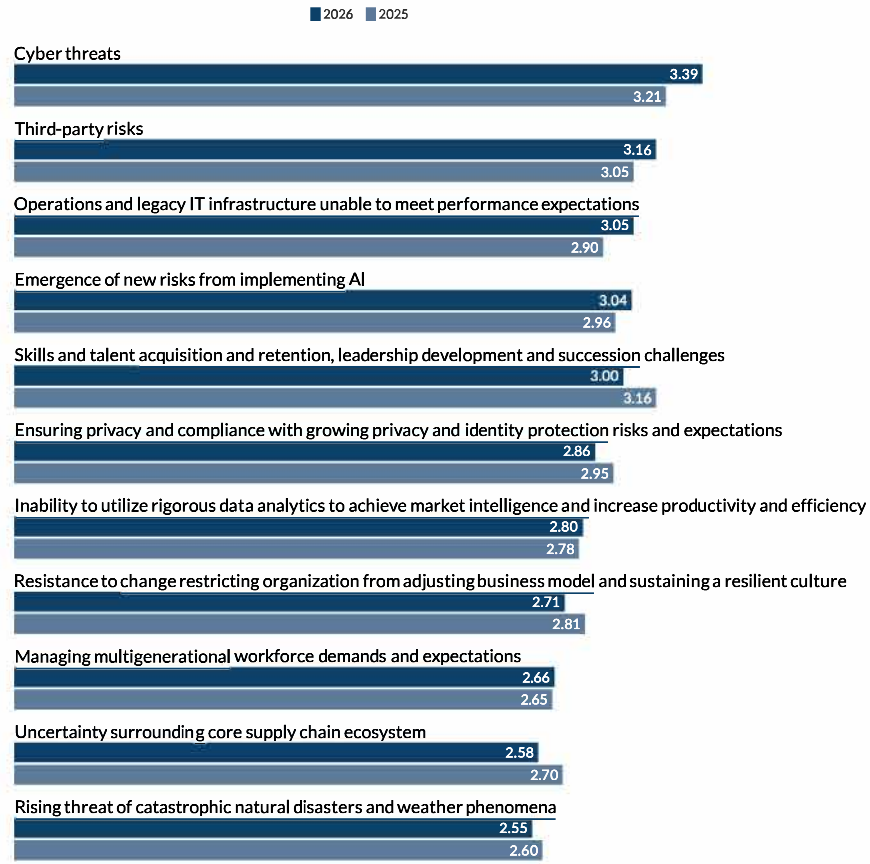
Dominance of operational risk concerns

Five of the top 10 near-term risks are operational in nature, signaling executive focus on **internal resilience and executional reliability**. These risks — cyber threats, third-party dependencies, legacy IT infrastructure, emerging IT and AI implementation challenges, and skills acquisition/retention — are deeply interconnected and reflect the pressure organizations face to deliver consistent performance in a world that is being disrupted digitally. Operational risks are no longer "back-office" concerns — they are front-and-center in strategic planning and execution. Operational risk management must now be integrated with enterprise strategy and aligned with technology-driven transformation goals.

Cyber threats are the top concern globally, reflecting a growing recognition that digital vulnerabilities are not just technical issues; they are existential threats. Executives are increasingly aware that cyber resilience must be embedded into enterprise strategy. Concern about cybersecurity was the number one risk concern for respondents across all sizes of organizations. Addressing evolving cybersecurity threats must be treated as a strategic imperative, with organizations needing to integrate cyber risk metrics into C-suite and boardroom performance dashboards.

Reliance on **third-party** external vendors and ecosystem partners introduces systemic vulnerabilities. Third-party risk spans cybersecurity, compliance, reputation and operational continuity. Executives are concerned about the lack of visibility into vendor practices, especially in multitiered supply chains and cloud-based services. Holistic third-party risk management frameworks, including continuous monitoring and scenario-based stress testing, are becoming more critical than ever. When considered together, **cyber threats** and **third-party risks** highlight the fragility of IT infrastructures and the need for robust governance across extended enterprises with a multiplicity of attack vectors.

Figure 4: Operational risks — near-term outlook



Legacy infrastructure and **AI implementation** risks underscore the tension between innovation and operational readiness. Operations and outdated legacy IT infrastructure systems and insufficient digital capabilities hinder innovation and competitiveness. Legacy infrastructure affects data integration, process efficiencies, customer experiences, time-to-market and the ability to pivot in the face of change. Prioritizing digital modernization along with clear ROI metrics will help ensure IT investments align with strategic goals and elevate digital capabilities across the enterprise. Of note, this issue is the highest elevated risk of this year's study, moving from the 13th-rated risk last year to the fourth-rated risk this year.

AI adoption is accelerating, but concerns about ethical dilemmas, regulatory uncertainty and operational disruption are growing. The rapid evolution of AI capabilities combined with the lack of governance frameworks makes the management of risk associated with AI difficult to identify, track and manage. Organizations may benefit from establishing cross-functional AI oversight committees to monitor and manage risks associated with AI deployments.

Talent challenges remain a critical concern, although the level of risk has abated slightly relative to views expressed in our last survey. **Attracting and retaining skills needed** and **developing leadership talent** are key concerns among executives surveyed, as they create challenges to building and sustaining the strong executive bench so critical to succession planning and long-term success. The decline from last year may reflect a number of factors — short-term hiring improvements and the effects of AI deployments, for example — but long-term concerns persist nonetheless. Talent-related risks reflect the **strategic importance of human capital** in sustaining competitive advantage and highlight the importance of integrating talent strategy with business strategy. Metrics on employee engagement and retention and the evolving leadership pipeline health will help senior management monitor emerging talent challenges.

Top macroeconomic concerns

Three of the top 10 near-term risks reflect macroeconomic concerns — economic conditions, labor availability and global trade policy shifts — that can disrupt strategic momentum. While these risks are somewhat outside the organization's control, their impact on cost structures, supply chains and market access is profound.

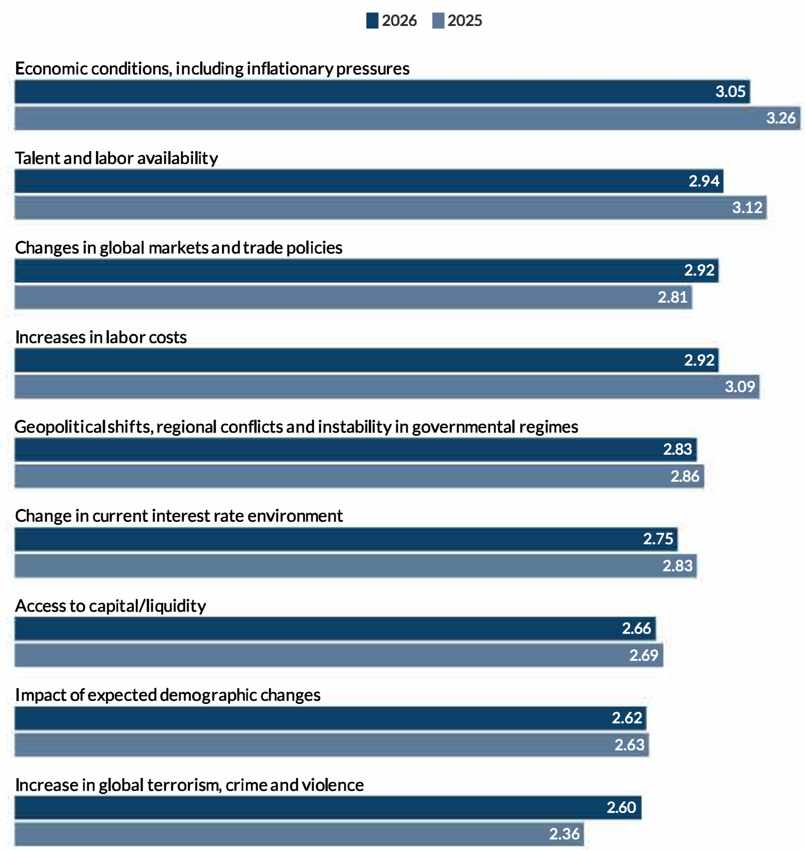
While economic uncertainty has declined somewhat relative to last year's survey, where this was the top-ranked risk, it continues to threaten margins, strategic investments and hiring decisions. Executives are navigating interest rate uncertainty, shifting consumer demand and geopolitical tensions. The slight decline in concern over inflation may suggest short-term stabilization, but executives remain cautious about long-term volatility. **Labor availability** and **global trade policies** are other factors impacting concerns over the economy.

The **availability of talent in the marketplace** is tied to demographic shifts, evolving immigration policy, workforce aging and shifts in needed skills in light of new AI and other digital capabilities — issues that require long-term strategic workforce planning. The decline in this risk may reflect some short-term improvements, but long-term uncertainty persists as the impact of AI on workforce requirements is causing companies to rethink hiring plans with reductions in some skills due to AI benefits coupled with a growing need for talent and new skills to leverage AI capabilities.

Geopolitical tensions and shifting trade alliances are heightening concerns about **global markets and trade policies**. Executives are focused on managing the effects of fluctuating tariff policies, border restrictions and regionalization of trade. Organizations that diversify their supply chains to nearshore and reshore as well as monitor geopolitical developments can improve their ability to pivot in response to frequent and unexpected geopolitical shifts. In today's global markets, organizations are searching for ways to ensure their global strategies are achievable and resilient.

Risk-adjusting strategy is all about being able to withstand external shocks. As organizations navigate the above challenges, it becomes increasingly important to leverage advanced analytics, scenario planning and stress testing to anticipate potential market opportunities and emerging risks. Prioritizing transparency in forecasting, enhancing financial planning and cost optimization, and fostering open communications across the organization help leaders pivot their strategies and maintain flexibility in capital deployment.

Figure 5: Macroeconomic risks — near-term outlook



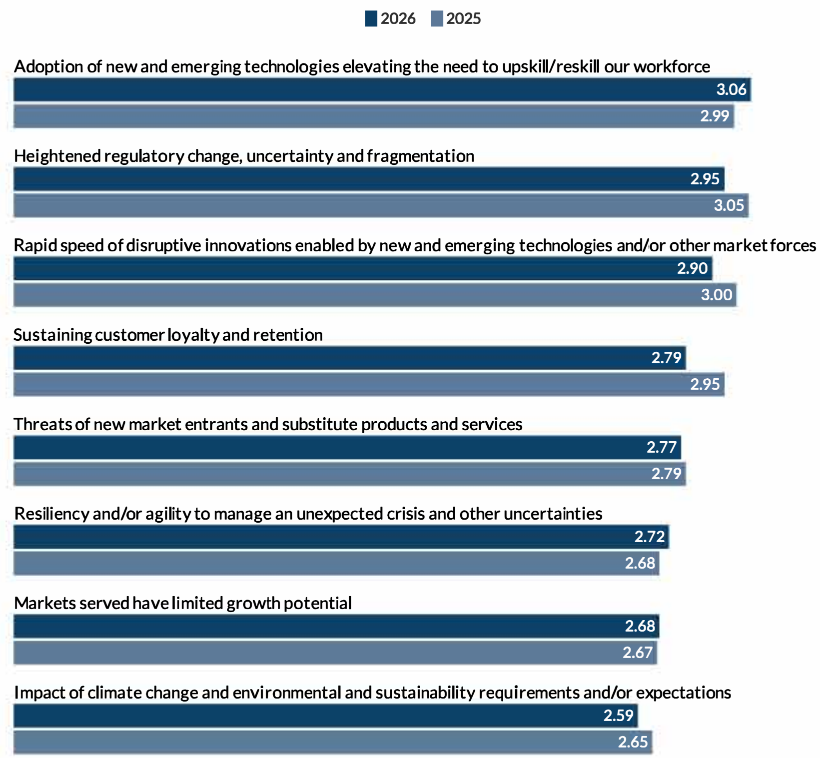
Top strategic risks

Though fewer in number among the top 10 near-term concerns, strategic risks — emerging technologies requiring workforce transformation and regulatory fragmentation — carry **high-impact potential**. These risks challenge the organization's ability to adapt, innovate and comply in a fast-changing environment. The **need to upskill/reskill** in response to emerging technologies is a strategic imperative, not just an HR issue. **Regulatory fragmentation** across jurisdictions increases complexity in designing and developing new innovation strategies and requires agile compliance approaches.

Respondents signaled an overarching concern that their organizations may struggle to **adopt new and emerging technologies** due to challenges they face in competing for the talent and skills needed to realize fully the value proposition used to justify investing in these promising capabilities. As the rapid pace of technological change outstrips workforce capabilities, a strategic talent gap arises, requiring organizations to train employees and align the culture with new capabilities. Generative AI, agentic AI and other forms of automation are reshaping job roles, workforce architecture and workflows. Organizations are recognizing that workforce transformation and talent readiness are core components of an effective digital strategy.

Regulatory change and complexity across jurisdictions increase operational burdens. Executives are concerned about fragmented landscapes in how data privacy, ESG, AI and other aspects of the business are regulated. Organizations should invest in regulatory intelligence to ensure compliance risk management is fully responsive to applicable laws and regulations and integrated into operations and operational and strategic decisions.

Figure 6: Strategic risks — near-term outlook



To provide insights about how different types of executives view near-term risks, we examined individual rankings of top risks across nine different positions. The table below highlights those risks that are ranked in the top five list of risks by position. The numbers (1 through 5) reflected in each column of the table indicate the relative rank within the top five for that risk by individuals in those positions.

Table 8: Top five near-term risks — by executive position*

Risks	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Cyber threats	1		1	1	1	1		1	1
Third-party risks			2	2	2	2		4	3
Emergence of new risks from implementing AI			4	5		3		5	4
Economic conditions, including inflationary pressures	4	5			5		4	3	
Skills and talent acquisition and retention, leadership development and succession challenges									5
Operations and legacy IT infrastructure unable to meet performance expectations			3	3	3	4			
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce		4	5		4	5			
Talent and labor availability	3	1					1		
Increases in labor costs	5	3					3		
Heightened regulatory change, uncertainty and fragmentation								2	2
Changes in global markets and trade policies				4					
Impact of expected demographic changes							5		
Managing multigenerational workforce demands and expectations							5		

Note: The number in each cell indicates the rank order of the top five risks by each executive position. Instances where the same rank is shown for more than one risk issue reflect ties.

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group. More extensive analyses across executive positions are available in a separate online appendix — visit www.protiviti.com or erm.ncsu.edu.

Across the board, **cyber threats** stand out as the most consistently ranked concern. This widespread prioritization underscores the almost universal recognition that cybersecurity is no longer a siloed IT issue but rather a strategic enterprise risk with implications for brand reputation, operational continuity and regulatory compliance. The fact that it tops the list for roles as diverse as the board, CIO/CTO and CRO suggests a shared understanding of its systemic nature and the need for cross-functional mitigation strategies.

Economic concerns also made it to the top five list of risks for the board and CEO along with several other members of the C-suite team. Uncertainties about inflation, government policies (including the evolving tariff landscape) and interest rates are triggering risk concerns across the executive team and board.

Talent-related risks — including labor availability, talent acquisition, upskilling and leadership development — also show strong representation, particularly among the CEO, CHRO and board. These concerns reflect the growing pressure to attract and retain mission-critical talent in a competitive and evolving labor market. Interestingly, CHROs rank "talent and labor availability" as their top concern, signaling the strategic importance of workforce planning in conjunction with digital transformation initiatives. The CEO's prioritization of both talent and labor availability and skills development further reinforces the strategic importance of human capital.

Differences in risk prioritization reveal how each role's functional lens shapes their risk perspective. For example, **regulatory change and fragmentation** is a top concern for the CRO and CAE — roles with responsibilities for compliance and governance support, oversight and assurance — while it does not appear in the top five for the CEO or COO. Similarly, **third-party risks** are more prominent for the CFO, CIO/CTO, CAE and COO, reflecting their respective focus on operational and financial exposure to vendors, service providers and other ecosystem partners.

Overall, the analysis reveals a **core set of shared concerns** — cybersecurity, talent and economic conditions — while also illustrating how **role-specific responsibilities** shape risk prioritization. This diversity of perspectives is valuable for enterprise risk management (ERM), as it ensures that risk oversight is both comprehensive and nuanced. Boards and executive teams should leverage these insights to foster cross-functional dialogue, align risk mitigation strategies and ensure that ERM reflects the full spectrum of leadership concerns.

Across the board, cyber threats stand out as the most consistently ranked concern. This widespread prioritization underscores the almost universal recognition that cybersecurity is no longer a siloed IT issue but rather a strategic enterprise risk with implications for brand reputation, operational continuity and regulatory compliance.

The following table summarizes the top five risks across the nine different industries we analyzed. Based on the comparative analysis of top five near-term risks across nine industry sectors, several key insights emerge that highlight both convergence and divergence in risk priorities.

Table 9: Top five near-term risks — by industry group*

Risks	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Cyber threats	1	1	5	1	1	1	2	4	1
Third-party risks	2	5	2	2	2	3	4		
Heightened regulatory change, uncertainty and fragmentation			4			2		1	
Economic conditions, including inflationary pressures		3		5	5		5	5	
Emergence of new risks from implementing AI		5		3	4				3
Increases in labor costs	4						3		
Operations and legacy IT infrastructure unable to meet performance expectations	3				3				5
Talent and labor availability						4		3	
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce				4		5			2
Rising threat of catastrophic natural disasters and weather phenomena			3						
Increase in global terrorism, crime and violence	5								
Impact of climate change and environmental and sustainability requirements and/or expectations			1						
Skills and talent acquisition and retention, leadership development and succession challenges								2	
Changes in global markets and trade policies							1		
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces									4
Sustaining customer loyalty and retention		4							

* More extensive analyses across industry groups are available in a separate online appendix — visit www.protiviti.com or erm.ncsu.edu.

Cyber threats are the most universally recognized risk, ranked first in six of the nine industry groups. This widespread concern reflects the pervasive nature of digital vulnerabilities across sectors. The consistency of this ranking suggests that cybersecurity is now viewed as a foundational risk that transcends industry boundaries, driven by increasing digitalization, data dependency and growing sophistication of threat actors.

Third-party risks also show broad relevance, appearing in the top five for seven of the nine industries. This reflects the growing reliance on external vendors, cloud providers, online platforms, distribution channels and communications channels in the ecosystem that introduce operational and reputational vulnerabilities. Interestingly, industries with complex supply chains or regulatory oversight — such as **Manufacturing and Distribution** and **Financial Services** — rank this risk high, indicating heightened sensitivity to vendor performance and compliance.

Differences in risk prioritization reveal how industry-specific dynamics shape risk perception. For example, **Energy and Utilities** uniquely ranks **impact of climate change and sustainability requirements** and **threats of natural disaster** as top concerns, reflecting regulatory pressures and environmental exposure. Meanwhile, **Not-for-Profit/Higher Education** prioritizes **skill and talent acquisition** and **talent availability**, reflecting the connectivity of policy shifts in public funding and related workforce challenges.

Finally, **technology-driven risks** — such as AI implementation and workforce upskilling — are more prominent in **Technology, Media and Telecommunications, Financial Services,** and **Healthcare,** where innovation cycles are rapid and digital transformation is core to strategy. The TMT sector, in particular, ranks multiple technology-related risks in its top five, underscoring the pressure to stay ahead of the curve.

These findings suggest that while some risks are universal, others are deeply shaped by industry context, operational models and strategic priorities. Organizations that use these insights to tailor risk management strategies and opportunity pursuits to their sector's unique exposure remain vigilant to cross-industry threats.

While some risks are universal, others are deeply shaped by industry context, operational models and strategic priorities.

The following table summarizes the top five risks across the different geographic regions we analyzed.

Table 10: Top five near-term risks — by geographic region

Risks	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Cyber threats	1	1	1	2	1	4	
Third-party risks	2	4	2	5	2		5
Emergence of new risks from implementing AI	4	5		3		5	1
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce		3		4	3	2	3
Operations and legacy IT infrastructure unable to meet performance expectations				1		1	2
Economic conditions, including inflationary pressures	3	2					4
Skills and talent acquisition and retention, leadership development and succession challenges			5			3	
Increases in labor costs			4		4		
Talent and labor availability			3				
Ensuring privacy and compliance with growing privacy and identity protection risks and expectations					5		
Heightened regulatory change, uncertainty and fragmentation	5						

Note: The number in each cell indicates the rank order of the top five risks by each geographic region.

Based on the comparative analysis of the top five near-term risks across seven global regions, several important patterns and regional nuances emerge that offer valuable insights into how geography shapes risk perception and prioritization.

Cyber threats are the most universally recognized concern, ranking in the top five for six of the seven regions and occupying the top spot in North America, Latin America, Europe and India. As with the industry groupings we examined, this widespread prioritization reflects the global nature of cyber risk. Interestingly, Australia and New Zealand did not rank cyber threats in their top five, likely due to the respondents in that region being heavily concentrated in government (57%) and mining (26%), indicating a different prioritization of relative risks in those sectors.

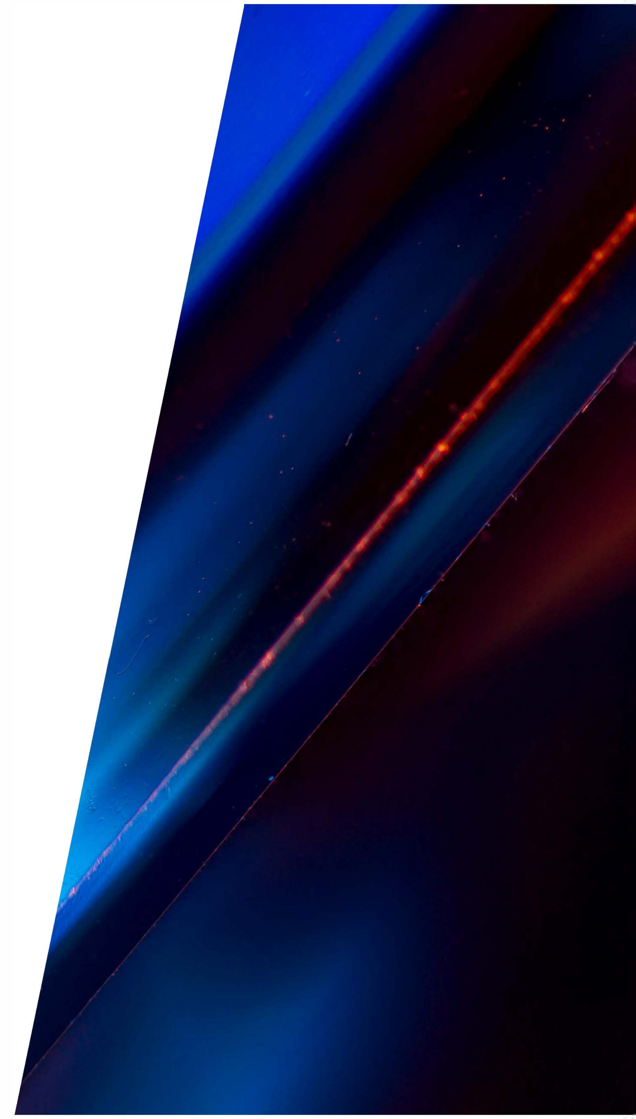
As with the industry groupings, **third-party risks** also show broad concern, appearing in the top five for six regions. North America, Europe and India rank it as their second-highest risk, highlighting its strategic importance in these regions. The presence of this risk in Latin America, the Middle East and Africa, and Australia and New Zealand suggests that supply chain vulnerabilities and partner dependencies are a shared global challenge, though the intensity of concern varies.

Regional differences become more pronounced when examining risks tied to **technology adoption and workforce transformation**. Latin America, Asia, India, and Australia and New Zealand all rank the need to upskill/reskill in response to emerging technologies within their top three, suggesting a strong regional focus on digital capability building. In contrast, this risk does not appear in the top five for North America or Europe, which may reflect more mature digital capabilities. However, concerns about talent and labor availability are high in Europe.

Other notable divergences include the **emergence of AI-related risks**, which are ranked highest in Australia and New Zealand (the top risk) and appear in the top five for North America, Latin America, the Middle East and Africa, and Asia. This suggests global concern about unintended consequences of AI deployments, though the degree of that concern varies. Meanwhile, concerns regarding **economic conditions and inflationary pressures** are more prominent in the Americas and Australia and New Zealand.

Overall, while some risks — like cyber threats and third-party dependencies — are globally recognized, others reflect **regional distinctions** in viewing **economic uncertainties, technological maturity** and **regulatory environments**. These insights underscore the importance of tailoring ERM strategies to regional contexts while maintaining a global view on systemic risks.

> While some risks — like cyber threats and third-party dependencies — are globally recognized, others reflect regional distinctions in viewing economic uncertainties, technological maturity and regulatory environments.



The following table summarizes the top five risks across the different categories of organizational size.

Table 11: Top five near-term risks — by organization size

Risks	Largest organizations	Medium-to-large organizations	Small-to-medium organizations	Smallest organizations
Cyber threats	1	1	1	1
Third-party risks	2	2	3	
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce	3		2	5
Emergence of new risks from implementing AI	5		4	4
Operations and legacy IT infrastructure unable to meet performance expectations	4	4	5	
Economic conditions, including inflationary pressures		3		2
Skills and talent acquisition and retention, leadership development and succession planning		5		3

Note: The number in each cell indicates the rank order of the top five risks by each group of organizations.

Based on the analysis of risk perceptions across four organizational size categories, several key insights emerge that highlight both shared concerns and distinct priorities shaped by scale and complexity.

Once again, **cyber threats** are the most universally recognized risk. Being ranked the top risk across all four size categories underscores the pervasive nature of cybersecurity concerns, regardless of organizational scale. Also, **third-party risks** are prominent among all categories except for the smallest organizations (in fact, the risk does not appear in their top five). Larger companies likely have more complex vendor networks and outsourcing arrangements, making them more vulnerable to disruptions or reputational damage stemming from external partners.

Our findings suggest that while some risks are universal, others are shaped by the structural realities of organization size, resource availability and strategic complexity.

For example, the results for **economic conditions and inflationary pressures** may reflect greater sensitivity to margin pressures and resource constraints among midsized and smaller entities. Similarly, the results for **skills and talent acquisition and retention** suggest that workforce challenges are particularly acute in medium-to-large and the smallest organizations, possibly due to competition for specialized talent or succession planning concerns.

Interestingly, **technology-related risks**, including the need to upskill for emerging technologies and the risks associated with AI implementations, are more widely recognized among the largest and smallest organizations. Large organizations are likely to face pressure to innovate at scale, while small organizations may be grappling with how to adopt new technologies without the benefit of deep internal expertise.

Being ranked the top risk across all four size categories underscores the pervasive nature of cybersecurity concerns, regardless of organizational scale.

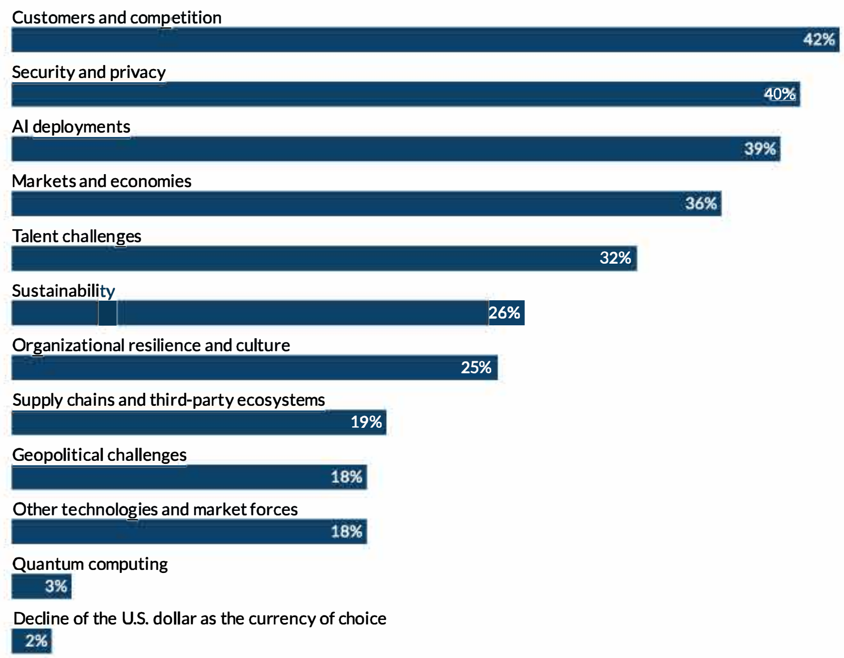
06

Managing long-term risks (next 10 years)

In addition to obtaining an understanding of near-term concerns, we also asked respondents to select from a list of 12 risk themes what they believe represent the top three risk areas their organizations are likely to consider most when evaluating strategies and making investments over the next 10 years. We formulated the risk themes considering the 28 specific risk areas we examined over the near-term to simplify the survey participants' long-term risk assessment.

Participants provided a rank-ordered list of their top three risk themes important to their organization over a 10-year time horizon. Figure 7 shows the risk themes listed in rank order based on the frequency that each risk theme was included in the respondents' top three choices. This list provides an indication of what our 1,540 respondents perceive to be their organization's most significant long-term risk concerns in light of their organization's business model and strategy.

Figure 7: Long-term risks



Percentages reflect frequency with which each area was selected among the top three.

Based on the rank-ordered list of long-term risk themes, here are several key insights that would be particularly valuable for boards and executive teams to monitor and discuss as they look out over the next decade:

- **Strategic focus on market positioning and trust:** The top four long-term concerns — customers and competition, security and privacy, AI deployment, and markets and economies — reflect a clear emphasis on maintaining competitive relevance and stakeholder trust in a rapidly evolving digital landscape. Executives are signaling that long-term strategy must prioritize customer experiences, data protection and responsible innovation. These themes are deeply interconnected with an emphasis on growth, market share and brand credibility.

- **Talent and technology as dual enablers — and risks:** Talent challenges combined with AI deployment both rank highly, suggesting that the workforce implications of emerging technologies are persistent long-term as well as near-term concerns. The dual focus on enabling tools and potential risks implies that long-term investments must include robust workforce development, responsible AI governance and cultural transformation to support innovation.

- **Broader systemic risks are rising — but unevenly prioritized long-term:** Themes like sustainability, organizational resilience, supply chains and geopolitical challenges reflect growing awareness of systemic disruptions — from climate change to global instability. However, their lower rankings suggest that while these risks are acknowledged, they may not yet be fully integrated into strategy setting and execution. Management and boards should consider whether these areas are underweighted in current risk frameworks, especially given their potential to reshape markets and supply chains long-term.

- **Emerging and peripheral risks require strategic foresight:** Risks such as quantum computing and the potential decline of the U.S. dollar are currently viewed as peripheral with their low prioritization. Nonetheless, forward-looking organizations should monitor these developments and consider scenario planning to ensure strategic agility as the question of their relevance and potential impact is clarified. If either of these developments become a reality, it will be too late for the unprepared.

These insights suggest that a long-term view of risk is truly strategic and must encompass market positioning, technological expansion, workforce transformation and systemic resilience so that new opportunities and emerging risks are not overlooked. This forward-thinking approach helps executive teams adapt more quickly to shifts in the external environment through better anticipation of market trends and technological advancements, challenging underlying strategic assumptions, formulating plausible as well as extreme scenarios, stress testing strategic alternatives, and making more informed decisions about resource allocation, capability building and prioritizing investments. Such vigilance is table stakes in the C-suite and boardroom.

Table 12: Top three long-term risks — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
AI deployments	36%	39%	36%	40%	49%	46%	38%	37%	33%
Markets and economies	43%	31%	38%	37%	33%	45%	33%	37%	36%
Customers and competition	47%	48%	37%	31%	30%	24%	37%	59%	60%
Security and privacy	32%	19%	45%	50%	50%	64%	42%	23%	25%
Talent challenges	36%	43%	33%	30%	23%	30%	33%	29%	30%
Sustainability	14%	14%	36%	33%	34%	30%	21%	15%	14%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

Directors and most C-suite leaders share concerns about long-term AI deployment risks and potential impacts from shifting markets and economies. The same thing can be said regarding concerns related to customers and competition, with the exception of COOs, CIOs/CTOs and CISOs, who prioritize data, technology and market dynamics — in that order. Interestingly, CEOs and board members focus more on talent challenges than other members of the C-suite, recognizing the importance of talent to organizational success. Effective strategic oversight at the highest level requires a comprehensive approach to talent management to ensure the organization has the right people in place to execute its shared vision and address future challenges.

Table 13: Top three long-term risks — by industry group

	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Security and privacy	58%	28%	35%	47%	56%	37%	22%	29%	57%
AI deployments	41%	43%	20%	47%	30%	45%	29%	29%	53%
Markets and economies	37%	34%	37%	40%	39%	34%	39%	19%	32%
Customers and competition	25%	55%	29%	48%	21%	48%	45%	59%	30%
Sustainability	38%	19%	43%	19%	48%	12%	31%	15%	25%
Supply chains and third-party ecosystems	14%	30%	37%	8%	6%	15%	34%	10%	8%
Organizational resilience and culture	25%	24%	26%	25%	23%	29%	20%	49%	18%
Talent challenges	25%	30%	26%	33%	31%	32%	33%	41%	30%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each industry group are highlighted in blue.

Three industry groups place higher emphasis on sustainability matters:

- Many governments prioritize sustainability matters over commercial sectors due to their public accountability, regulatory authority, commitment to long-term stewardship and the need to address pressing global challenges. By leading the way, they can create a framework that encourages commercial sectors to adopt responsible sustainability practices.
- The Energy and Utility sector's elevated focus on sustainability is driven by responses from our 70 respondents representing non-U.S. companies due to the scale of their environmental impact, regulatory pressures, resource management challenges, stakeholder expectations and the essential nature of their services. By prioritizing sustainability, these companies not only comply with legal and societal demands but also secure the viability of their long-term market permission to operate.
- Companies in Aerospace and Defense are driven by regulatory compliance, market demands, technological advancements and the need to sustain long-term viability. Given the commercial airline sector's cross-border operations, a sustainability focus makes sense because of requirements across the globe.

Energy and Utility companies emphasize supply chains and third-party ecosystems to drive efficiencies due to the complexity of their operations that encompass various interconnected stages, including extraction, generation, transmission, distribution and retail. The integration of smart grid technologies and the Internet of Things necessitates collaboration with various technology providers and service partners. In addition, these companies are increasingly focused on sustainability and reducing their carbon footprints, which often involves working with suppliers and third parties that share similar goals and practices.

Table 14: Top three long-term risks — by geographic region

	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Security and privacy	38%	28%	45%	47%	50%	30%	51%
Customers and competition	45%	43%	36%	37%	49%	48%	30%
Markets and economies	36%	37%	31%	43%	37%	43%	43%
AI deployments	44%	41%	39%	37%	47%	33%	24%
Sustainability	16%	23%	34%	44%	23%	21%	54%
Talent challenges	28%	36%	27%	29%	20%	53%	36%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each geographic region are highlighted in blue.

Two regions place a higher priority on sustainability matters.

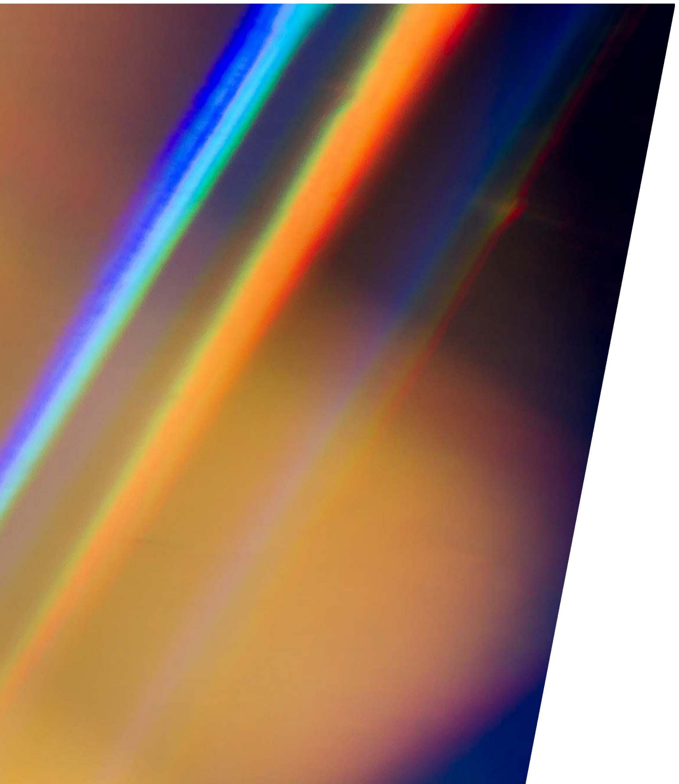
- **Middle East and Africa:** Many Middle Eastern countries struggle with water scarcity and desertification, while climate change brings extreme temperatures and unpredictable weather. Traditional reliance on oil exports calls for economic diversification as global energy demand shifts to renewables. Africa's large youth population is more environmentally conscious. Many nations in the Middle East and Africa region have joined international climate change agreements because of mutual interest in compelling developed economies to reduce carbon emissions.
- **Australia and New Zealand:** This year's concentration of the region's respondents in government and mining is the likely reason for the stronger emphasis on sustainability.

Asia places a higher priority on talent challenges, likely because of demographic trends (aging population). Other factors include economic growth priorities, competitive pressures for talent with Western economies and the need for innovation.

Table 15: Top three long-term risks — by organization size

	Largest organizations	Medium-to-large organizations	Small-to-medium organizations	Smallest organizations
Customers and competition	43%	40%	41%	47%
AI deployments	40%	40%	38%	41%
Security and privacy	41%	39%	45%	34%
Markets and economies	40%	35%	35%	36%
Talent challenges	27%	33%	31%	37%

Results across organization size are reasonably consistent. The largest organizations report a slightly stronger focus on markets and economies, and the smallest, to no surprise, recognize talent challenges as a top long-term risk.



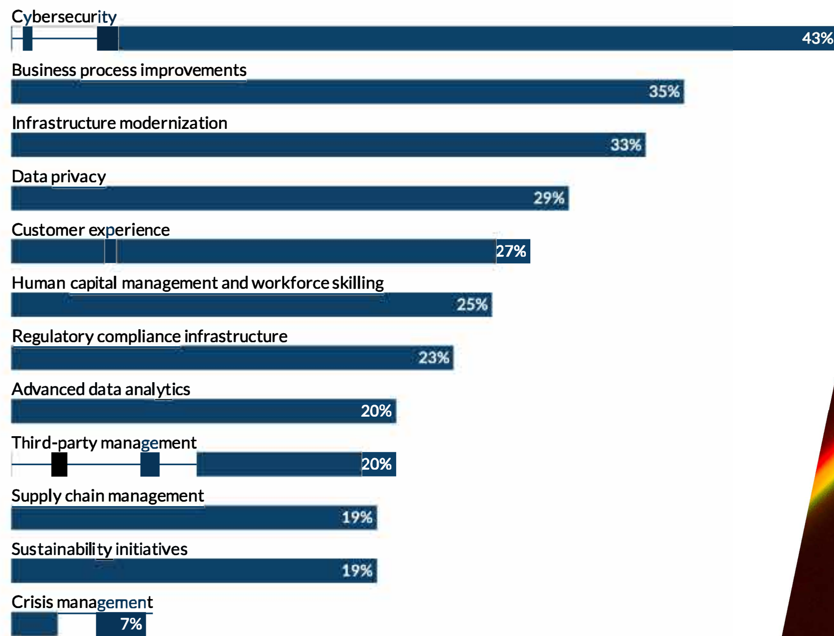
07

Strategic investment priorities

We asked respondents to identify the top three strategic investment priorities, in rank order, in which their organizations are likely to invest the most over the next two to three years given the opportunities and risks our report has highlighted. We provided a list of 12 investment areas that relate to some of the strategic and operational near-term risk issues our survey examined.

Figure 8 shows the number of times each investment area was included among the top three choices by the 1,540 respondents.

Figure 8: Top strategic investment priorities



Percentages reflect frequency with which each area was selected among the top three.

The consensus in the overall results confirms that leaders are focusing on **resilience, relevance** and **execution**. Capital is being dedicated to fixing the operational core, ensuring security compliance and building the necessary infrastructure to scale AI and other advanced digital capabilities. With **data privacy** and **customer experience** ranked fourth and fifth, respectively, the propensity to invest in all of these areas suggests that many leaders are thinking and acting digitally. The overall survey results define the baseline investment thesis, clustering the top priorities into a clear hierarchy of foundational needs, operational levers and growth engines.

As organizations adopt AI and connect more devices, the surface area for attacks expands exponentially, making **cybersecurity** the highest-priority non-discretionary area of spending. It is a **fiduciary obligation** and **brand protection** necessity. The high ranking of **data privacy** reinforces this defensive posture. With regulatory shifts like GDPR in the EU and CCPA in California, investment in privacy infrastructure is seen as inseparable from security, forming a comprehensive **digital defense layer**.

In tandem, **infrastructure modernization** is another investment priority. Legacy systems cannot support the computational demands of AI, the data volumes of modern operations or the speed required for competitive redeployment. Evolving the infrastructure is therefore the necessary antecedent investment that unlocks the value of cybersecurity (security-by-design), process automation and digital disruption.

The high prioritization of **business process improvements** confirms that investment focus is being directed to operational leverage. Process automation and enhanced decision-making offer the most direct path to realizing ROI from AI and automation tools. This investment is aimed squarely at **removing friction, accelerating cycles, lowering the cost-to-serve (reducing labor costs) and speeding up quality decision-making.**

While **human capital management and workforce skilling** ranks sixth overall, its high prioritization by roles such as the CHRO and in labor-intensive industries demonstrates it is the **critical bridge investment** and an essential indicator of strategic alignment. Organizations wisely recognize that defensive and infrastructural spending and process improvements are useless without the human capital to manage the new systems and drive the change. This spending acts as an **enabling investment** to ensure the benefits of technology investments are fully realized. Organizations that fail to align their investments with aggressive talent upskilling will risk turning capital expenditures into potentially high-risk, low-return assets.

As a top five priority, **customer experience** clearly demonstrates that even amid intense defensive spending, executives are dedicating budget to market differentiation and revenue growth. Improving customer experiences is the primary external-facing metric of the firm's overall digital maturity. That focus drives foundational investments channeled toward improving customer-facing processes and creating demonstrable customer value.

Table 16: Top three strategic investment priorities — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Cybersecurity	32%	27%	39%	39%	42%	53%	25%	51%	51%
Business process improvements	48%	60%	21%	20%	32%	24%	46%	48%	51%
Customer experience	36%	42%	19%	15%	21%	17%	25%	33%	43%
Infrastructure modernization	32%	32%	32%	34%	30%	21%	37%	44%	33%
Data privacy	21%	10%	40%	42%	39%	54%	25%	7%	7%
Human capital management and workforce skilling	40%	50%	18%	19%	16%	15%	63%	23%	33%
Regulatory compliance infrastructure	12%	13%	30%	26%	32%	26%	8%	20%	17%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

Strategic priorities diverge significantly when viewed through the lens of functional accountability, reflecting the primary duties and immediate pressures of each C-suite role.

The roles responsible for high-level strategy and overall outcomes — **board members and CEOs** — exhibit a strong focus on **business process improvements** and **human capital,** followed by **customer experience.**

- The **CEO** and **board** prioritize execution and impact. The focus is on how the organization operates and the capability of the team to deliver superior outcomes. They delegate the primary technical defense to the CFO and CIO/CTO, but demand results in operational excellence.

The executives responsible for protecting the balance sheet and ensuring operational stability have a distinctly defensive investment profile.

- The top investment priorities for **CFOs** and **COOs** are aligned: **data privacy, cybersecurity** and **infrastructure modernization.** This is a clear **"protect the fortress"** strategy. For the CFO, these are non-negotiable costs of fiduciary duty. For the COO, system stability and data integrity are prerequisites for reliable operations. The relative de-prioritization of growth-related spending (like customer experience) shows a current preference for operational integrity over immediate expansion.

- **CIOs/CTOs** and **CISOs** also prioritize **data privacy, cybersecurity** and **regulatory compliance.** This is a profile dominated by the **technical defense layer.** They recognize that the pressures of digital deployment necessitate a robust, compliant foundation to manage increasing complexity and fragmented regulatory oversight.
- **CROs and CAEs** focus on **cybersecurity** and **business process improvements.** The oversight and control functions are interested in the areas most critical for risk reduction and assurance: securing the system and ensuring the underlying processes and platforms are relevant, stable, reliable and resilient.
- The **CHRO** is the only executive to lead with **human capital management and skilling** as their top strategic investment priority, followed by **business process improvements** and **infrastructure modernization.** This is a sophisticated understanding of the value chain: The best investment is in employees, who will then optimize the processes with a strong focus on operational improvements.

Table 17: Top three strategic investment priorities — by industry group

	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Cybersecurity	42%	41%	33%	57%	36%	38%	30%	37%	55%
Infrastructure modernization	36%	24%	63%	25%	43%	29%	39%	44%	20%
Business process improvements	26%	33%	30%	40%	15%	42%	42%	54%	28%
Data privacy	48%	23%	9%	33%	50%	20%	12%	9%	52%
Customer experience	7%	42%	16%	37%	9%	31%	20%	49%	24%
Supply chain management	18%	36%	34%	4%	2%	13%	43%	0%	10%
Regulatory compliance infrastructure	30%	18%	37%	23%	35%	24%	16%	19%	19%
Sustainability initiatives	21%	14%	27%	11%	38%	16%	23%	9%	19%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each industry group are highlighted in blue.

An industry context defines the most pressing investment priority, shaped by the sector's regulatory environment, asset base and customer engagement model. Industries dealing with highly sensitive data or critical infrastructure place an existential premium on defense.

- **Financial Services** and **Technology, Media and Telecommunications:** Both include **cybersecurity, data privacy** and **business process improvements** in their top three strategic investment priorities. For Financial Services, this investment focus protects customer assets and system integrity. For Technology, Media and Telecommunications, it protects proprietary IP and product platforms.

- **Government:** The Government sector leads with **data privacy,** prioritizing the protection of citizen data and public trust over all other areas. This is followed by **infrastructure modernization** and **sustainability initiatives,** confirming the urgent need to replace legacy technology and manage cyber threats.

Sectors relying on vast physical assets and complex logistics prioritize the underlying platforms.

- **Manufacturing and Distribution** and **Energy and Utilities:** Both rank **infrastructure modernization** as a high priority. This is the prerequisite for deploying any smart factory, grid optimization or supply chain tracking technology. Without a modern infrastructure backbone, automation efforts are at risk of being stalled. Manufacturing and Distribution also includes **business process improvements** and **supply chain management,** focusing on efficiency and protecting operational technology systems. Energy and Utilities follows with **regulatory compliance infrastructure** and **supply chain management.**

Customer- and patient-centric industries focus their primary investment on improving the experience and delivery of services.

- **Consumer Products and Services:** Leads with **customer experience**, the clearest revenue driver. This is followed by **cybersecurity** to protect brand trust and **supply chain management** to ensure product availability. This investment focus is designed for **brand growth and fulfillment**.

- **Healthcare** and **Not-for-Profit/Higher Education:** Both prioritize **business process improvements** and **customer experience** as top investments. In these environments, this focus offers an effective strategy to combat administrative inefficiencies and optimize resource deployment. These are followed by **cybersecurity** for Healthcare and **infrastructure modernization** for Not-for-Profit/Higher Education, confirming a universal focus on streamlined service delivery.

Overall, our survey results identify three critical, interlocking insights for investment strategy over the next two to three years.

- **The inseparability of defense and transformation:** The data shows a unified, three-part digital foundation investment: cybersecurity, data privacy and infrastructure modernization. These three areas must be funded and executed as a single, coherent program, not as siloed departmental budgets. Failure in any one area — a cyber breach, a privacy violation, a system outage or an inability to innovate in a rapidly evolving marketplace — will neutralize gains made in process or customer experience improvements. Investment in this digital foundation is now the core enabler of transformation, not a separate cost center.

- **The bottleneck of talent skilling:** While human capital management and workforce skilling ranks sixth overall, it functions as a strategic bottleneck for the entire investment portfolio. Technology systems are being funded and processes are being reimagined as disruptive innovation continues, but the people required to operate and optimize the new systems and processes are a mid-tier priority. Organizations must prioritize human capital management in planning transformation initiatives. Skilling should be viewed as an expedited prerequisite for achieving ROI in process improvements and enhancing customer experiences. The true value of a large infrastructure investment is only realized when the workforce can fully utilize the new capabilities, demanding a proportional investment in human capital and workforce development to capture the expected value and returns.
- **The shift from project-based to platform investment:** The high ranking of infrastructure modernization (and its elevation as a near-term risk) suggests executives are recognizing the limits of tactical, project-based IT spending. The move to modern infrastructure (cloud, modular systems, centralized data platforms) is a commitment to a platform-based operating model. This platform approach facilitates continuous **business process improvements** and provides a robust engine for **advanced data analytics**, which, while a mid-tier investment priority, is the long-term engine for competitive differentiation. Executives must ensure their infrastructure modernization investments are guided not just by cost savings, but also by the ability to iterate and scale new AI-driven processes rapidly.

In summary, the most successful organizations over the next two to three years will be those that master the alignment between their defensive and offensive investments, secured by a dedicated and upskilled workforce.

> Organizations must prioritize human capital management in planning transformation initiatives. Skilling should be viewed as an expedited prerequisite for achieving ROI in process improvements and enhancing customer experiences.

Closing comments

The results of this year's survey of 1,540 board members and C-suite executives reveal optimism about growth opportunities despite economic, workforce and technological challenges. The findings emphasize that organizations must pursue strategic growth and business resilience together in today's complex, dynamic risk landscape.

The most successful organizations will be those that treat opportunity and risk as interdependent forces — embedding agility, foresight and cross-functional collaboration into the core of their strategic agenda. This report is intended to catalyze those conversations and support leaders in building organizations that thrive amid uncertainty and change.

For more detailed results from our survey based on executive role and industry, appendices are available at www.protiviti.com and erm.ncsu.edu.

Research team and authors

NC State University's ERM Initiative

Mark Beasley
Professor and Director of the ERM Initiative

Bruce Branson
Professor and Associate Director of the ERM Initiative

Don Pagach
Professor and Director of Research of the ERM Initiative

Protiviti

Carol Beaumier
Senior Managing Director

Matthew Moore
Managing Director

Jim DeLoach
Managing Director

Kevin Donahue
Senior Director

Shaun Lappi
Research Manager

Shannon West
Project Manager

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

About NC State University's ERM Initiative

The Enterprise Risk Management (ERM) Initiative in the Poole College of Management at NC State University provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, host executive workshops and educational training sessions, and issue research and thought papers on practical approaches to implementing more effective risk oversight techniques (erm.ncsu.edu).

protiviti®

NC STATE Poole College of Management
Enterprise Risk Management Initiative

www.protiviti.com

erm.ncsu.edu

Audit Committee

Annual Internal Audit Plan and Risk & Control Discussion

Item 7f

March 9, 2026

Presented by: Araceli Muñoz, Senior Audit Manager
Lina Tan, Principal Auditor
Sherman Hung, Principal Auditor

Item 7f
Internal Audit Plan and Risk & Control Discussion

Subject

Annual Internal Audit Plan and Risk & Control Discussion

Purpose

1. Explain how the Office of the General Auditor creates the annual risk-based internal audit plan
2. Provide an overview of internal control
3. Share current risk information
4. Obtain the Board's input regarding the District's internal control environment and current risk profile

Next Steps

Audit Committee and Board approval of the Internal Audit Plan for Fiscal Year 2026/27 in June 2026

Creating the Risk-Based Internal Audit Plan

Creating the Risk-Based Internal Audit Plan

Audit Department Responsibilities
[Admin. Code § 6451 (d)(1)]

Develop and present a flexible annual audit plan to the Audit Committee for review and approval. This plan should:

- Be developed utilizing a risk-based methodology
- Include risks or internal control concerns identified by:
  - Management
  - Board of Directors

Creating the Risk-Based Internal Audit Plan

Introduction

Global Internal Audit Standard 9.4

The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives.

Requirements

- Consider the internal audit mandate
- Specify internal audit services that support Metropolitan
- Consider coverage of high-risk areas
- Identify resource requirements
- Be dynamic and timely

Process Overview

1. Understand the organization
2. Identify, assess, and prioritize risks
3. Estimate resources & identify engagements
4. Prepare the audit plan
5. Propose, finalize, and present audit plan for Board approval
6. Execute audit plan

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Understand the Organization

- Understand governance, risk management, & control processes
  - Review key documents
  - Meet with the Board
  - Hold management meetings
  - Obtain internal audit staff input
- Identify emerging risks
- Update audit universe

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Identify, Assess, and Prioritize Risks

- Understand business objectives, strategies, & risks
- Identify & document risks
- Assess risk assessment method
- Measure risks
- Score & prioritize auditable units

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Measure Risks

- Auditable unit
- Risk Ratings
  - Impact
    - Loss exposure – financial, reputational
    - Strategic risk – political, legal
  - Likelihood
    - Control environment
    - Complexity
    - Assurance coverage
    - Board/management concern
  - Velocity

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Score & Prioritize Auditable Units

- Risk factor weights
- Preliminary risk score
- Review 1
- Executive management review
- Review 2
- Final risk score
- Auditable unit ranking

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Additional Planning Considerations

- Board & management requests
- Assurance needs
- Mandated engagements (law or regulation)
- Activities critical to mission, strategy, or high-risk areas
- Advisory or ad hoc requests
- Resource availability (time and staffing)

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Estimate Resources

- Assess staff's knowledge, skills, & abilities
- Coordinate coverage with other assurance providers
- Calculate available plan hours

Identify Engagements

- Update service portfolio
- Identify planned engagements
- Determine any audit coverage limitations
- Ascertain additional skills required

Creating the Risk-Based Internal Audit Plan

- 1. Understand
- 2. Risks
- 3. Resources & Engagements
- 4. Audit Plan
- 5. Board Approval
- 6. Execute Plan

Prepare the Audit Plan

- Executive summary
- Department overview
- Risk assessment process
- Risk assessment summary
- Service portfolio
- Planned engagements
- Risk coverage map
- Resource plan
- Organizational chart
- Standards

Creating the Risk-Based Internal Audit Plan

1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

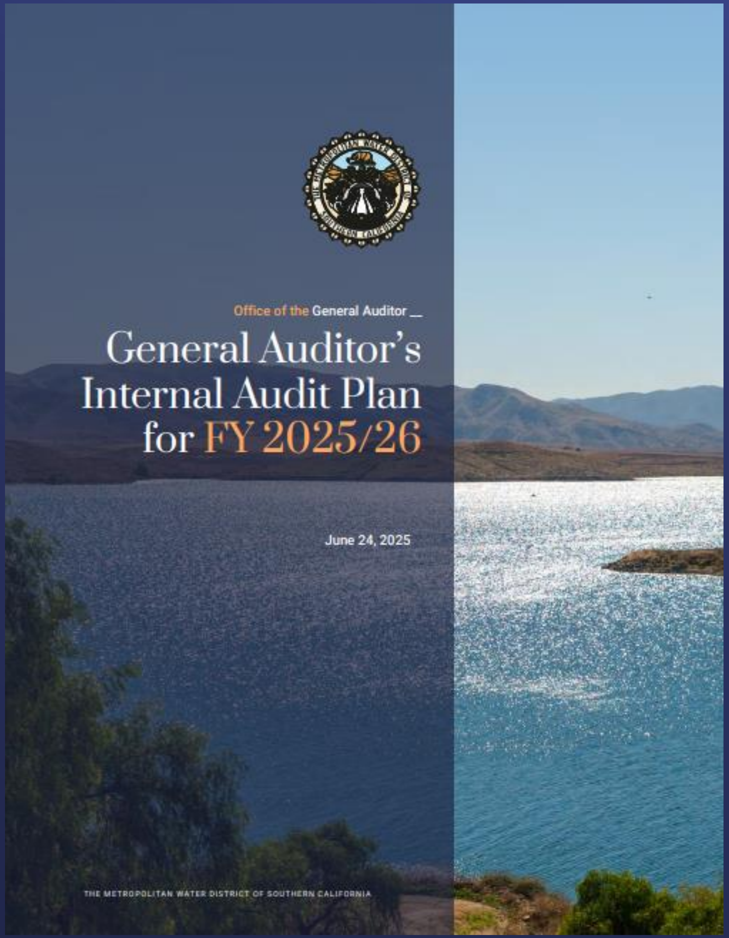
Present Audit Plan for Board Approval

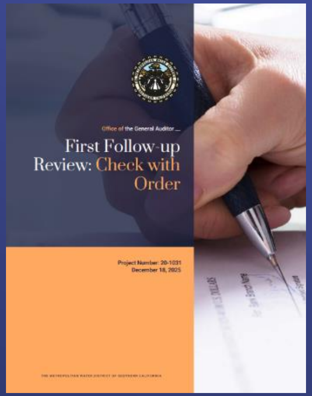
- Share with department heads
- Present to the Audit Committee for approval
- Obtain Board approval
- Distribute

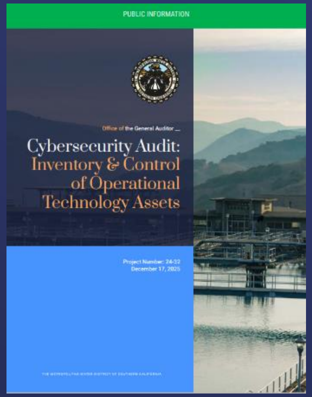
Creating the Risk-Based Internal Audit Plan

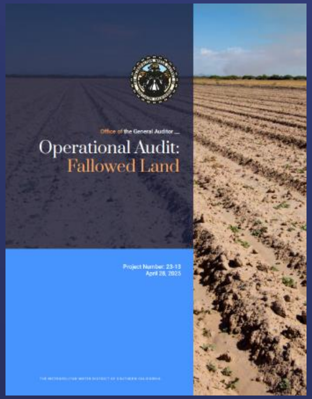
1. Understand
2. Risks
3. Resources & Engagements
4. Audit Plan
5. Board Approval
6. Execute Plan

Executing the Audit Plan









Creating the Risk-Based Internal Audit Plan

Questions?

Internal Control

Executive Committee: Duties & Functions

[Admin. Code § 2416 (b)(4)]

Internal Control

Consider the effectiveness of the District's internal control system, including information technology security and control

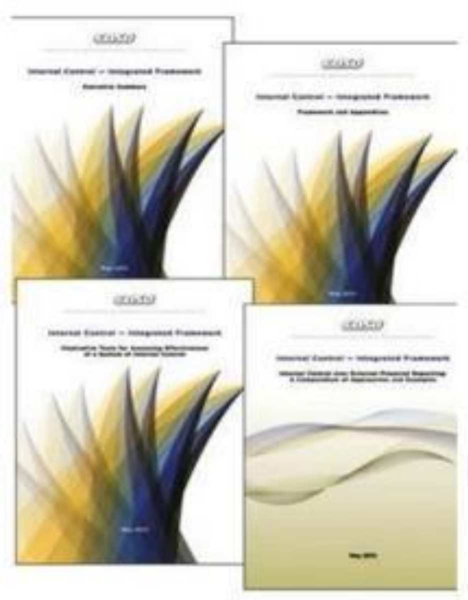
What is Internal Control?

Internal Control

A process, effected by the entity's Board of Directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Source: COSO, May 2013

Internal Control



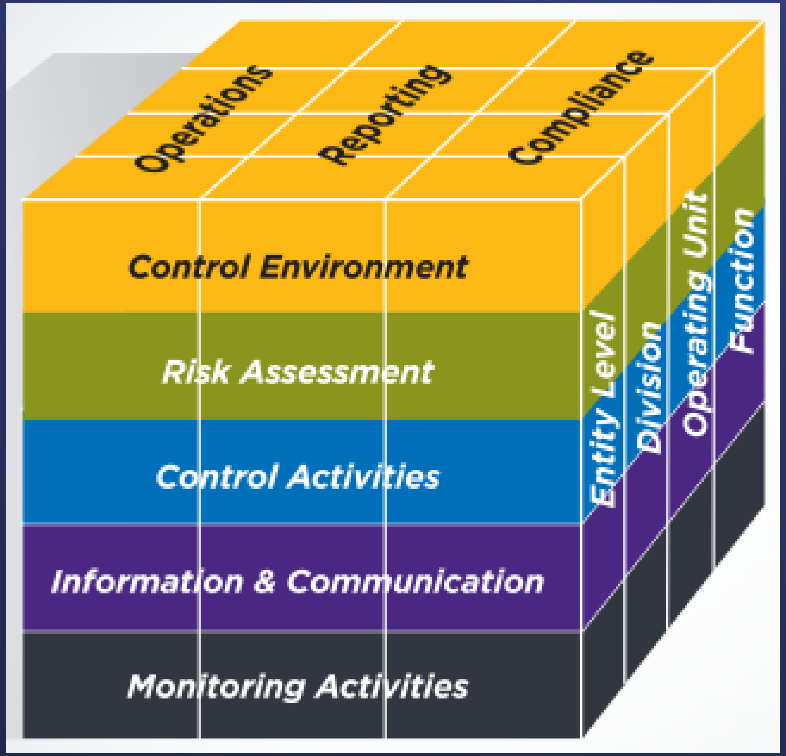
COSO Internal Control-Integrated Framework

- Leading internal control framework:
  - Designing
  - Implementing
  - Evaluating
- Released in 1992; updated in 2013
- Future initiative: Adoption by Metropolitan

COSO Internal Control-Integrated Framework

Internal Control

Objectives



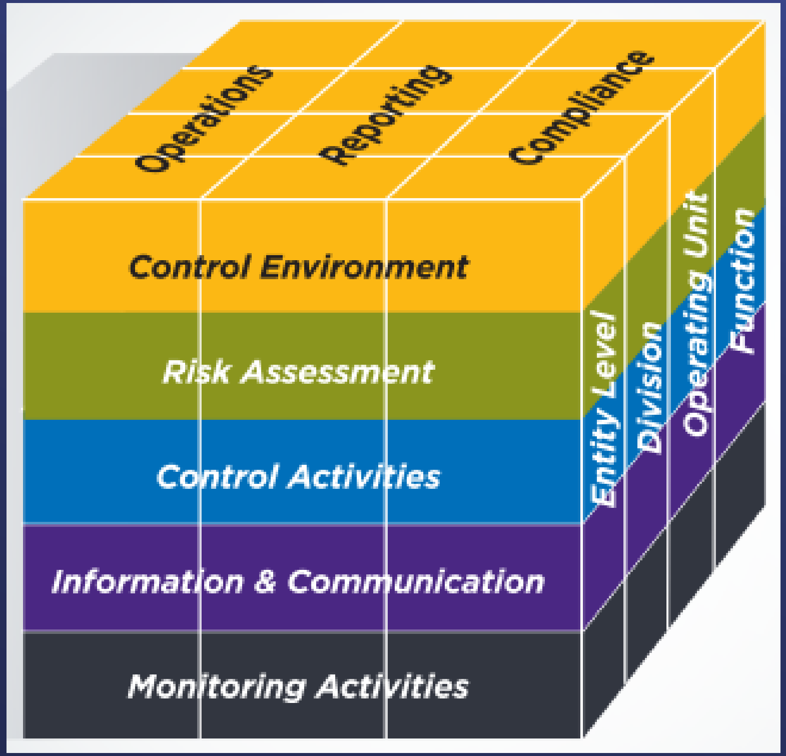
Operations:

- Strategic Plans
- Effective and Efficient
- Safeguarding Assets

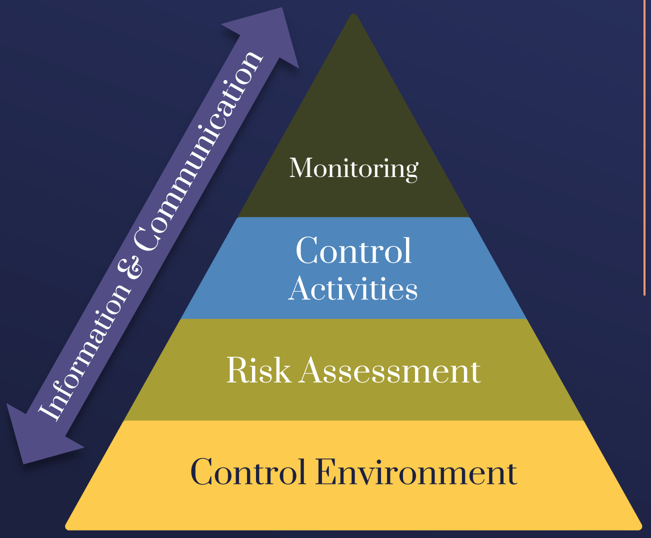
COSO Internal Control-Integrated Framework

Internal Control

Components



Internal Control

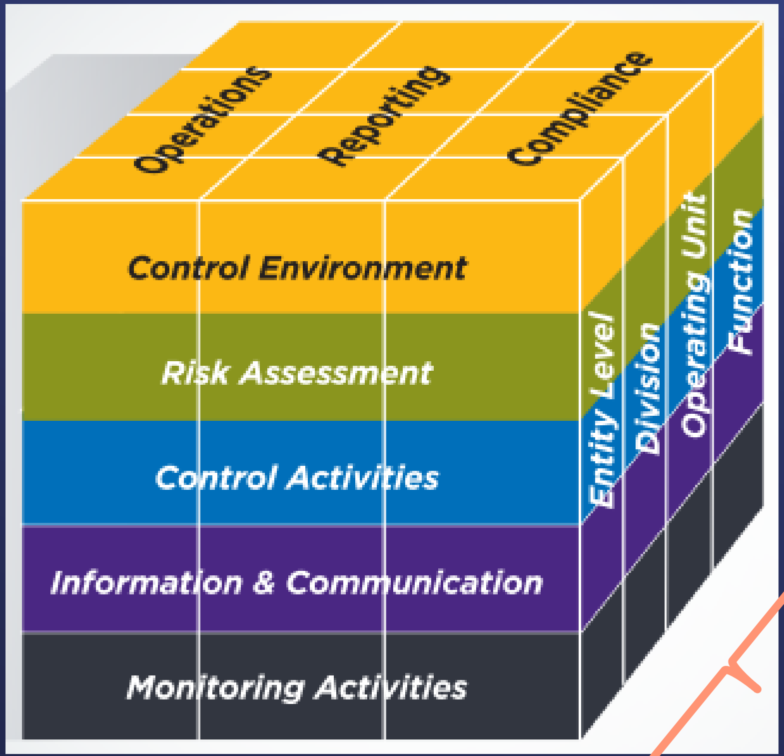


Control Environment

- The foundation for the District's internal control system
- Consists of five principles:
  1. Board and management demonstrate commitment to integrity and ethical values
  2. Board oversees the District's internal control system
  3. Management establishes structure, responsibility, and authority
  4. Management demonstrates commitment to employee competence
  5. Management enforces accountability

COSO Internal Control-Integrated Framework

Internal Control



Organizational Structure

Internal Control

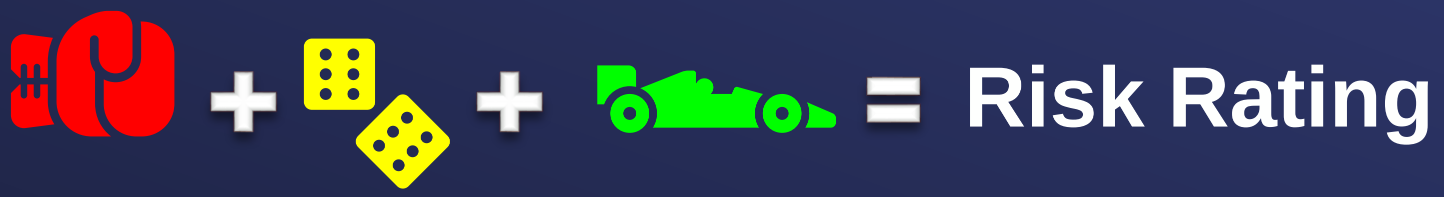
Questions?

Risk Considerations

Definition of Risk

What is Risk?

- The possibility of an event occurring that will impact objectives
- Positive (opportunity) or negative
- Risk is generally measured in terms of:
  - Impact or consequence
  - Likelihood or probability
  - Velocity



Source: IIA

Risk Areas

Business resilience	Governance/corporate reporting
Climate change/environment	Health/safety
Communications/reputation	Human capital
Cybersecurity	Market changes/competition
Digital disruption (e.g., AI)	Mergers/acquisition
Financial/liquidity	Organizational culture
Fraud	Regulatory change
Geopolitical/macroeconomic uncertainty	Supply chain (e.g., third party)

Source: IAF Risk in Focus 2026

Top 5 Risks

IIA - Risk in Focus 2026	Protiviti - Top Risks 2026
Cybersecurity	Cyber Threats
Digital Disruption (including AI)	Third-Party
Regulatory Change	Economic Conditions
Business Resilience	New Risks from Implementing AI
Geopolitical uncertainty	Regulatory Changes

Sources: IAF Risk in Focus 2026 and Protiviti Top Risks 2026

Risk Considerations

Geopolitical Uncertainty

- 5th highest risk
- Highest gain in risk rating
- Rapid changes in U.S. policies
- Challenges include:
  - Coping with new volatility
  - Policy change uncertainty

Source: IAF Risk in Focus 2026

Risk Considerations

Digital Disruption

- 2^{nd} highest risk
- Top 5 risks by 53% of audit leaders
- Challenges include:
  - Increase in cyber attacks
  - Workforce adoption
  - Governance restrictions

Source: IAF Risk in Focus 2026

Risk Considerations

Questions?

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Appendix

Board Committees & Functional Areas

Appendix

Board Committees & Functional Areas

Executive Committee
- General Manager
- Board Support Services

Legislation & Communications
- External Affairs

Legal & Claims
- General Counsel

Appendix

Board Committees & Functional Areas

Engineering, Operations, & Technology

Power Operations & Planning	Water Treatment
Infrastructure Reliability	Water Quality
Information Technology (General)	Cybersecurity
Water Conveyance & Distribution	Program Management
Water Operations & Planning	Planning
Operations Support	Engineering Design

Appendix

Board Committees & Functional Areas

One Water & Adaptation

- Centralized Grants & Research
- Bay Delta Initiatives
- Water Resource Implementation
- Water Resource Planning & Development
- Sustainability, Resilience, & Innovation
- Land Management
- Environmental Planning

Appendix

Board Committees & Functional Areas

- Finance, Affordability, Asset Management, & Efficiency
- Business Continuity
- Treasury & Debt Management
- Administrative Services
- Controller
- Revenue & Budget
- Risk Management

Appendix

Board Committees & Functional Areas

Organization, Personnel, & Effectiveness

- Human Resources
- Employee Relations
- Security
- Operational Safety & Regulation
- Training

Board Committees & Functional Areas

Appendix

Community & Workplace Culture

Diversity, Equity, & Inclusion (DEI)

Equal Employment Opportunity (EEO)

Ethics Office

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Committee Item
INFORMATION

Audit Committee

3/9/2026 Committee Meeting

7g

Subject

Study, advise on, or recommend Board member/Board committee audit assignment requests

Executive Summary

This item covers Audit Committee discussion on requests for audit assignments from individual board members or board committees, and provision of direction and prioritization to the General Auditor for these requests.

Applicable Policy

Metropolitan Water District Administrative Code Section 6450(f): Powers and Duties

Metropolitan Water District Administrative Code Section 6451: Audit Department Charter

Details & Background

The General Auditor prepares a risk-based annual audit plan in accordance with Metropolitan Administrative Code Section 6451 and professional internal auditing standards. This plan is flexible in nature and subject to change as risks evolve during the fiscal year and as the General Auditor deems it necessary to modify the plan. Additionally, the General Auditor may receive requests from individual board members or board committees to perform audit assignments that are not included in the approved annual audit plan.

Requests presented to the Audit Committee should include the risk or internal control concern and the objective or question to be answered by the audit or review.

A portion of Metropolitan Administrative Code Section 6450(f) relevant to this item states:

> The General Auditor may receive requests from time to time from the other executive officers or committees of the Board to perform audit assignments which are not included in the approved annual Audit Business Plan. Similarly, the General Auditor may identify a need to include new assignments in the Audit Business Plan during the year. The General Auditor shall have sufficient latitude and discretion to include those new assignments in the annual Audit Business Plan as the General Auditor deems necessary based upon their professional judgement and available resources. Requests from other committees of the Board and individual board members desiring specific audit assignments shall be submitted to the Audit Committee for study, advise, and recommendation. Once the audit assignment is approved by the Board, the General Auditor reserves the right to determine how to best fit the directed audit assignment into the Audit Business Plan.