IT Risk Management: IT Audit

Agenda – Purpose of Presentation

- Define Purpose of IT Audit Coverage
- Identify Scope of IT Audit/Risk Based Audit
- Describe Roles and Responsibilities
- Identify Supervisory Expectations

Purpose of IT Audit

- Provides Risk-Focused evaluation of the effectiveness of controls over IT risks
- Evaluates risk management, internal controls and compliance with policies
- Remains risk-focused to ensure right scope, depth, and focus
- Promotes current and sound internal controls
- Ensures timely resolution of audit deficiencies
- Informs the board of the effectiveness of risk management

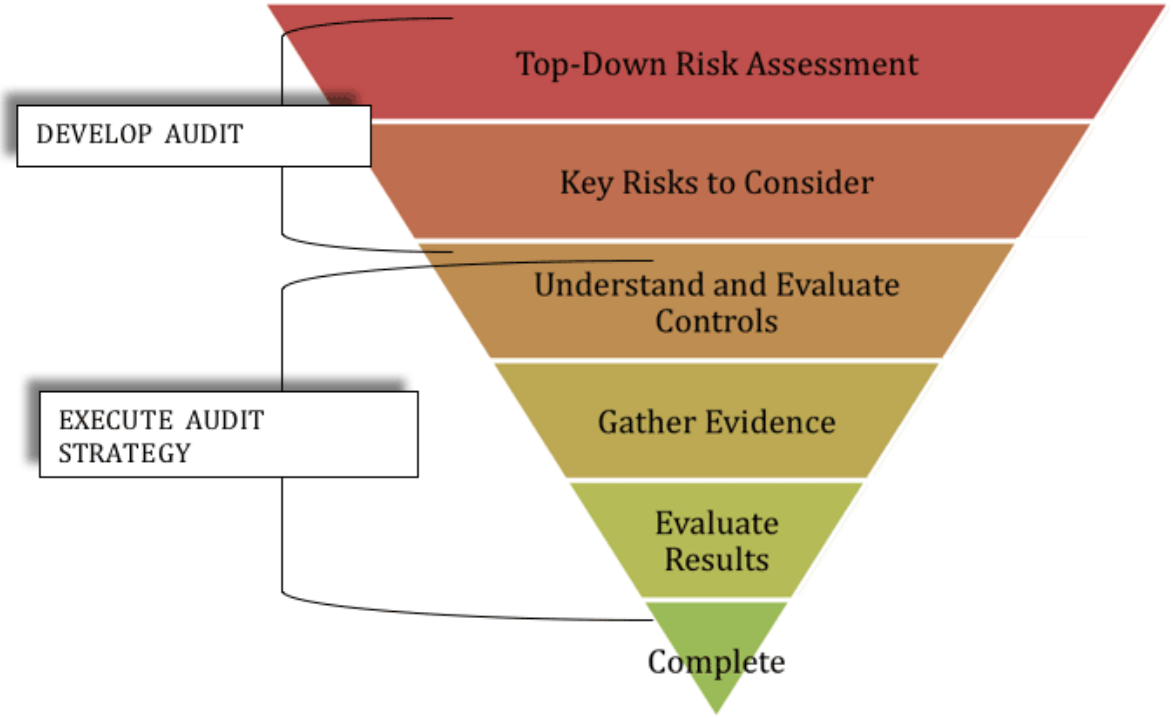
Scope of IT Audit

Dynamic nature of IT emphasizes importance of risk-based audit work, some areas for consideration include:

- IT management
- IT strategic planning
- Data center operations
- Client/server architecture
- Local and wide area networks
- Telecommunications
- Physical and information security
- Electronic banking
- Systems development
- Business continuity planning

Risk Based Auditing

- An effective risk-based auditing program will cover all of an institution's major activities.
- The frequency and depth of each area's audit will vary according to the risk assessment of the area.
- The audit program should be appropriate for the size and complexity of the institution.

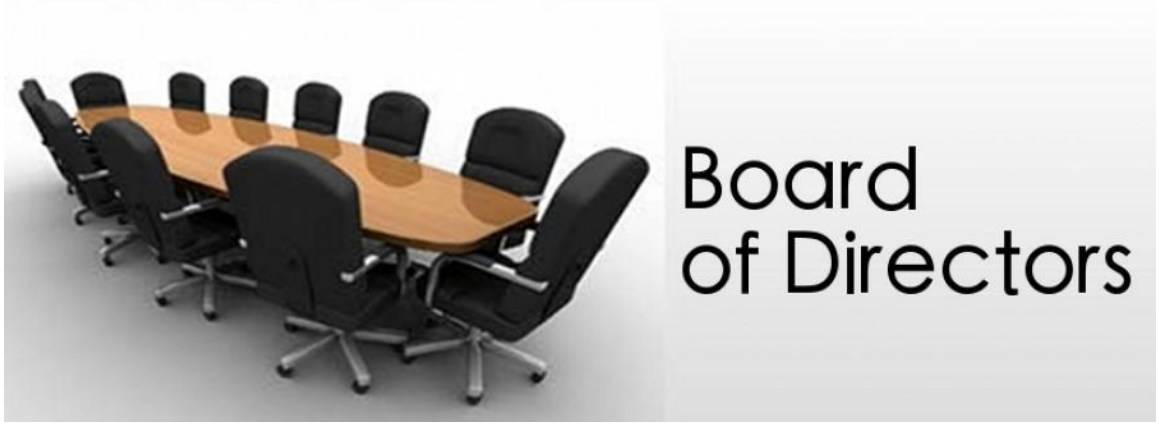


Risk Based Auditing

- Risk-based IT audit programs should:
  - Identify data, application and operating systems, technology, facilities, and personnel
  - Identify business activities and processes
  - Include profiles of significant business units, departments, and product lines or systems, and associated business risks and control features
  - Document the structure of risk and controls throughout the institution
  - Annual board or audit committee approval
  - Implement the audit plan
  - Include a program that monitors the risk assessment and updates it at least annually.

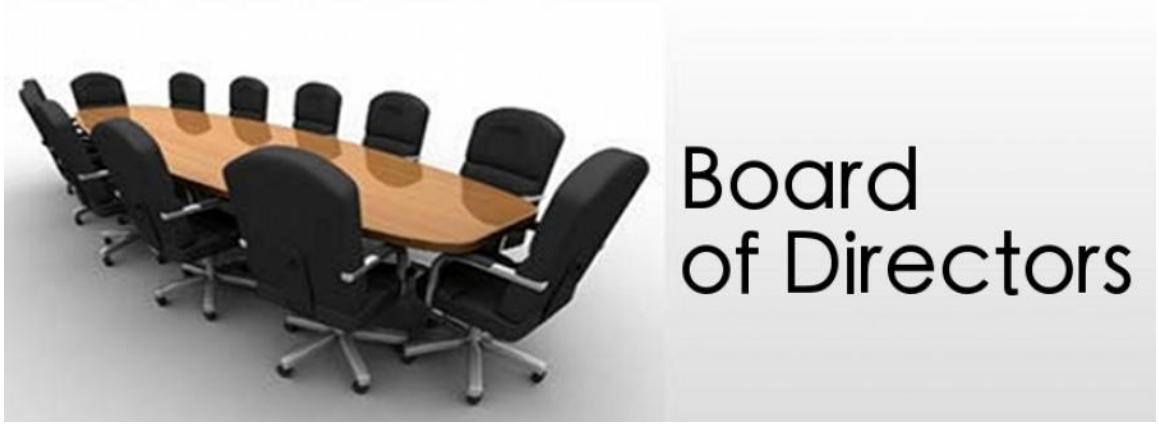
Board of Directors / Senior Management

- Responsible for ensuring that the system of internal controls operates effectively through an effective internal audit function.
  - Provide an internal audit function capable of evaluating IT controls
  - Engage outside consultants or auditors to perform the internal audit function, or
  - Use a combination of both methods to ensure adequate IT audit coverage.
- Establish an audit committee to oversee audit functions and report to full board on significant audit matters.



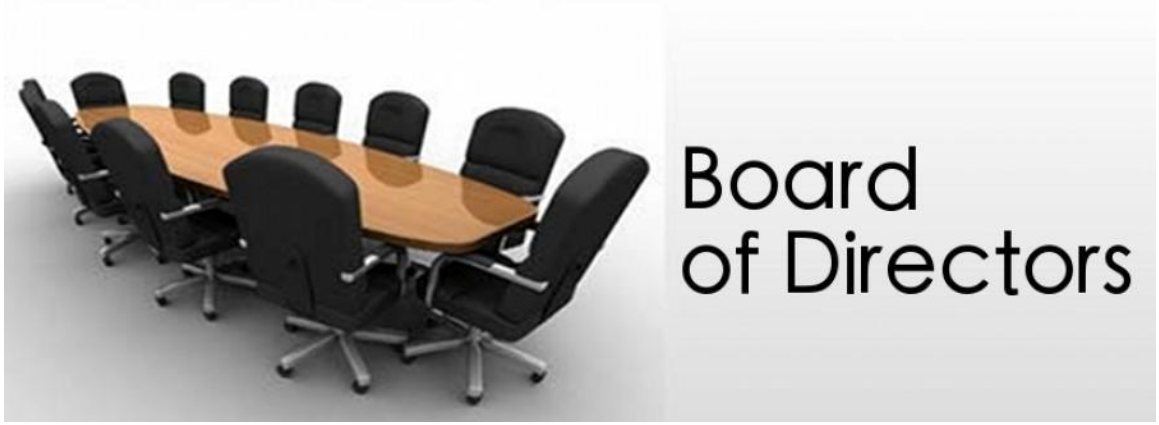
Board of Directors / Senior Management

- Ensure that written guidelines for conducting IT audit have been adopted
  - Review and approve audit strategies, policies and programs
  - Monitoring the effectiveness of the audit function
- Assign responsibility for the internal audit function to a member of management – internal audit manager.
- Ensure independence of the internal audit function.



Board of Directors / Senior Management

- Be aware of and understand significant risks and control issues associated with the institution's operations including risks in new products, emerging technologies, information systems, and electronic/mobile banking.
- Board and audit committee members should seek training to fill in knowledge gaps.
- Meet periodically with internal and external auditors to discuss audit work performed and conclusions reached on IT systems and controls.



Audit Management

- Implementing board-approved audit directives
- Oversee the audit function
- Provide leadership and direction in communicating and monitoring audit policies, practices, programs, and processes.
- Establish clear lines of authority and reporting
- Ensure the necessary independence, experience, education, training, and skills

Internal Audit Manager

- Internal control risk assessments
- Audit plans
- Audit programs
- Audit reports
- Oversee audit staff
- Provide policies and procedures to guide audit staff
- Ensure adequate expertise and resources to identify inherent risks and assess effectiveness of controls in IT operations

Internal Audit Staff

- Assess independently and objectively the controls, reliability, and integrity of IT environment.
- Evaluate IT plans, strategies, policies, and procedures to ensure adequate management oversight.
- Assess day-to-day IT controls to ensure compliance with policies and standards set forth by the board
- Operational audits and systems development audit to ensure appropriate internal controls are in place

Internal Audit Staff

- Identify weaknesses
- Review management plans for addressing weaknesses
- Monitor resolution
- Report to the board or audit committee on material weaknesses

Operating Management

- Formally and effectively respond to IT audit or examination findings and recommendations
- Correcting root causes of the audit or control exceptions

- Audit should:
  - Document, report and track recommendations and outstanding deficiencies, and
  - Conduct timely follow-up audits to verify the effectiveness of management's corrective actions for significant deficiencies.

External Auditors

- Review IT controls and part of overall evaluation of controls when providing as opinion on the adequacy of an institution's financial statements.
- Review general and application controls affecting financial statement preparation and reporting.
- Extent of work needs to be clearly defined in the engagement letter.
  - Scope
  - Objectives
  - Resource requirements
  - Audit timeframe
  - Resulting reports

Independence

- Board of directors should ensure that audit department does not participate in activities that may compromise, or appear to compromise independence
- Determining independence:
  - Position with organization and line of reporti
  - Activities and responsibilities
  - Free from management interference
  - Access to needed records
  - Adequate staffing
  - Periodic discussions with or presentations to audit committee or board of directors
  - Requirement that management respond formally and timely to significant adverse audit findings

Outsourcing Internal IT Audit

- Contract between institution and a third-party to provide internal IT audit services
- An acceptable practice used institutions of varying sizes and complexities
- May take many forms varying from providing expertise to internal audit staff on a particular project to the come outsourcing of all internal audit work
- Board and senior management retain all responsibility
- Institution should conduct appropriate due diligence
- Ensure proper oversight of outsourced internal audit work

Evaluating IT Audit

- Directorate Oversight
- Independence
- Risk assessment
- Audit planning
- Scope
- Audit work papers
  - Timeliness and quality of reports
  - Thoroughness and quality of work papers
- Monitoring and resolution of issues
- Qualifications of IT auditors
- Effective reporting to Board & other Stakeholders

Evaluating IT Audit

- Qualification of Internal & External IT auditors
  - Training
  - Expertise
  - Experience
  - Credentials

Supervisory Considerations

Structure and Reporting

- Organizational structure, committee membership and reporting relationships
- Reporting process and disposition of potential issues
- Management and scoping of external auditor engagements
- Board approval of independence, audit charter and internal standards
- Accountability for and status of plan
- Regularity and content of reports and board packages
- Board awareness and involvement in modifications to plan and target dates for issues

Supervisory Considerations

Quality of the Work Performed

- Root cause of issue identified
- Significant risks covered: information security, cybersecurity, business continuity, vendor management
- Audit schedules/cycles tie to audit universe/risk assessment
- Repeat audit findings clearly identified
- Findings and conclusions accurately depict operating environment
- Findings noted in work papers are the same as those reported to management
- Independently report audit issues to senior management/Board

Supervisory Considerations

Management Responsiveness

- Issue tracking and reporting process (Outstanding issue report)
- Audit department independence and standards
- Management response captured with estimated completion date