Audit Subcommittee of the Executive Committee

Annual Audit Risk Assessment & Internal Control Discussion

Item 3a

April 23, 2024

Item 3a
General Auditor FY 2024/25 Business Plan

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 a primer on risk and internal control
3. Facilitate a discussion of potential risks Metropolitan and its associated business functions face

Next Steps

Audit subcommittee approval and Board approval of the General Auditor Business Plan for Fiscal Year 2024/25 on May 28, 2024 and June 11, 2024 respectively

Creating the Internal Audit Plan

Creating the Internal Audit Plan

Administrative Code 6451(d)(1) Audit Department Charter: Responsibilities

Develop and present a flexible annual audit plan to the Executive 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 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

Creating the Internal Audit Plan

Annual Risk Assessment & Audit Plan

1. Understand the organization
2. Identify, assess, and prioritize risks
3. Coordinate with other providers
4. Estimate resources
5. Propose plan and solicit feedback
6. Finalize and communicate plan

Creating the Internal Audit Plan

Understand Metropolitan

- Identify business objectives, risks, and strategies
- Identify and review key documents
- Consult with key stakeholders
- Create the audit universe

Creating the Internal Audit Plan

General Auditor's Risk Assessment

- Significance of independent risk assessment
- Understanding Metropolitan's business objectives, strategies, and risks
- Documenting risks
- Risk assessment approach
- Measuring risks
- Validating risk assessment

Creating the Internal Audit Plan

Additional Planning Considerations

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

Creating the Internal Audit Plan

Estimate Resources

- Assess team skills
- Coordinate coverage with other assurance and consulting providers
- Identify any additional skills required
- Calculate available plan hours
- Identify planned audits and advisory projects

Creating the Internal Audit Plan

Draft the 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

Creating the Internal Audit Plan

Propose the Plan and Solicit Feedback

Share with the Board and senior management

- Results of the risk assessment
- How results drive the audit plan
- Confirm coverage of high-risk areas
- How engagements will add value to Metropolitan
- Disposition of any Board or management requests

Creating the Internal Audit Plan

Communicate to Finalize the Audit Plan

- Present the audit plan to the Audit Subcommittee of the Executive Committee and Executive Committee for approval
- Obtain board approval of audit plan

Creating the Internal Audit Plan

Questions?

Internal Control

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

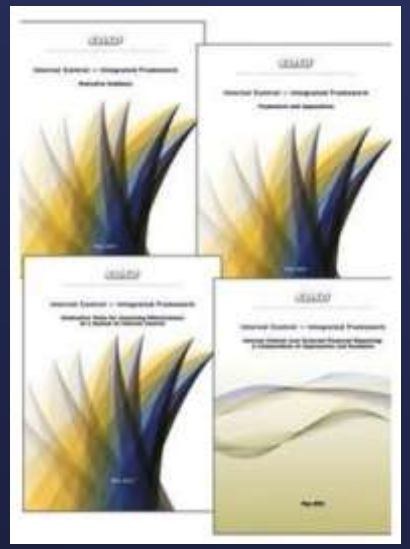
What is Internal Control?

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** - Effectiveness and efficiency of operations
- **Reporting** - Reliability of reporting for internal and external use
- **Compliance** - Compliance with applicable laws and regulations

SOURCE: COSO, May 2013

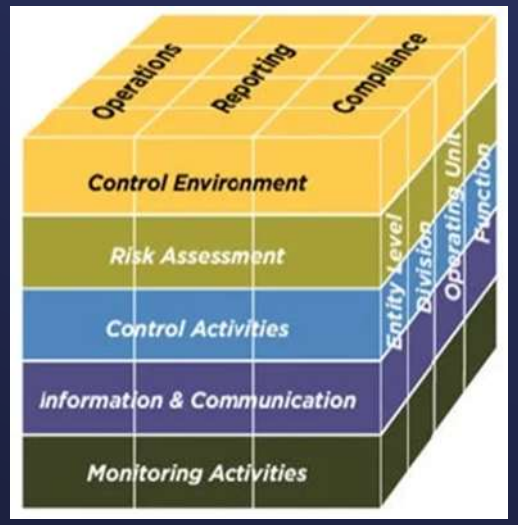
Internal Control



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

Internal Control

Examples

- **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

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

Internal Risks

- Integrity, ethical values, culture
- Role, authority, responsibility
- Management's philosophy and operating style
- Legal/compliance
- Organizational structure
- Governance-related decision-making
- Personnel and resource capabilities (e.g., capital, time, processes, systems, and technologies)
- Management of third-party business relationships
- Needs and expectations of key internal stakeholders
- Internal policies

Risk Considerations

External Risks

- Political
- Environmental
- Social
- Technological
- Economic
- Legal
- Regulatory

Risk Considerations

Non-Financial Risks

- Social responsibility
- Reputational
- Data governance
- Intellectual property
- Compensation
- Employee conduct
- Labor management
- Ethical and corporate culture
- Public health
- Diversity, equity, and inclusion
- Human resources
- Environmental (greenhouse gas emissions, waste management, material sourcing, climate change)

Risk Considerations

Board Committee & Functional Areas

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

Risk Considerations

Board Committee & Functional Areas

Engineering, Operations, and Technology

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)

Risk Considerations

Board Committee & Functional Areas

Engineering, Operations, and Technology (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

Risk Considerations

Board Committee & Functional Areas

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

Risk Considerations

Board Committee & Functional Areas

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)

Risk Considerations

Board Committee & Functional Areas

One Water & Stewardship

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

Risk Considerations

Board Committee & Functional Areas

One Water & Stewardship (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

Risk Considerations

Board Committee & Functional Areas

Legislation & Communications

External Affairs

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

Legal & Claims

General Counsel

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

Risk Considerations

Board Committee & Functional Areas

Finance & Asset Management

Business Continuity

Strategies for critical operations during 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

Risk Considerations

Board Committee & Functional Areas

Finance & Asset Management (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

Risk Considerations

Board Committee & Functional Areas

Ethics, Organization, and Personnel

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

Risk Considerations

Board Committee & Functional Areas

Ethics, Organization, and Personnel (con't)

EEO

Non-Discrimination, EEOC, and OFCCP regulatory compliance

Employee Relations

Employee relations, contract negotiations, performance management

Ethics

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

Risk Considerations

Board Committee & Functional Areas

Equity, Inclusion, and Affordability

Diversity, Equity, and Inclusion

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

Risk Considerations

Public Sector Internal Audit Focus

Operational and compliance risks receive the most audit effort:

1. Operational (20%)
2. Compliance/regulatory (19%)
3. Cybersecurity (11%)
4. Financial (10%)
5. Other IT (8%)

SOURCE: IIA Pulse of Internal Audit 2024

Risk Considerations

Internal Audit Focus

Other areas of internal audit effort include:

- Enterprise risk management
- Fraud
- Third-party relationships
- External audit support
- Cost/expense reduction
- Governance and culture

SOURCE: IIA Pulse of Internal Audit 2024

Risk Considerations

Audit Project Considerations

Internal audits commonly consider in each project:

- Fraud (92%)
- IT (68%)
- Governance/culture (67%)
- Cybersecurity (54%)
- Cost/expense reduction (55%)
- Third-party relationships (40%)
- Sustainability (24%)

SOURCE: IIA Pulse of Internal Audit 2024

Risk Considerations

Artificial Intelligence

Internal audit involvement with artificial intelligence (AI)

- 45% researching future use of AI
- 18% using AI for audit activities
- 12% auditing how the organization uses AI

SOURCE: IIA Pulse of Internal Audit 2024; based upon internal audit functions of 10 to 24

Risk Considerations

Highest Risk Areas

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

- Cybersecurity (77%)
- Other IT (56%)
- Third-party relationships (50%)
- Compliance/regulatory (37%)
- Enterprise risk management (32%)
- Governance/Culture (27%)
- Cost/expense reduction (27%)

SOURCE: IIA Pulse of Internal Audit 2024

Risk Considerations

Prior Audit Risk Assessment

Areas previously identified as higher audit risk:

- Business Continuity
- Cybersecurity
- Human Resources
- Power Operations & Planning
- Water Conveyance & Distribution

Risk Considerations

Board Briefing

1. Cybersecurity
2. Human Capital
3. Market Changes
4. Business Continuity
5. Current Risk Ranking
6. Future Risk Expectations

SOURCE: IA Foundation Risk on Focus 2024

Risk Considerations

Board Discussion

- Risks
- Internal Control
- Associated Projects

Thank You

Presenters

- Scott Suzuki, General Auditor
- Kathryn Andrus, Deputy General Auditor
- Chris Gutierrez, Audit Program Manager
- Andrew Lin, Principal Auditor
- Bonita Leung, Senior Auditor
- Faviola Sanchez, Deputy Auditor III


THE METROPOLITAN WATER DISTRICT OF
SOUTHERN CALIFORNIA
1928