Special Audit Committee

Annual Audit Risk Assessment & Internal Control Discussion

Item 7a

April 22, 2025

Item 7a
Annual Audit Risk Assessment & Internal Control Discussion

Subject

Annual Audit Risk Assessment & Internal 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 information on current risk data and facilitate a Board discussion of risks and internal control concerns

Next Steps

Audit Committee approval and Board approval of the General Auditor Business Plan for Fiscal Year 2025/26 on June 10, 2025

Creating the Risk-Based Internal Audit Plan

Creating the Risk-Based Internal Audit Plan

Administrative Code

645l(d)(l) Audit Department Charter: Responsibilities

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.

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 mandate
- Specify internal audit services that support Metropolitan
- Consider coverage of high-risk areas
- Identify resource requirements
- Be dynamic and timely

Creating the Risk-Based Internal Audit Plan

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

Understand the Organization

- Identify objectives, strategies, structure
- Review key documents
- Update audit universe
- Facilitate annual audit risk assessment & internal control discussion with the Board
- Hold management meetings
- Obtain internal audit staff input

Identify, Assess, and Prioritize Risks

Creating the Risk-Based Internal Audit Plan

- Understand the significance of independent assessment
- Identify business objectives, strategies, and risks
- Document risks
- Select risk assessment method
- Measure risks
- Score auditable units
- Validate risk assessment

Creating the Risk-Based Internal Audit Plan

Measure Risks

- Auditable unit
- Impact factors
  - Loss exposure – financial, reputational
  - Strategic risk – political, legal
- Likelihood factors
  - Control environment
  - Complexity
  - Assurance coverage
  - Board management concern
- Velocity

Score Auditable Units

Creating the Risk-Based Internal Audit Plan

- Risk factor weights
- Preliminary risk score
- Review 1
- Executive management review
- Review 2
- Final risk score
- Auditable unit ranking

Additional Planning Considerations

Creating the Risk-Based Internal Audit Plan

- Board and management requests
- Mandated audits (law or regulation)
- Mission-critical audits
- Coverage of risks by assurance providers
- Advisory or ad hoc requests
- Administrative activities
- Special projects or initiatives to improve internal audit
- Non-audit activities

Estimate Resources & Identify Engagements

Creating the Risk-Based Internal Audit Plan

- Assess internal audit staff knowledge, skills, abilities
- Coordinate coverage with other assurance providers
- Calculate available plan hours
- Prepare service portfolio
- Identify planned audits and advisory engagements
- Ascertain any additional skills required
- Determine any audit coverage limitations

Prepare the Audit Plan

Creating the Risk-Based Internal Audit Plan

- Executive summary
- Department overview
- Strategic goals
- Risk assessment process
- Risk assessment summary

- Service portfolio
- Planned audit and advisory engagements
- Risk coverage map
- Resource plan
- Organization chart
- Standards

Propose , Finalize, and Present Audit Plan for Board Approval

Creating the Risk-Based Internal Audit Plan

- Share audit plan with department heads
- Present the audit plan to the Audit Committee for approval
- Obtain board approval of audit plan
- Distribute the audit plan

Creating the Risk-Based Internal Audit Plan

Questions?

Internal Control

Administrative Code 2416(b)(4) Executive Committee: Duties & Functions

Consider the effectiveness of the District's internal control system, including information technology security and control.

Internal Control

What is 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

What is COSO Internal Control-Integrated Framework

- Released by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1992 and updated in 2013

- Recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control

- Future initiative for Metropolitan to adopt COSO

Internal Control

Components of COSO Internal Control-Integrated Framework

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

Component Examples

Internal Control

- **Control Environment** - Management establishes standards of conduct
- **Risk Assessment** - Management identifies, analyzes, and responds to risks related to achieving defined objectives
- **Control Activities** - Management segregates duties and responsibilities among different people to reduce risk of error, misuse, or fraud
- **Information & Communication** - Management communicates quality information throughout the entity using established reporting lines
- **Monitoring** - Management performs ongoing monitoring of the internal control system including regular management and supervisory activities, comparisons, and reconciliations

Internal Control

Control Environment

The foundation for the district's internal control system has five principles:

1. The Board and management demonstrate commitment to integrity and ethical values
2. The 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

Internal Control

Internal Control System Roles

EVERYONE has a responsibility for internal control:

- Board of Directors
- Management
- Staff

Organizational Objectives Categories

Internal Control

- Operations
- Reporting
- Compliance
- Safeguarding of assets

Internal Control

Questions?

Risk Discussion

Definition of Risk

What is a 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 Considerations

Risk Drivers

Direct – have a strong influence on how priorities and audit scope are set

- Regulations
- Financial impact
- Business opportunity

Indirect – may take longer to influence risk levels

- Politics
- Public opinion
- Social impact

SOURCE: Internal Audit Foundation 2025 Risk in Focus

Risk Considerations

Risk Areas

1. Business continuity
2. Climate change
3. Communications/reputation
4. Cybersecurity
5. Digital disruption
6. Financial liquidity
7. Fraud
8. Geopolitical uncertainty

SOURCE: Internal Audit Foundation 2025 Risk in Focus

Risk Considerations

Risk Areas (con't)

9. Governance/corporate reporting
10. Health/safety
11. Human capital
12. Market changes/competition
13. Mergers/acquisition
14. Organizational culture
15. Regulatory changes
16. Supply chain

SOURCE: Internal Audit Foundation 2025 Risk in Focus

Public Sector Internal Audit Focus

Risk Considerations

Operational and compliance risks receive the most audit effort:

1. Operational (22%)

2. Compliance/regulatory (20%)

3. Financial areas (9%)

4. Other IT (8%)

5. Cybersecurity (7%)

6. Enterprise risk management (7%)

SOURCE: IIA Pulse of Internal Audit 2025

Public Sector Internal Audit Focus

Risk Considerations

Other areas of internal audit effort include:

- Cost/expense reduction

- Fraud

- Governance and culture

- Third-party relationships

- External audit support

SOURCE: IIA Pulse of Internal Audit 2025

Audit Project Considerations

Risk Considerations

Public sector internal audits generally consider these areas:

- Compliance (85%)
- Operational efficiency (81%)
- Operational controls (73%)
- Fraud (73%)
- Enterprise risk management (55%)
- Cost/expense reduction (48%)
- IT (46%)
- Governance/culture (47%)

SOURCE: IIA Pulse of Internal Audit 2025

Audit Project Considerations

Risk Considerations

Other areas considered by public sector internal audits:

- Cybersecurity

- Business resilience

- Third-party relationships

- Financial reporting

- Privacy

- Sustainability

SOURCE: IIA Pulse of Internal Audit 2025

Artificial Intelligence

Risk Considerations

Internal audit involvement with artificial intelligence (AI):

- 65% planning to increase AI involvement

- 41% using AI for audit activities

- 25% using AI for advisory services

- 15% auditing how the organization uses AI

SOURCE: IIA Pulse of Internal Audit 2025

Risk Considerations

Digital Disruption

Defined as the risks and opportunities presented to an organization from emerging technologies, such as AI

Risk considerations for the impact of digital disruptions:

- Risk projected to rise from 4th to 2nd highest risk in 3 years globally
- Ranked in the top 5 risks by 48% of audit leaders in North America – expected to reach 70% in 3 years
- AI-driven risks impact areas such as cybersecurity, human capital, fraud, communications, and reputation
- Challenges include upskilling staff, adopting new tools, and global disparities in access to knowledge

SOURCE: IIA Risk in Focus 2025

Climate Change

Risk Considerations

Risk considerations for the impact of climate change

- Currently ranked relatively low
- Expected to rise from 13th to 5th highest risk in 3 years
- Sustainability reporting and compliance requirements are key drivers
- May cause supply chain disruptions, higher operational costs, flooding, and more
- Challenges include accurate reporting of sustainability initiatives and avoidance of reputational damage

SOURCE: IIA Risk in Focus 2025

Highest Risk Areas – Public Sector

Risk Considerations

In the public sector, technology drives the highest two risks:

- Cybersecurity (71%)
- Other IT (56%)
- Compliance/regulatory (48%)
- Third-party relationships (43%)
- Operational (33%)
- Cost/expense reduction (32%)

SOURCE: IIA Pulse of Internal Audit 2025

Board Discussion

Risk Considerations

- Risks

- Internal Control

- Associated Projects

Thank You

Presenters

- Scott Suzuki, General Auditor

- Kathryn Andrus, Assistant General Auditor

- Chris Gutierrez, Audit Program Manager

- Lina Tan, Principal Auditor

- Bonita Leung, Senior Auditor

The Metropolitan Water District of Southern California

Supplemental Slides

Board Committees & Functional Areas

Board Committees & Functional Areas

Risk Considerations

Executive

General Manager

Management and administration of district activities based upon board policy/direction, business planning and strategic priorities, enterprise risk management, control environment

Board Support Services

Administrative support to the Board and the Office of the Chair; board document management system

Board Committees & Functional Areas

Risk Considerations

<u>Engineering, Operations, and Technology</u>

Power Operations & Planning

CRA energy, renewable energy credits, GHG allowances, wholesale energy, electric reliability

Cybersecurity

Cybersecurity standards and policies, protect against cyber threats, SOC

Water Conveyance & Distribution

O&M for CRA, SWP, and distribution system (pumping plants, pipelines, service connections to member agencies, hydroelectric plants, storage, reservoirs)

Board Committees & Functional Areas

Risk Considerations

<u>Engineering, Operations, and Technology</u> (con't)

Water Operations & Planning

Plans and implements the movement and use of water resources, SCADA

Information Technology (General)

Governance and IT project management, infrastructure, applications and support (Oracle, WINS, WorkTech)

Operations Support

Manufacturing Services unit, Construction Services unit, Power & Equipment Reliability unit, Fleet Management, Facility Asset Management

Board Committees & Functional Areas

Risk Considerations

Engineering, Operations, and Technology (con't)

Infrastructure Reliability

Construction and procurement contracts, inspection, testing, surveying, right-of-way and property rights, condition assessments

Water Treatment

Treatment processes, drinking water regulation compliance; chemical handling, O&M for five water treatment plants

Water Quality

Chemical and biological analyses, optimizing treatment processes, testing new technologies; preserve and improve source water quality

Board Committees & Functional Areas

Risk Considerations

Engineering, Operations, and Technology (con't)

Planning

Facility, drought, & seismic resiliency planning, dam safety, hydraulic analysis/modeling, substructure protection, contract administration, engineering standards, CIP

Program Management

Planning/delivery of capital/O&M projects for treatment plants, systems, Pure Water, land planning & acquisition

Engineering Design

Technical assessments, designs for facilities, specifications for construction, technical support (construction, commissioning, operation)

Board Committees & Functional Areas

Risk Considerations

One Water & Adaptation

Sustainability, Resilience, and Innovation

Environmental & infrastructure issues, environmental responsibility, environmental impact; CAMP4W

Land Management

Easements, annexations, external leases, land use & protection

Centralized Grants & Research

State grants, federal grants, non-profit grants

Environmental Planning

Environmental laws and regulations compliance, CEQA, obtaining permits/approvals, habitat conservation

Board Committees & Functional Areas

Risk Considerations

One Water & Adaptation (con't)

Water Resource Planning and Development

Development of resource programs, projects, and infrastructure, IRP, LRP, WSDM, UWMP

Water Resource Implementation

Water resource programs, contracts, CRA, SWP, water transfers, water recycling, groundwater recovery, conservation

Bay Delta Initiatives

Delta Conveyance Project, Delta improvements, scientific research, protect/restore fish, wildlife, ecosystem

Board Committees & Functional Areas

Risk Considerations

<u>Legislation & Communications</u>

External Affairs

Legislative services, conservation & community services including education programs, member services & public outreach, media and communications, inspection trips

<u>Legal & Claims</u>

General Counsel

Represents Metropolitan in litigation and other proceedings, provides legal advice, drafts, reviews, and negotiates contracts, monitors and analyzes pending and enacted legislation

Board Committees & Functional Areas

Risk Considerations

<u>Finance, Affordability, Asset Management, and Efficiency</u>

Business Continuity

Strategies for critical operations during an emergency or other business disruption, business impact analyses, MetAlert

Administrative Services

Contracting/purchasing, inventory, warehousing, reprographics, technical writing, records, E-forms, enterprise content management, rideshare program

Revenue & Budget

Budget, cost-of-service development, rates, and charges recommendations; cost monitoring, analysis, and planning

Board Committees & Functional Areas

Risk Considerations

<u>Finance, Affordability, Asset Management, and Efficiency</u> (con't)

Treasury & Debt Management

Cashflow, banking, receipts, payments, debt obligations, disclosures, investor and bond rating agency relations; taxes, charges, p-card, petty cash

Controller

Billing, accounts payable, accounts receivable, payroll, and financial reporting, trust funds, fixed asset accounting

Risk Management

Casualty insurance, excess and specialty insurance policies to supplement self-insured liability and property program, contract risk

Board Committees & Functional Areas

Risk Considerations

<u>Organization, Personnel, and Effectiveness</u>

Human Resources

Development, training, classification and compensation, recruitment, benefits, HR systems

Operational Safety & Regulation

Complying with all regulatory and occupational health and safety regulations and requirements; training, EOC

Security

Protection of Metropolitan's Board of Directors, executive management, employees, patrons, infrastructure, equipment, and physical assets

Board Committees & Functional Areas

Risk Considerations

<u>Organization, Personnel, and Effectiveness</u> (con't)

Employee Relations

Employee relations, contract negotiations, performance management

Training

Workforce training programs, including planning, needs assessment, program development, and evaluation

Board Committees & Functional Areas

Risk Considerations

Community and Workplace Culture

Diversity, Equity, and Inclusion

Champions, educates and influences a diverse and inclusive work environment, disadvantaged business enterprise (DBE), workforce development, tribal outreach and engagement

Ethics

Promotes ethical culture & education, administers and advises on ethics policies; reviews ethics compliance, investigates violations

EEO

Non-Discrimination, EEOC, and OFCCP regulatory compliance