Developing an Effective Internal Audit Program

May 5, 2025

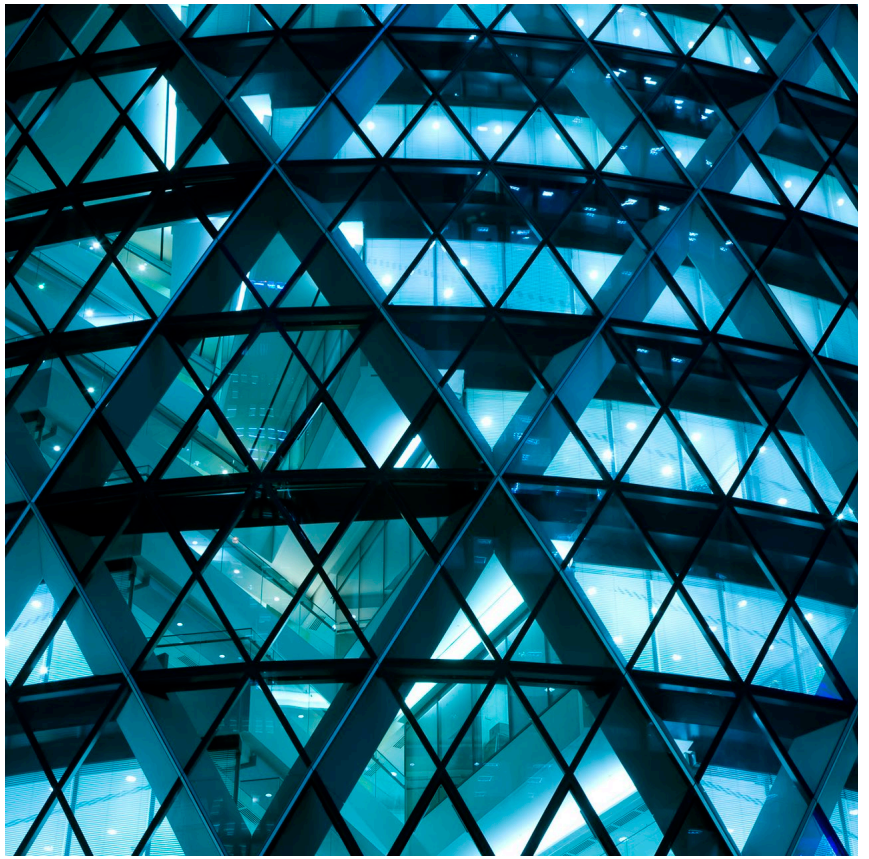
forvis mazars

Introduction

- Senior Manager in national Internal Audit practice
  - Experience includes serving as the lead project manager to provide full outsourced internal audit services for Chicago market
- Internal Audit professional
  - 22 years of internal audit experience
  - Including 18 years of leading internal audit functions as chief audit executive
- Started career in public accounting (assurance practice for 12 years)
- Certified Internal Auditor (CIA) and Certified Public Accountant (CPA)
- Member of the Institute of Internal Auditors (IIA) and the American Institute of CPAs (AICPA)

Agenda

1. Why Internal Audit?
2. Prepare and Organize
3. Develop and Execute
4. Maintain and Continuously Improve
5. Internal Audit Execution – Practical Tools / Examples
6. Q & A



01

Why Internal Audit?

Purpose of Internal Audit*

Internal auditing **strengthens** the organization's **ability** to **create, protect, and sustain value** by providing the board and management with **independent**, **risk-based**, and **objective assurance**, **advice**, **insight**, and **foresight**.

Internal Audit enhances organization's ability to:

- Achieve its objectives
- Have strong governance, risk management and controls
- Improve decision making and oversight
- Increase reputation and credibility with stakeholders
- Serve the public interest

Internal Audit's effectiveness is driven by:

- Competent professionals following Global Internal Audit Standards
- Being independently positioned with direct accountability to the board
- Being free from undue influence and maintaining objectiveness

* Source: The Institute of Internal Auditors' Global Internal Audit Standards (2024)

forvis mazars

What Can Go Right?

The Value of Improved Business Processes

Process Improvement Can Drive Organizational Value By

- Enhancing efficiency
- Reducing costs
- Improving customer satisfaction
- Increasing employee engagement
- Improved regulatory compliance

What Can Go Wrong?

The Value of Internal Controls – Trust but Verify!

10 / 80 / 10 Rule

- Based on fraud presentation from former FBI Special Agent (for organizations in general), his professional judgement concluded:
  - 10% of employees would never steal
  - 10% of employees will likely steal at some point in time
  - 80% of employees may or may not steal, depending on situation

Good people can make bad decisions

Proper control environment/procedures foster good decisions

forvis mazars

The 80% - What Can Happen
A Case Study

- Female All-American athlete and honor student
- Came from strong supportive family
- Career started with small growing company - she worked very hard
- 1st theft - not initially intended (failed to reimburse employer for personal flight)
- Based on personal budget at home and due to reduced income for time off with a new baby, it perpetuated into various cases of theft in which she would say “I will only do this one more time.”

The 80% - What Can Happen
A Case Study

- She ended up stealing more than $500,000 over four years
- Her world came crumbling down after guilt got to her / turned herself in
- She went to prison for 18 months (5 weeks after giving birth)
- As she took her first steps into federal prison, she looked through the glass panels in prison hallway and saw her parents crying as they held her baby
- At that time, she realized she not only hurt herself and her employer but also her family

02

Prepare and Organize

Determine the Governance Structure

Ultimate Accountability is Key

Dual Reporting for Internal Audit is effective & aligns with professional standards

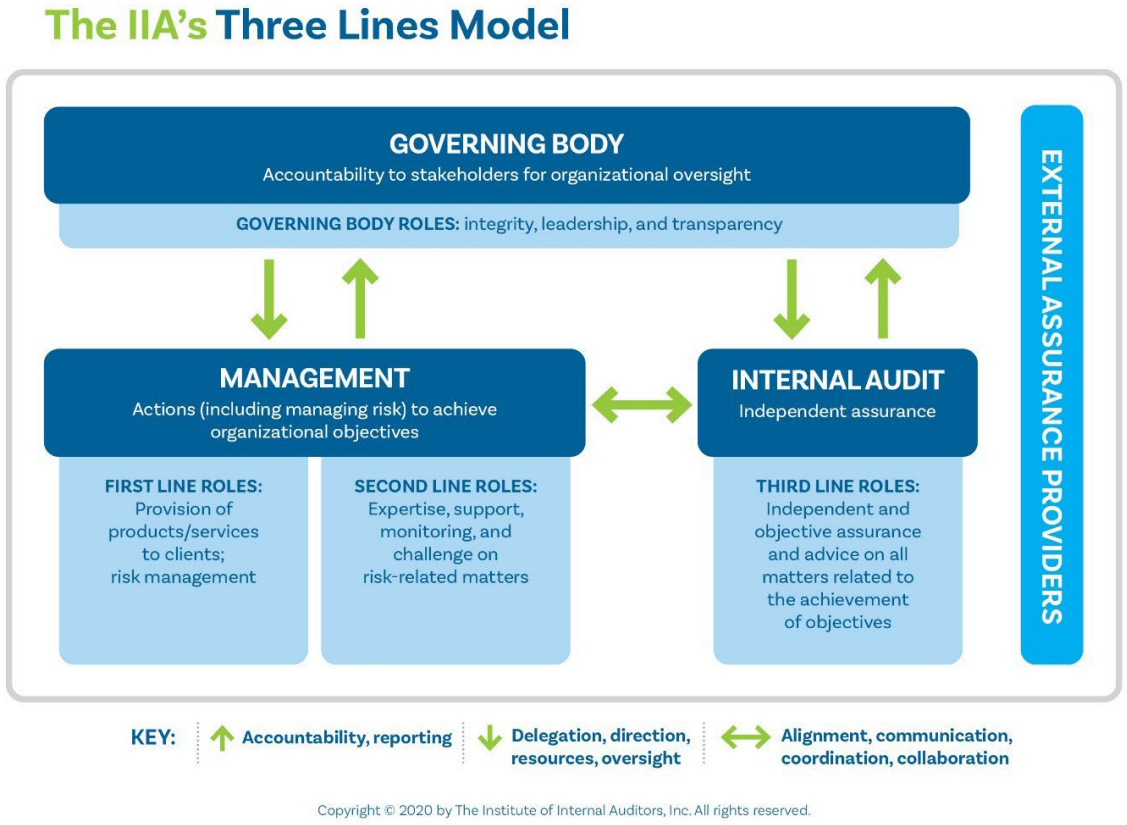
- Functional reporting - board of directors committee, such as an audit or finance committee
- Administrative reporting - senior management such as CEO or CFO

Demonstrates organizational commitment and independent stature

Determine the Governance Structure

The Three Lines Model* – A Best Practice

- Board
  - Provide Oversight
- Management (1st Line)
  - Most directly aligned with delivery of products/services
- Management (2nd Line)
  - Assists with managing risk
- Internal Audit (3rd Line)
  - Provide independent and objective assurance and consulting



* Source: The Institute of Internal Auditors

Determine the Governance Structure
Develop an Internal Audit Charter

- What is an Internal Audit Charter?
  - A formal mandate that provides the IA function the ability to perform its duties and responsibilities
- A charter should:
  - Establish position within organization
  - Authorize access
  - Grant authority
  - Detail reporting structure
  - Communicate purpose
  - Outline responsibilities

Determine the Operating Structure
Building the Right Team / How They Will Operate

- There are 3 primary options to choose from to determine the size and make-up of the internal audit team
  - In-house – Staffed by internal employees
  - Co-source – Staffed with a combination of internal and external resources
    - Common example – Hire Chief Audit Executive (CAE) to lead IA function and then fully or partially staff with external resources
  - Outsource – Fully staffed using a third-party service provider

Determine the Operating Structure

Building the Right Team / How They Will Operate

Consideration Points

1

In-House

- Maintain institutional knowledge
- Sole focus is on organization
- Potential source of future management talent

2

Co-Source

- IA leadership maintained in-house
- Flexible staffing
- Access to 3rd party specialists
- Quicker start-up

3

Outsource

- Fastest start-up option
- Access to 3rd party tools and methodologies
- Flexible staffing

forvis mazars

Determine the Operating Structure

Building the Right Team / How They Will Operate

Consideration Points

1

In-House

- Slowest start-up option
- Need to develop methodology and tools
- Staffing is least flexible
- Limitations on breadth of specialized resources

2

Co-Source

- Scalable
- Allows for an internal employee liaison with service provider

3

Outsource

- Scalable
- Recommend an internal employee liaison
- Utilize service provider to assist in plan to transition to co-source or in-house model

03

Develop and Execute

Developing the Game Plan

Steps to Deploying the Internal Audit Function

Once the governance and operating structure is defined, the team can get to work. The following are the key steps to functional deployment:

- Identification of the audit universe
- Developing a risk-based internal audit plan
- Audit engagement execution and reporting of results
- Follow-up audit procedures
- Building internal relationships

Identification of the Audit Universe

Understand the Organization / Define the Scope

- Understand organizational strategy and objectives
- Break organization down into functions, divisions, departments, etc.
  - These are areas of the organization that could be audited
- Develop a basic list of business processes
  - Key activities that help organization achieve objectives
- Inventory the key IT systems that support the business operations

Ensure that all relevant areas of the organization are included

Identification of the Audit Universe
Performing a Risk Assessment

- Identify potential risk areas considering auditable entities documented
- Use interviews or surveys to capture input from management from all functional areas of organization
- Consider external factors such as industry, geography, market conditions and regulatory environment
- Coordinate with ERM function within the organization, if applicable
- Score risks identified based on likelihood and potential impact
    - Often documented on a risk heat map

Communicate results of risk assessment and audit universe to management and board committee for feedback

Developing a Risk-Based Internal Audit Plan
Tailoring a Plan for Your Organization

- Identify audit engagements that address significant risk areas
- An internal audit plan should include a blend of the following:
  - Risk areas rated as high or moderate risks
  - Rotational assessment of critical business process areas
    - E.g. - Disbursements process; financial close and reporting
  - Assurance and consulting (advisory) engagements
    - According to a survey* of CAE's, the future ideal state for internal audit activity would be 60% assurance / 40% advisory

* Source: 2025 IIA Leadership Academy (current state – 75% assurance; 25% advisory

Developing a Risk-Based Internal Audit Plan
Tailoring a Plan for Your Organization

- Consider available resources and estimate requirements
  - In-house vs. external resources
  - Specialized expertise, such as IT audit skills
- Obtain management's input and propose plan to board committee
- Finalize the plan and schedule resources appropriately

Developing a Risk-Based Internal Audit Plan

Tailoring a Plan for Your Organization

Best Practice Ideas

- Plans often cover a 3-to-5-year timeframe
- Must be flexible for adjustments, based on current needs and changes in risk factors
- Cannot audit everything in a single year
- Start with engagements that may yield "quick wins"
  - Non-complex areas that can be completed in short period of time
- Allocate some budgeted hours each year for ad-hoc requests that may arise during each year

Audit Engagement Execution

The Plan to Conduct Each Audit Project

- Phases of an internal audit engagement
  - Planning
  - Fieldwork
  - Reporting
- Supervision and review throughout the engagement
  - Internal audit management should actively supervise and review audit work throughout each step of the engagement

Audit Engagement Execution

Planning Phase

- Gather background information including relevant data points
- Hold discussions with management to obtain business expertise and insight
- Identify engagement level risks to be evaluated
- Finalize scope, timeline and deliverables with management before fieldwork begins

Planning is the key to an effective and efficient internal audit project

Audit Engagement Execution

Fieldwork Phase

Common Practices for Performing Fieldwork

- Review relevant documentation gathered in planning phase
- Perform walk-throughs of in-scope business processes
- Document understanding of processes via flowcharting or narratives
- Prepare Risk and Control Matrix to document risks and controls
- Perform validation procedures to test controls
- Conclude on assessment results
  - Best Practice – Utilize data to support audit observations

Audit Engagement Execution
Reporting Phase

- Debrief engagement results with management to validate accuracy of results
- Prepare report to summarize audit observations and recommendations
- Obtain management's response and related action plans
- Periodically, summarize all engagement results for presentation to management and applicable board committee (i.e. – quarterly)

Follow-Up Audit Procedures

Steps to Follow-Up on Previously Reported Results

- Maintain a log of previously reported audit recommendations
- Track status of management action plan implementation
- Perform testing procedures to validate corrective action (scope based on risk level of reported issue)
- Report action plan progress and validation testing results to senior management and board committee

Follow-up audit procedures help facilitate accountability and continuous improvement to business process and controls

forvis mazars

Building Internal Relationships
Being Viewed as a Trusted Business Advisor

- Effective internal audit departments communicate regularly
- Routine connection points with management at all levels
  - "Stay in the know"
  - Be the team that management wants to call for assistance
  - Get invited to provide consulting before system/process changes
- Periodic internal control tips to management (via intranet/email)
- Maintain independence
  - Cannot make management decisions
  - Avoid conflicts of interest (in fact and in appearance)

04

Maintain and Continuously Improve

Maintain and Continuously Improve

Adhere to Standards / Quality Assurance

How to Maintain Quality

- Follow the IIA's Global Internal Audit Standards
- Implement a Quality Assurance and Improvement Program (QAIP)
- Periodic internal and external reviews to ensure conformance to IIA standards
- Internal Audit team members to maintain ethical standards and continuing professional education (CPE)
- Communicate results of QAIP to management and the board

Maintain and Continuously Improve

IIA Global Internal Audit Standards

International Professional Practices Framework*

International Professional Practices Framework®
(IPPF)

* Source: The Institute of Internal Auditors' Global Internal Audit Standards (2024)

forvis mazars

Maintain and Continuously Improve

Periodic Internal and External Assessments*

The Internal Audit Function Should Have Ongoing Evaluation

- Some form of internal assessments should be completed annually
- External Quality Assessments (EQA) must be conducted at least once every 5 years
  - Full-scope EQA – to be performed by qualified, independent assessor
  - Self-assessment with independent validation (SAIV)
    - Internal audit completes self-assessment
    - Qualified, independent assessor provides independent validation

* Source: The Institute of Internal Auditors' Global Internal Audit Standards (2024)

forvis mazars

05

Internal Audit Execution

Practical Tools / Examples

Internal Audit Execution - Practical Examples

COSO* Internal Control Framework

Management and Internal Audit Tool

- Widely accepted internal control framework
- The COSO cube is a structured way to think about internal controls
- Can be used by
  - Management – to establish controls
  - Internal audit – to assess controls

* *Internal Control – Integrated Framework* (Committee of Sponsoring Organizations of the Treadway Commission (COSO))

Internal Audit Execution - Practical Examples

Internal Control Maturity - Communication Tool

Assess at Process or Entity Level (insight for management)

Ad-Hoc >	Not Accountable >	Defined >	Managed >	Optimized >
▪ Control structure not defined / random occurrence	▪ Controls exist but lack documentation / adequacy / consistency	▪ Control structure documented / standardized / integrated	▪ Control process is regularly measured, assessed and tested	▪ Continuous process improvement / focused on mitigating risk

Lack of Control → Best In Class

forvis mazars

Internal Audit Execution - Practical Examples

Quick Start Wins

Evaluate if Basic Blocking / Tackling Is In Place

Examples of timeless internal controls:

- Timely account reconciliations
- Proper journal entry approval process
- IT Security access to key functions (i.e. – wire transfers)
- Proper handling of cash receipts and deposits
- Defined limits of authority

Monitoring Controls are Key

Helps Mitigate Segregation of Duties Risk

forvis mazars

Internal Audit Execution - Practical Examples

Quick Start Wins

Assess Management's Controls – Cash Disbursements

Review physical and IT security access for:

- Vendor master file – access to add / make vendor changes
- Processing accounts payable checks
- Processing electronic disbursements (ACH's, Wire Transfers)
  - Use of Multi-Factor Authentication (MFA)

Internal Audit Execution - Practical Examples

Data Analytic Examples

Look for Patterns in Data – Cash Disbursements

- Duplicate payments
- Vendor disbursements to employee addresses
- High volume / low average $ invoices (below DOA levels)
  - Example fraud – in excess of $1 million with only 1 level of management approval

Internal Audit Execution - Practical Examples

Proactive Recommendations to Management

Periodic Fraud Prevention Tips

- Reporting / Analysis / Reconciliations
  - Ensure periodic follow-up questions are asked to team members (including remote workforce); Let everyone know “you are looking”
- Invoices / Contracts
  - “Pause before you sign” – Signatures without thought make it easy for those who are trying to fool you
- Make “surprise” visits to remote locations
- Be alert to your surroundings – managers are first line of defense

Internal Audit Execution - Practical Examples

Other Tools for Assessing Internal Controls

- Reporting on key data / metrics
  - Can include simple reporting in Excel
  - More advanced reporting with data mining tools
- Self-assessment surveys from process and control owners
- Segregation of duties matrices
- Confidential Hotline
- Be creative

Your approach is creative. Unfortunately, we won't be able to use it because we have never done something like this before.

Internal Audit Execution – Practical Examples

Segregation of Duties (SOD)

Tool to Assess SOD Risk

Cash Disbursements			
Category of Duties	**Primary Activities / Sub-Processes**	**Who Performs Function**	**Mitigating Controls for Conflicting Duties**
Authorization	1. Initial 2. Secondary	1. Field management 2. Corporate management	No segregation of duties issues noted
Custody of Assets	1. Process check requests 2. Distribute checks	1. Accounts Payable 2. Administrative staff	No segregation of duties issues noted
Recording	1. Approve journal entries	1. Controller	No segregation of duties issues noted
Control Activity (i.e. – reconciliation)	1. Reconciles G/L to A/P subledger	1. Accounting staff	No segregation of duties issues noted

forvis mazars

•06

Questions?

Thank You

forvis mazars

Contact

Forvis Mazars

Jeff McCall, CIA, CPA

- Senior Manager
- P: 816.489.4225
- jeff.mccall@us.forvismazars.com