Lecture 3: The Audit Process

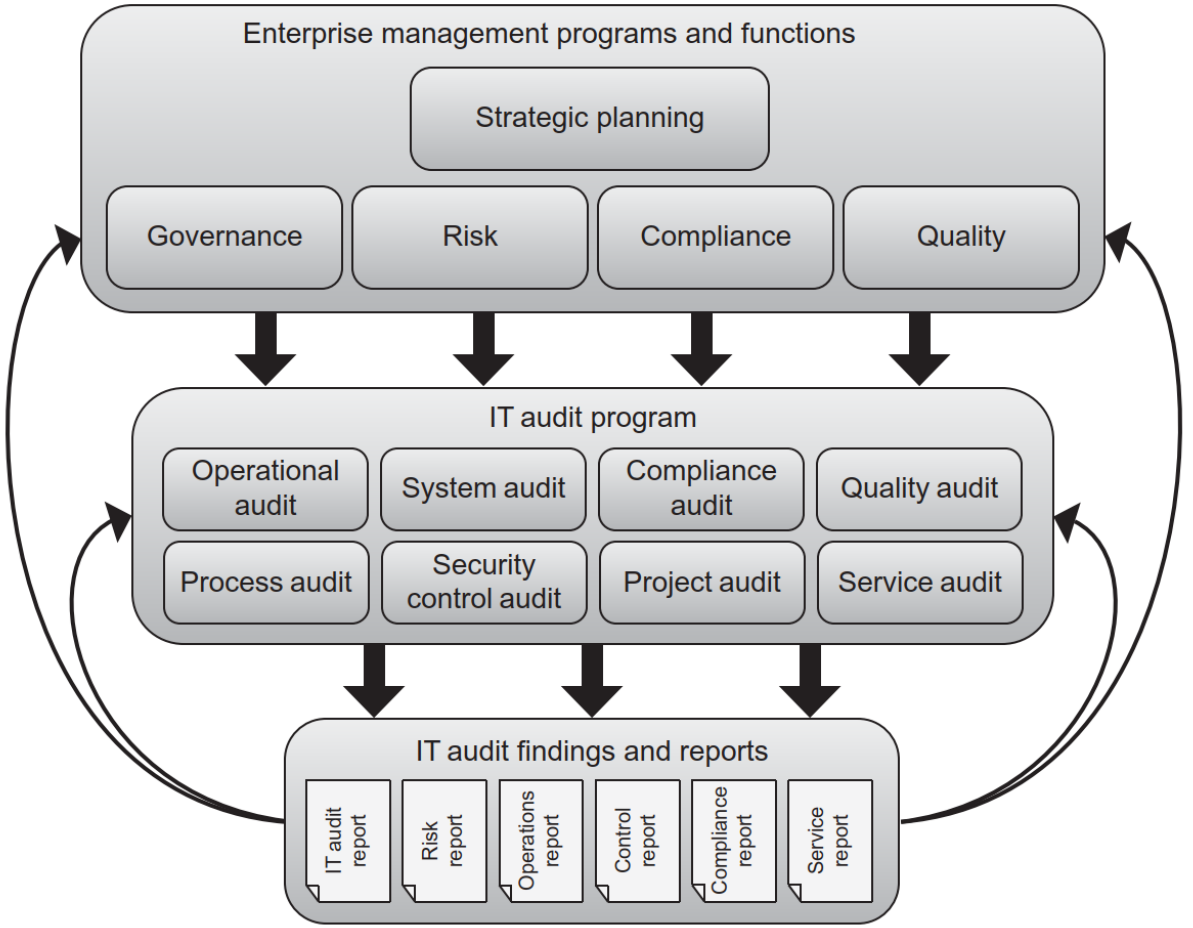
Aron Kondoro

IS 369: IT Audit & Controls

Introduction

- The IT audit process supports the work of the financial/operation audit by providing reasonable assurance that information and information technology are processing as expected

IT Audit in Context



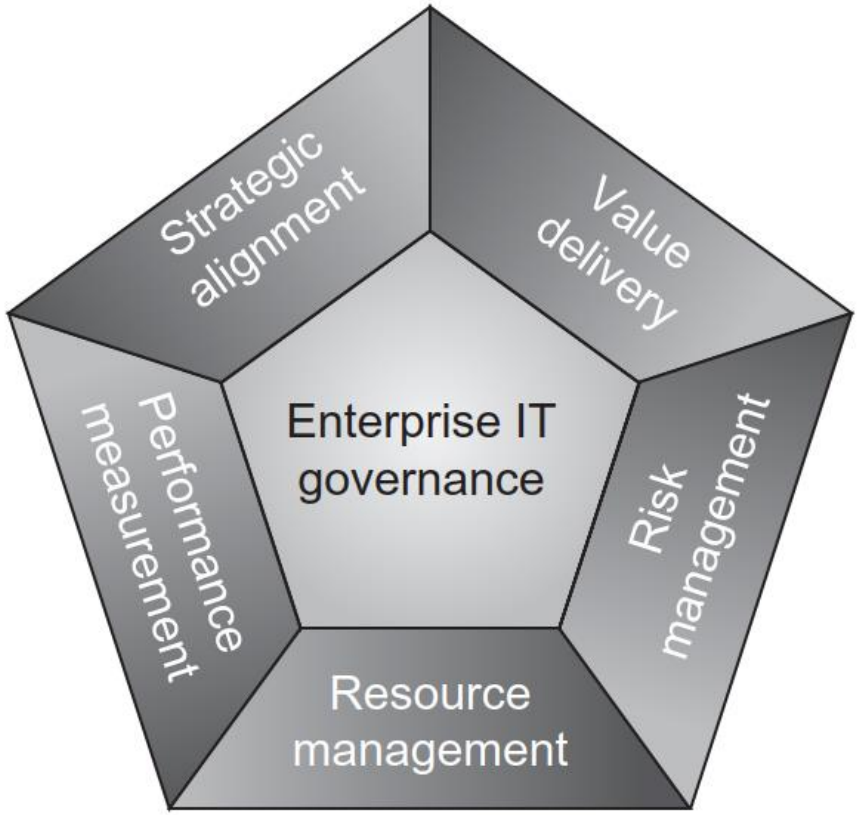
IT Governance

- The term ***governance*** in business contexts refers generally to the set of policies, processes, and actions taken by management to define organizational strategy and operate the organization in a way intended to help realize its business goals and objectives
- ***IT governance*** refers to the structure and processes organizations use to try to ensure that their IT operations support the overall goals and objectives of the organization

IT Governance

- According to the IT Governance Institute, governance objectives applicable to virtually any organization include
  - aligning IT strategy with enterprise strategy
  - allocating IT resources efficiently to support the achievement of organizational objectives and realize the value anticipated from IT investments
  - performance measurement to allow organizations to assess to what extent they are achieving their objectives
  - effectively managing IT-related risk

IT Governance Focus Areas



IT Governance Processes

- IT governance comprises a wide range of processes and controls for applications, systems, networks, infrastructure, personnel, and data centres and other facilities, including:
  - IT-related policies
  - standard operating procedures
  - management plans
  - performance monitoring and management
  - supervisory or oversight functions
  - IT controls and control monitoring
  - system and software development processes and
  - operations and maintenance activities.

IT Governance Scope and Frameworks

- The IT governance function and its associated processes and activities can apply at multiple levels of an organization
  - internal controls
  - business functions and processes
  - Infrastructure
  - system operations and maintenance
  - individual projects
  - enterprise-wide
- IT Governance frameworks
  - Control Objectives for Information and Related Technology (COBIT)
    - principles, policies and frameworks; processes; organizational structures; culture, ethics and behavior; information; services, infrastructure and applications; and people, skills and competencies
  - ISO/IEC 38500
    - focuses on corporate IT governance, emphasizing high-level principles and recommendations that organizational executives or other leaders with responsibility for governance should consider

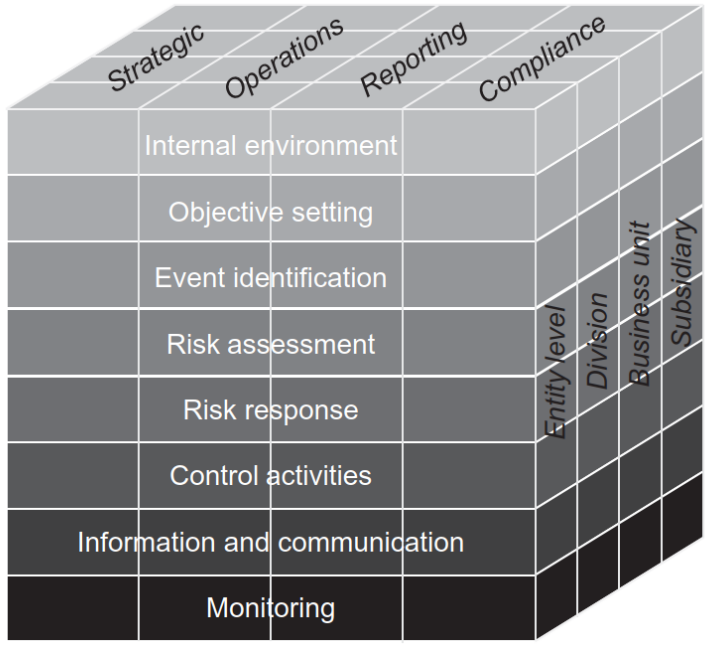
Risk Management

- The International Organization for Standardization (ISO) defines risk simply as the ***effect of uncertainty on objectives***
- a function of threats and vulnerabilities applicable to an organization, where the magnitude of risk is expressed in terms of the ***impact*** that could occur should a potential threat materialize and the ***likelihood*** of that occurrence

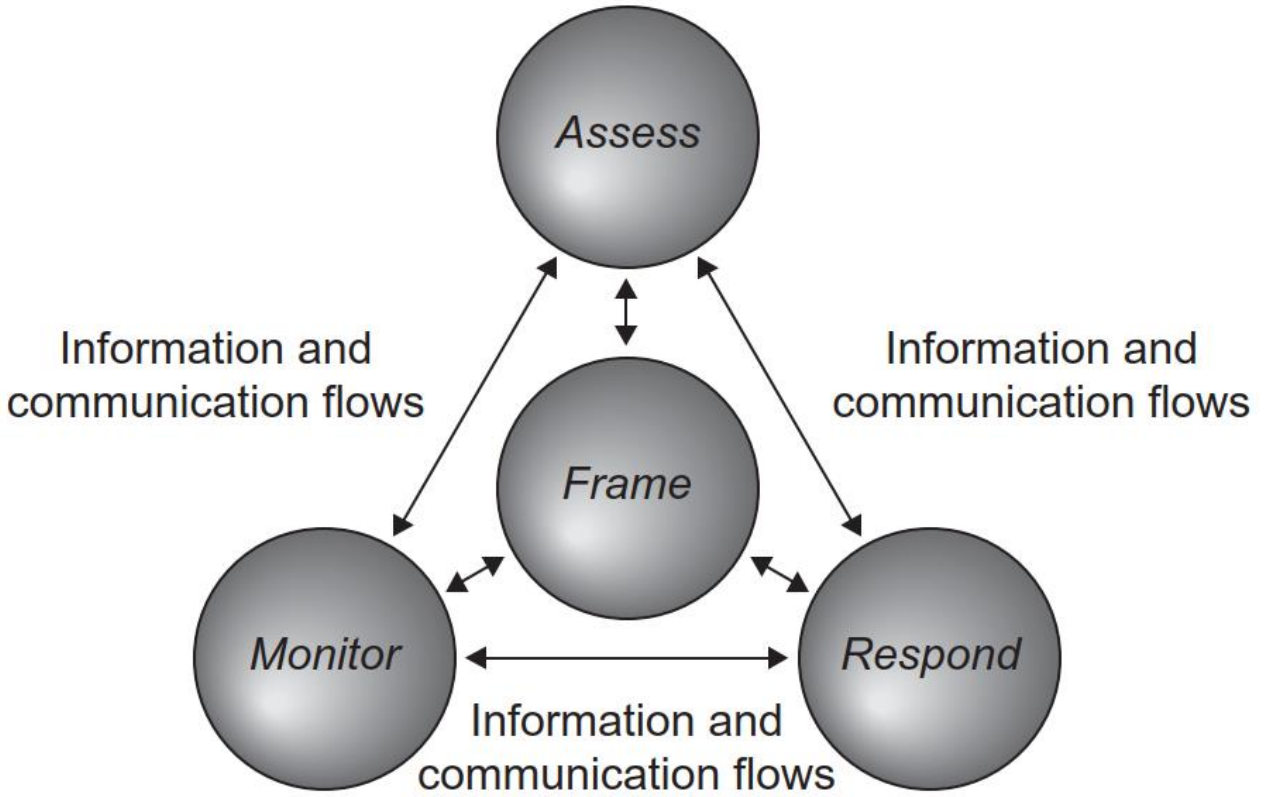
IS 369: IT Audit & Controls

Committee on Sponsoring Organizations of the Treadway Commission (COSO)

- an integrated risk management perspective spanning all types of risk, all levels of an organization, and multiple types of organizational objectives



Risk Management



Role of IT Audit in Risk Management

- Risk Management identifies assets in an organization and evaluates the threats and other sources of risk to those assets
  - The results of risk management activities influence the way the IT audit program plans and conducts audits
  - Findings and recommendations from IT audits represent important inputs into ongoing risk planning, assessment, and response
  - focusing first on IT processes or components assessed to have the highest risk or on those considered to be of greatest value to the organization
- IT audits are an important internal source of vulnerability information
  - Common Vulnerabilities and Exposures (CVE) database, the Computer Emergency Response Team Coordination Center (CERT/CC)

Compliance and Certification

- **Compliance** is one dimension of governance used to measure progress or organizational maturity
  - consider all requirements applicable to an organization and assess the extent to which the organization meets those requirements, identifying any gaps or failures to satisfy requirements that may exist
- **Certification** is a special type of compliance
  - organizations typically adopt standard processes or methodologies in a specifically prescribed manner and then have their compliance evaluated by an external entity explicitly authorized to grant certification

Types of Organizational Certifications

Certification Focus	Certifications
Quality management	• ISO 9001 • ISO 14001
Information security management	• ISO/IEC 27001 • Cybertrust
Service management	• CMMI for services • ISO/IEC 20000
Service organization controls	• SSAE 16 • ISAE 3402 • SOC 2 and 3
Process improvement	• CMMI • ISO/IEC 15504 • Six Sigma
Products or technologies	• Common criteria • CESG assisted products scheme (United Kingdom) • FIPS (United States)

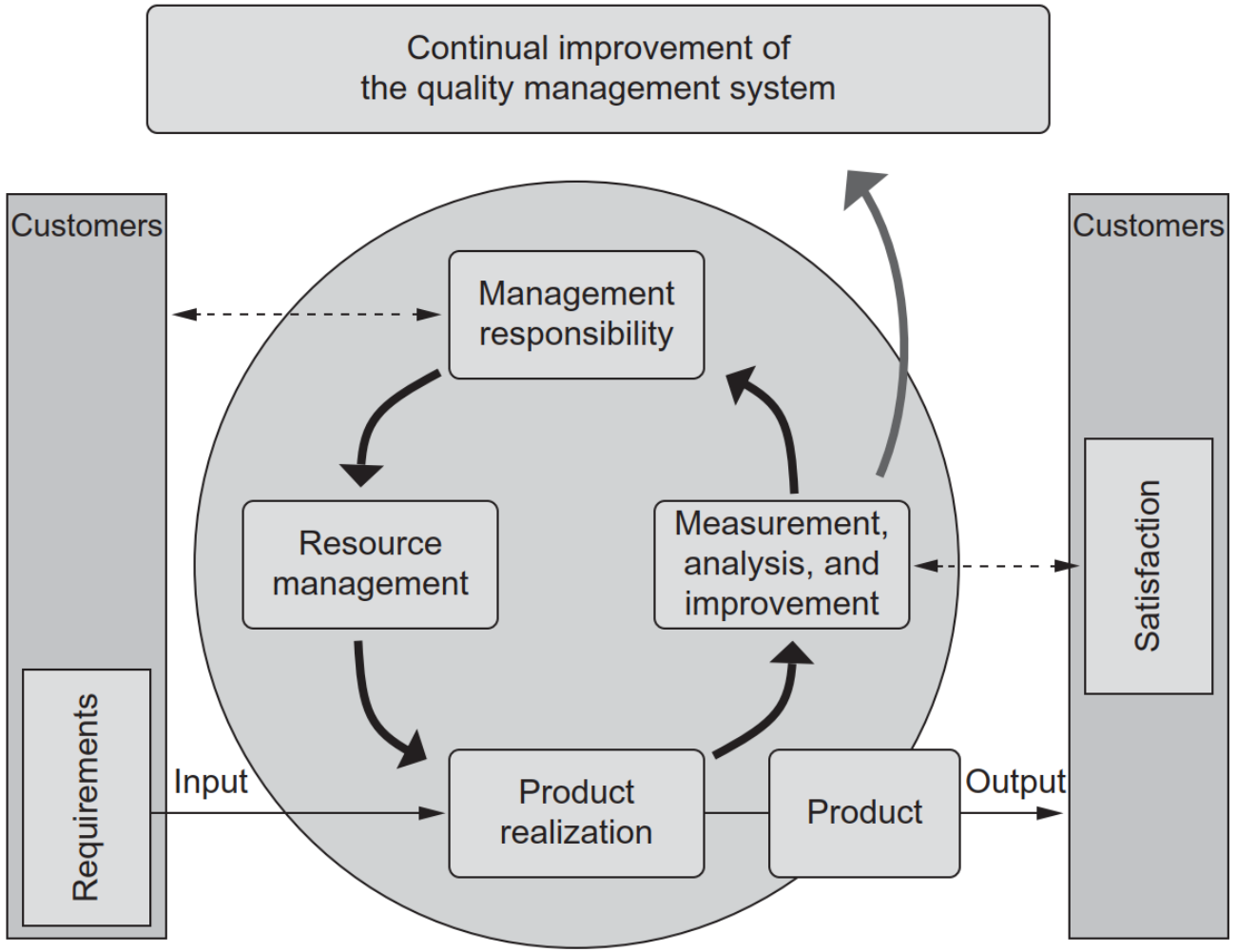
Management of Compliance and Certification

- Subject of external audits intended to enable an objective determination by an outside entity of adherence to regulatory or industry standards or certification criteria
- Organizations need their own internal processes to assess certification and compliance to help ensure that they conform to applicable requirements and can demonstrate evidence of their compliance if and when they need to

Quality Management and Quality Assurance

- ***Quality assurance*** refers to the processes associated with achieving and maintaining a desired level of quality in a product or service
- ***Quality control*** focuses on maintaining consistent quality over time
  - E.g. meeting a specific standard or producing a product with characteristics satisfying prescribed criteria or falling within a specified tolerance level
- ***Quality management*** comprises all coordinated activities related to quality including quality planning, quality assurance, quality control, and quality improvement

Quality Management Process – ISO 9001



Role of IT Audit in Quality Management

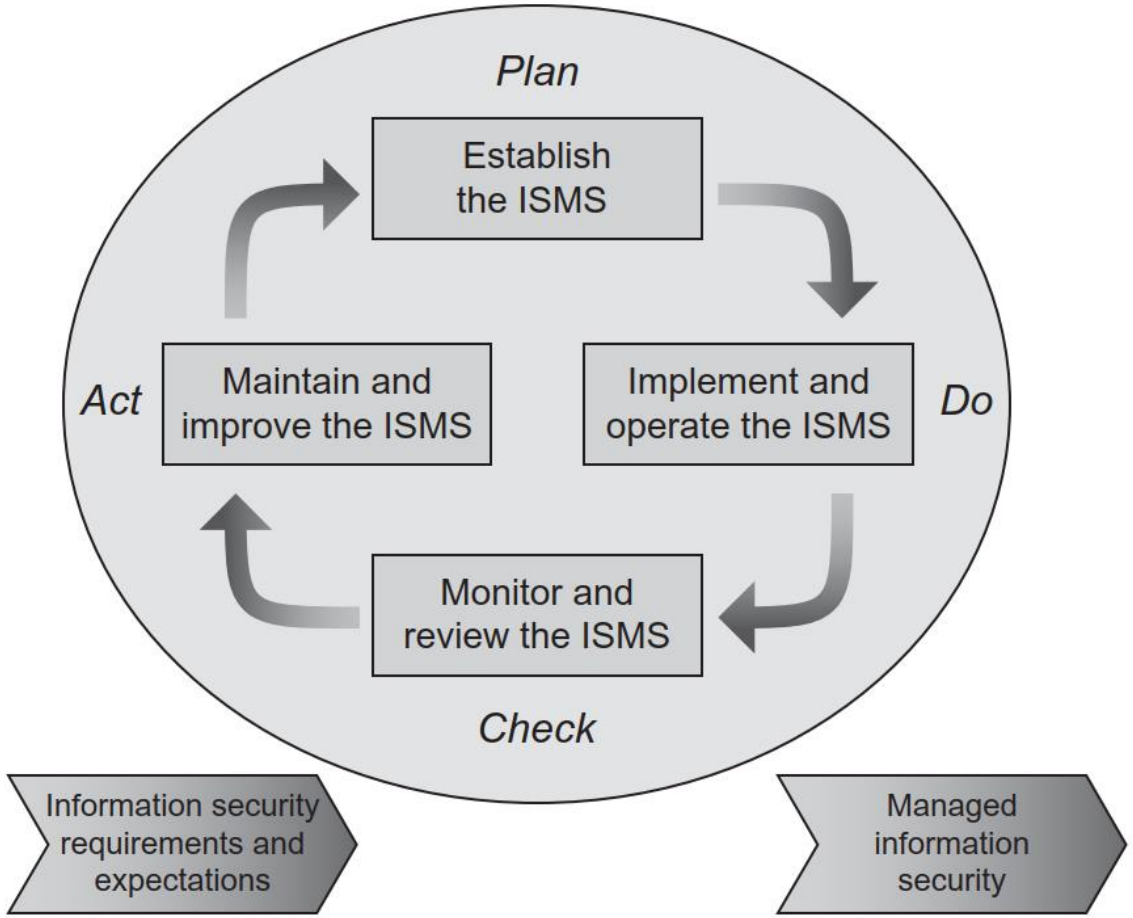
- IT auditing supports organizational quality management functions by confirming that operational processes produce the intended result and that the outputs of those processes satisfy quality-related criteria
- The results of IT audits performed in support of quality assurance can either
  - Confirm adherence to quality criteria and achievement of quality objectives
  - identify deviations from product specifications or service levels that become targets for corrective action

Information Security Management

- Security controls—administrative, technical, and physical—are the primary focus of information security management and of the IT auditing or assessment activities performed in support of information security programs
- ***Information security management*** entails the **selection, implementation, configuration, operation, and monitoring of security controls** sufficient to protect the **confidentiality, integrity, and availability** of information systems and the data they contain
- In current practice, information security management emphasizes
  - continuous monitoring of security controls
  - independent security control assessments to gauge the effectiveness of the controls organizations implement and maintain

IS 369: IT Audit & Controls

Information Security Management Standards - ISO/IEC 27001



Role of IT Audit in Information Security Management

- Information security management supports IT auditing by taking responsibility for implementing and correctly configuring internal controls related to security
- IT auditing also supports information security management, by
  - providing detailed, critical examinations of internal controls implemented to achieve security objectives
  - confirming that IT operations match organizational policies, procedures, standards, and guidelines.
- Information security management programs are also the subject of IT audits

Audit Universe

- Document key business processes and potential audit areas
- Incorporate enterprise-wide risk assessment
- Establishes a risk-based internal audit process
- COBIT provides a comprehensive list of IT processes

Audit Universe

- Audit universe includes
  - Basic functional audit area
  - Organizational objectives
  - Risks of not achieving objectives
  - Controls that mitigate the risks

Exhibit 3.1 Example of an Audit Universe Related to the IT Area of an Organization

Basic Functional Audit Area: Information Technology *Organization's Objective: To provide secure access to financial information, technology, and services for all authorized employees.*			
Key Business Process	*IT Audit Objective*	*IT Risk*	*IT Mitigating Control*
Access Control Management	System's security is appropriately implemented, administered, and logged to safeguard against unauthorized access to or modifications of programs and data, that result in incomplete, inaccurate, or invalid processing or recording of financial information.	Users possess privileges that are not consistent with their job functions, thus allowing unauthorized or incorrect modifications to financial or accounting data, which could cause segregation of duties conflicts, unprevented or undetected errors, incorrect financials, or management decisions based upon misleading information.	User access privileges are periodically reviewed by application owners to verify access privileges remain appropriate and consistent with job requirements.
Change Control Management	Programs and systems are appropriately implemented in a manner supporting the accurate, complete, and valid processing and recording of financial information.	Developers or programmers have the ability to promote incorrect or inappropriate modifications or changes to financial data, programs, or settings into the production processing environment, thus resulting in invalid accounting data and/or fraud.	Application systems, databases, networks, and operating systems are developed, modified, and tested in an environment separate from the production environment. Access to the development and test environments is appropriately restricted.
Management of Data Center, Network, and Support	Data are appropriately managed to provide reasonable assurance that financial data remain complete, accurate, and valid throughout the update and storage process.	Financial reporting information and accounting data cannot be recovered in the event of system failure, impacting the entity's ability to report financial information according to established reporting requirements.	Backups are archived off-site to minimize risk that data are lost.

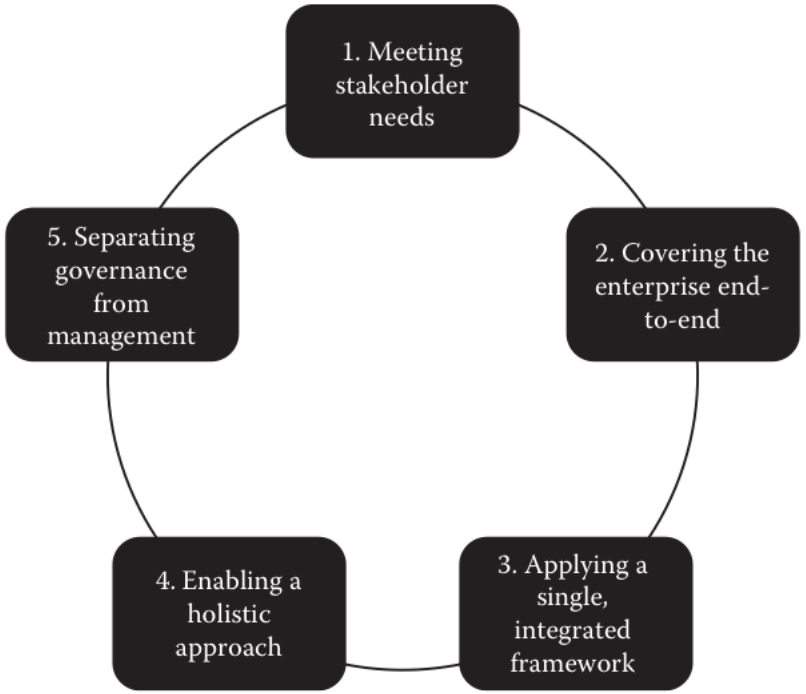
Audit Standards

- Professional Organizations:
  - American Institute of Certified Public Accountants (AICPA)
    - Generally Accepted Auditing Standards (GAAS)
    - Statements of Auditing Standards (SAS)
  - Financial Accounting Standards Board (FASB)
    - Generally Accepted Accounting Principles (GAAP)
  - The Institute of Internal Auditors (IIA)
    - Statements on Internal Auditing Standards (SIAS)
  - Information Systems Audit & Control Association (ISACA)
    - COBIT- Control Objectives for Information Technology

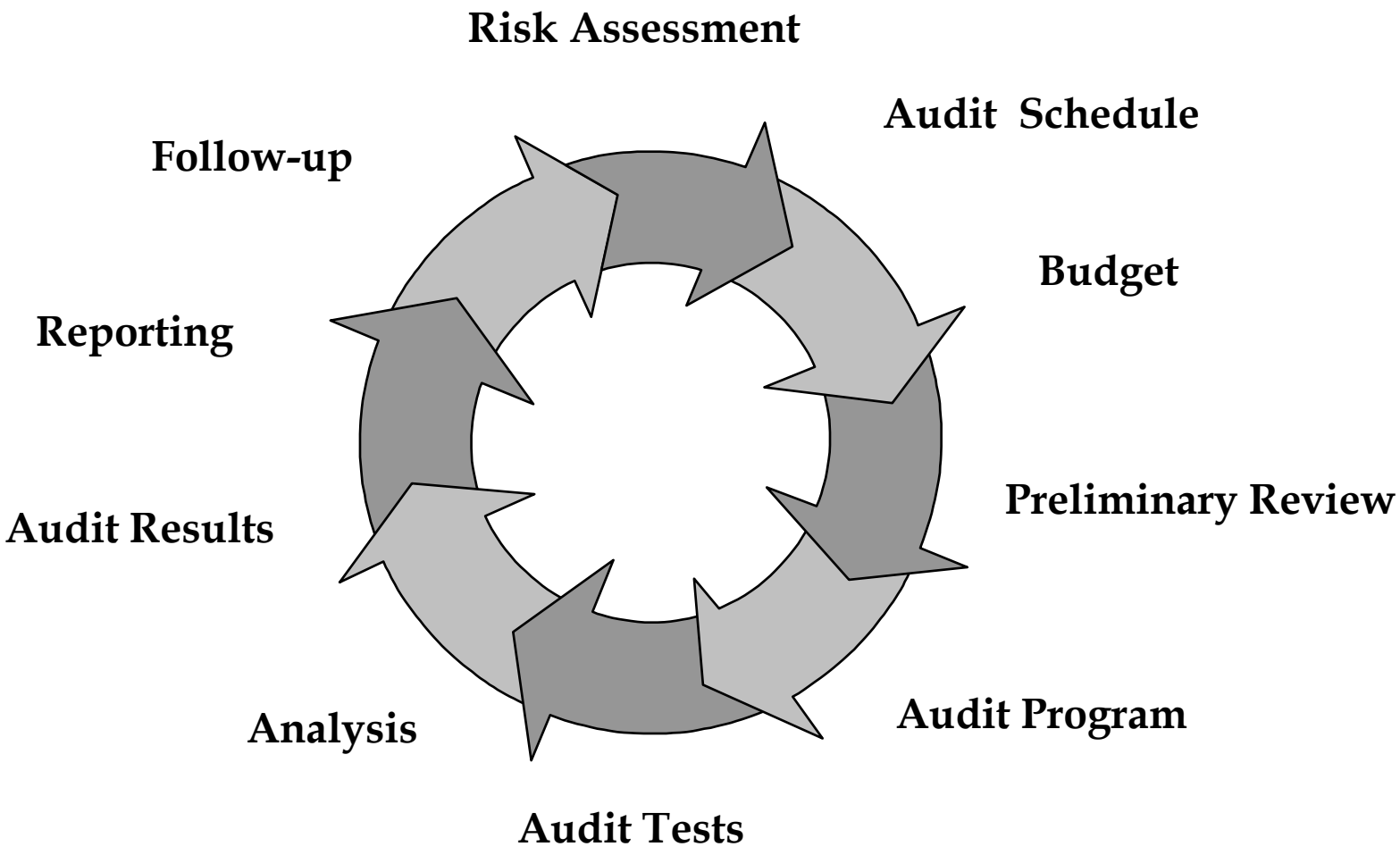
COBIT

- Authoritative, international set of generally accepted IT practices or control objectives that help employees, managers, executives and audit:
  - Understanding IT systems
  - Discharging fiduciary responsibilities
  - Deciding adequate levels of security and controls
- Allows management to benchmark its environment and compare with other organizations

COBIT Principles



The Audit Process



Risk Assessment

- Assist organizations in developing audit plans
  - Improve quality, quantity, and accessibility of planning data i.e. risk areas, past results, budget info
  - Examine audit projects and choose based on risk
  - Provide framework for allocating audit resources to achieve max benefits

Risk Assessment Process

- Identify changes in organization risk areas
- Identify new risk areas as they arise
- Access current regulatory and legal impacts
- Leverage information gathered during the audit process (prior audit findings)
- Prioritize risk areas based on objective and subjective evaluation

NIST Recommended Steps for Risk Assessment

1. Identify or characterize assets e.g financial applications
2. Define vulnerabilities and threat sources
3. Determine likelihood or probaility levels e.g. very high, high, medium etc.
4. Assign magnitude of impact
5. Associate assets with corresponsinf IT/business risks
6. Compute risk rating i.e probability x impact
7. Recommend controls

Audit Planning

Audit Plan

- Define scope
- State objectives
- Structure an orderly approach
- Provide for measurement of achievement
- Assure reasonable comprehensiveness
- Provide flexibility in approach

Objective and Context

- The objective is what we are trying to accomplish
  - E.g. gain assurance of an A/R balance
- The context is the environment in which we perform our work
  - E.g. centralized common system

Develop Audit Schedule

- Consider budget and resource constraints
- Plan audits and resources
- Prepare for audit
  - Audit selection
  - Definition of scope
  - Determine contacts and communication
  - Select audit team
- Define preliminary audit scope

Audit Budget and Scoping

- Organizations need to determine the number of available hours to decide the number of audits per year
  - Available hours per area, staff personnel
- Scope defines the area to be reviewed
  - Relevant financial applications, databases, OS, networks etc
- Scope should define critical business processes supported by selected applications
- Handouts: Budget and scoping examples

Audit Tasks

- Preliminary review
- Preliminary evaluation of internal controls
- Design audit procedures
- Test controls
- Final evaluation of internal controls
- Substantive testing
- Documenting results

Audit Process

Preliminary Review

- Gathering data
  - Nature of business
  - Financial history
  - Systems involved
  - Current procedures
- Methods
  - Interviews
  - Existing documentation
    - Policies, procedures, past audit reports

Design Audit Procedures

- Formal plan for reviewing and testing each significant audit subject area disclosed during fact gathering
  - Prepare an audit program specifically for area being audited
  - Select verification techniques applicable to each area
  - Prepare instructions for performance of tests

Types of Audits

- Audit procedures are very specific to the type of audit:
  - Reviewing information system management, policies, procedures, and standards
  - Supporting financial audits and auditing financial applications
  - Auditing system development and production applications
  - Auditing information processing facilities
  - Technical reviews of networking environment

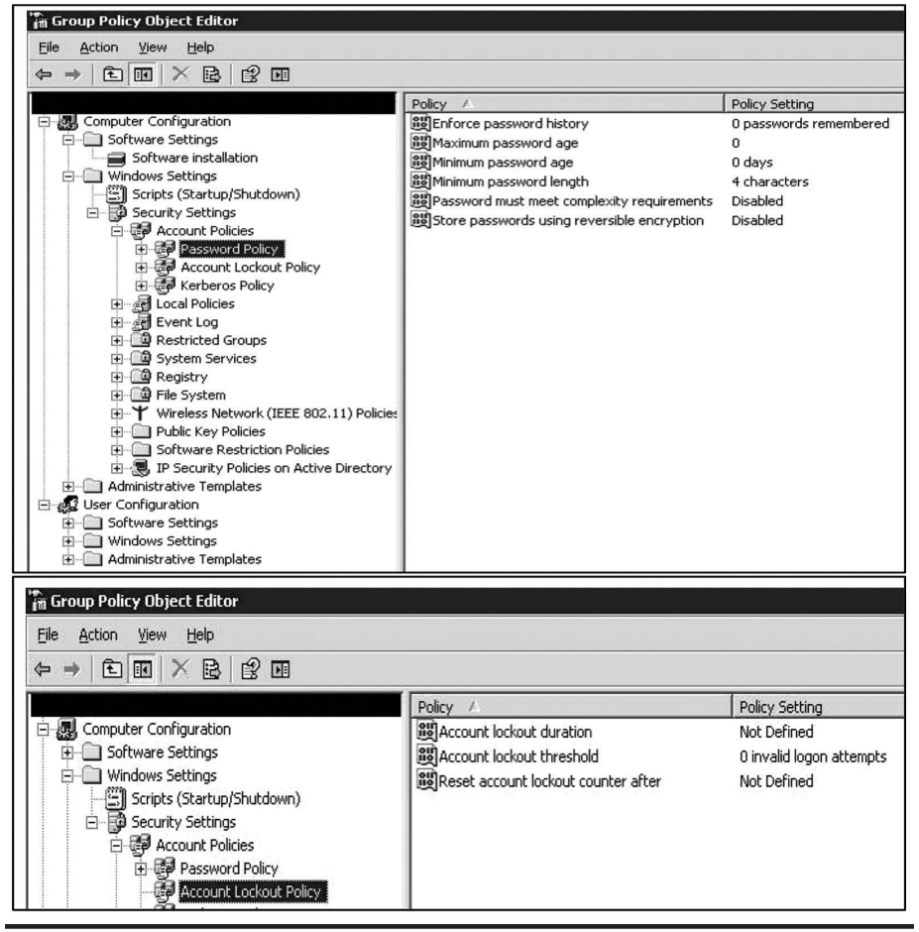
Fieldwork

- Define objectives
- Build basic understanding
- Evaluate controls, strengths, and weaknesses
- Design the audit procedures
- Test critical controls, processes, and apparent exposures
- Evaluate the results

Evaluation of Internal Controls

- Validate work performed
- Perform substantive testing where controls are not effective
- Document results
  - Audit findings
  - Analysis
  - Re-examination
  - Verification
  - Conclusion

Example of evidence supporting logical security



#	*Network / System / Financial Application*	*Logical Setting*				
		Enforce Password History	*Minimum Password Age*	*Minimum Password Length*	*Password Complexity*	*Account Lockout*
Per Company Policy [*working paper (w/p) ##*] {1}		5 passwords remembered	90 days	6 characters	Enabled	3 invalid login attempts
Actual Testing Performed						
	Local Area Network (LAN) / Windows	0 passwords remembered {a}	0 days {a}	4 characters {a}	Disabled {a}	0 invalid login attempts {a}
1	Financial Application X	{b}	{b}	{b}	{b}	{b}
2	Financial Application Y	Option not available—Application limitation {d}	90 days {c}	6 characters {c}	Enabled {c}	3 invalid login attempts {c}

Note: The password values above were obtained through observation, and with the assistance of [*name of Information Security Administrator*].

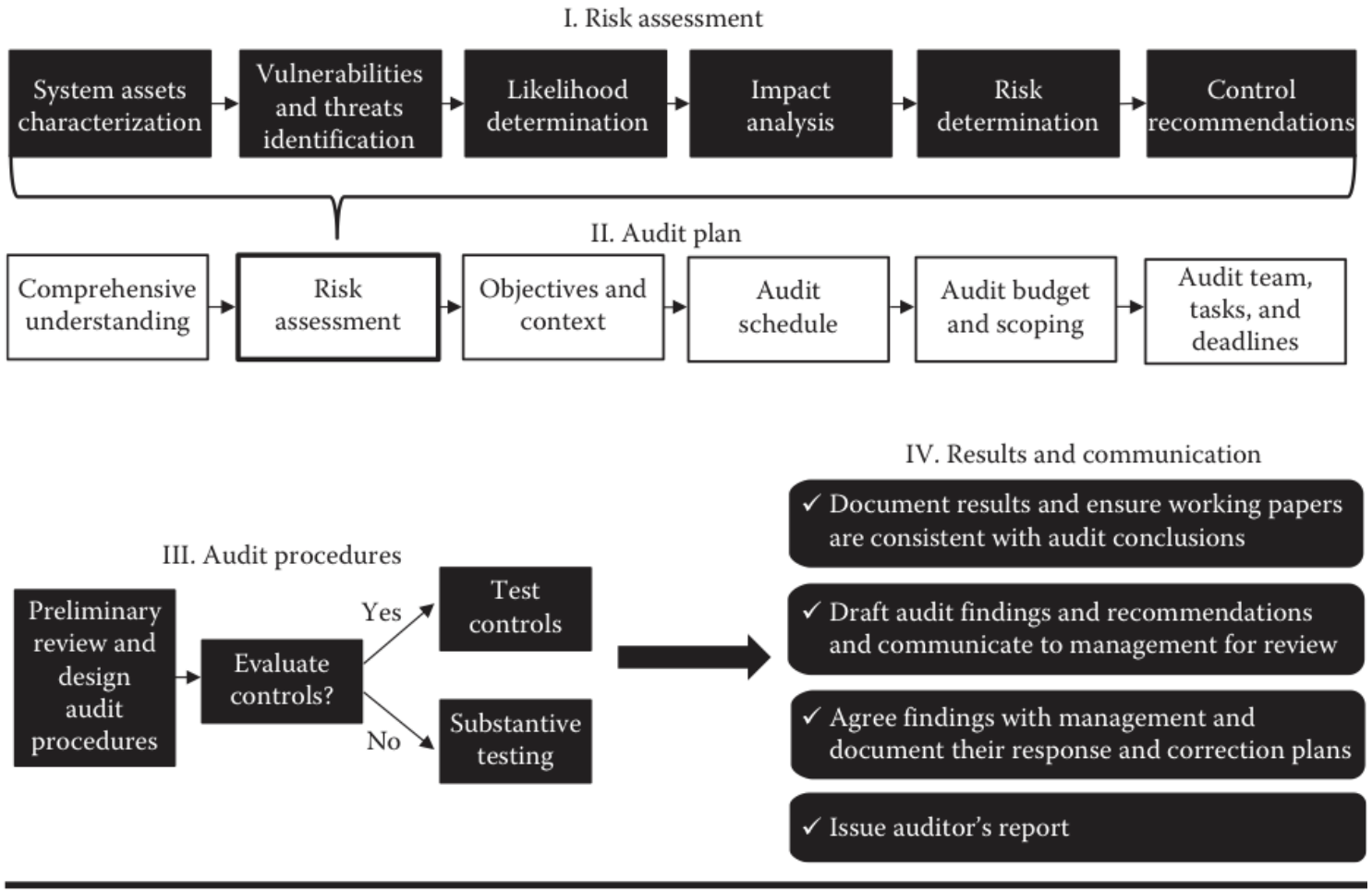
Documentation

- Findings
  - Name of IT environment, IT area affected (e.g. ops, InfoSec, change control, Working paper test reference, general control that failed, brief description, classification per standard, evaluation of finding (design vs ops) etc
- Recommendations
  - Formal statement that describe course of action
- Working Papers
- Audit Report
- Audit Follow-up

Communication Strategy

- Identify reportable issues
- Measuring the severity of issues
- Frequency of reporting
- Points during the audit process when issues are communicated
- Levels of management to communicate issues

Summary of Audit Process



Further Reading

- Chapter 4 of course book
- Handouts