The Auditor’s Toolbox: Useful Tools and Techniques for the First Line of Defense

Presented By:
The Office of Internal Audit

Brenda Muirhead, Chief Auditor
Overview

- Introduction to Internal Audit
- The Three Lines of Defense Model
  - 1st line – Operational Management
  - 2nd line – Risk Management and Compliance Functions
  - 3rd line – Internal Audit
- Internal Controls and Fraud Awareness
Introduction to Internal Audit

Internal Audit Structure

• Administratively to the President
• Functionally to the Board

Internal Audit Purpose

Provide independent, objective assurance and advisory services that add value and accountability while driving improvement to the operations of the University.
Introduction to Internal Audit

Internal Audit Role

• Part of the administrative structure that helps units achieve their objectives, whom in turn help the University achieve its overall mission.

• Serve the University by protecting it from external and internal threats. This is done by assessing risks, advising on internal controls, investigating instances where the process lacked internal controls, and advising on corrective action plans.

• Assist leadership in striving to provide the maximum benefits while making the most efficient use of resources. This is done by identifying areas to increase efficiency and effectiveness of operations and minimizing occurrences of fraud, waste, and abuse.

Internal Audit Services

- Consulting: Facilitated Self Assessments, Consulting Engagements, Awareness Training
The Three Lines of Defense Model

1st Line: Functions that own and manage risks
2nd Line: Functions that oversee risks
3rd Line: Functions that provide independent assurance

Adapted from ECIIA/FERMA Guidance on 8th EU Company Law Directive, article 41
The Three Lines of Defense Model

1st Line of Defense: Operational Management

• Operational management naturally serves as the first line of defense because controls are designed into systems and processes under the guidance of operational management.

• There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events.

• The majority of fraud is detected at the first line:
  ▪ Reported to or discovered by management
  ▪ Reported to internal audit
  ▪ Reported to fraud and ethics hotline
    o Website: www.uoregon.ethicspoint.com
    o Toll Free: 1-855-388-2710
The Three Lines of Defense Model

1st Line of Defense: Operational Management

Managers that own and manage risks are responsible for:

- Identifying, assessing, controlling, and mitigating risks.
- Guiding the development and implementation of university policies.
- Designing, implementing, and maintaining written internal procedures.
- Maintaining effective internal controls.
- Implementing corrective actions to address process and control deficiencies.
- Ensuring that activities are consistent with goals and objectives.
The Three Lines of Defense Model

2nd Line: Functions that oversee risks

Adapted from ECIIA/FERMA Guidance on 8th EU Company Law Directive, article 41
The Three Lines of Defense Model

2nd Line of Defense: Risk Management and Compliance Functions

• Established by leadership to help build or monitor the first line-of-defense controls – but does not set the risk appetite

• Also ensures the first line is properly designed, in place, and operating as intended

• Second line typically includes:
  
  ▪ A risk management function (e.g. Enterprise Risk Services, Strategic Enterprise Risk Management and Compliance Committee)
  
  ▪ A compliance function (e.g. Athletics Compliance Officer, Research Compliance Services, HIPAA Compliance Officer, IT Security Officer)
  
  ▪ A controllership function (e.g. Business Affairs Office)

• Certain functions operate at the university-wide level; others are only relevant on a departmental level

• May intervene directly in modifying and developing internal control and risk systems; therefore cannot offer truly independent analyses to governing bodies regarding risk management and internal control
The Three Lines of Defense Model

2nd Line of Defense: Risk Management and Compliance Functions

Responsibilities of these oversight functions include:

- Supporting management policies, defining who is responsible, and setting goals for implementing
- Providing risk management framework
- Identifying known and emerging issues
- Identifying shifts in the organization’s chosen risk appetite
- Assisting management in developing processes and controls to manage the risks, issues, and shifts identified
- Identifying opportunities and areas for improving existing processes
- Provide guidance and training on risk management processes
The Three Lines of Defense Model

3rd Line: Functions that provide independent assurance

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Adapted from ECIIA/FERMA Guidance on 8th EU Company Law Directive, article 41
The Three Lines of Defense Model

3rd Line of Defense: Internal Audit

• Internal Audit provides the Board and Senior Management with comprehensive assurance based on the highest level of independence and objectivity within the organization not available in the second line of defense.

• Internal Audit provides assurance on the effectiveness of governance, risk management, and internal controls. This includes reporting on the performance of the first and second lines of defense in risk management and control objectives.
The Auditor’s Toolbox

• What if the first line of defense had the same tools the auditors use?

• What types of things would the auditor be looking for?

• If we passed all external audits, are we good?

• Is the program designed around compliance or does it maximize efficiency and effectiveness?

• Does the program’s internal controls align with the risk tolerance?

• Are controls preventative or detective?

• Are controls manual or automated?
The Auditor’s Toolbox

- Is trust an internal control?
- Are internal controls based on the people or the processes and systems?
- Are transactions authorized by the appropriate position?
- Most importantly, are the authorizations documented?
- Are adequate policies in place?
  - Are policies relevant to current processes?
  - Are policies reviewed periodically?
  - Do all employees have access to the policies?
  - Are new employees aware of the policies?
  - Are employees held accountable?
  - Are procedures in place to address policy violations?
The Auditor’s Toolbox

- Are procedures documented and approved by the department?
- Are transactions verified by another person?
- Are accounts reconciled and by who?
- Are key duties performed by separate employees? Why does this matter?
- Are processes monitored and modified when gaps are identified?
- Does information and communication flow through the organization horizontally and vertically?
- Why does employee turnover matter?
- Why are performance evaluations important?
The Auditor’s Toolbox

- How comfortable are you about the:
  - Accuracy and reliability of data?
  - Security of data?

- Do you feel comfortable reporting concerns to your superiors?

- Who is held accountable when something goes wrong?

- Can internal controls be bypassed without detection?
Fraud = “A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.”

- Includes any intentional or deliberate act to deprive another of property or money by guile (sly or cunning intelligence), deception, or other unfair means.
- Fraud is more likely to be detected by tips than by any other method.
- Most fraudsters exhibit behavioral traits that can serve as warning signs of their actions.
- Red flags generally will not be identified by traditional internal controls.
- Managers, employees, and auditors should be educated on these common traits to help identify patterns that might indicate fraudulent activity.
Internal Controls and Fraud Awareness

What should you do if you suspect fraud?

- If an employee is aware of fraudulent activity – they are obligated to report it.

- If something makes you uncomfortable or you aren’t sure what to do, call Internal Audit and discuss your concern. 541-346-6541

- The Oregon Government Ethics Law applies to all elected and appointed officials, employees and volunteers at all levels of state and local government in all three branches. Consult the Oregon Government Ethics Commission http://www.oregon.gov/OGEC/

- For situations where you prefer to make an anonymous report, the University contracts with an external provider to manage ethical and fraudulent concerns. Reports can be made through the following website: www.uoregon.ethicspoint.com or by calling 855-388-2710
Questions?