9. IT Infrastructure Auditing Concepts

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

- This section presents how to audit an IT infrastructure for compliance based on the compliance laws themselves, on the need to protect and secure business and consumer privacy data, and on the need to have properly documented and implemented security controls within the organization. Auditing standards and frameworks are also presented, along with what must be audited within the seven domains of a typical IT infrastructure.

Overview

At the end of this lesson, you will be able to;

- Describe the needs for system security compliance.
- Describe different auditing frameworks and standards.
- Explaining the planning, conducting and reporting IT security audit.

Overview

9.1 The Need for Information Systems Security Compliance

- 9.1.1. What Is an IT Security Assessment?
- 9.1.2. What Is an IT Security Audit?
- 9.1.3. What Is Compliance?
- 9.1.4. How Does an Audit Differ from an Assessment?
- 9.1.5. What If an Organization Does Not Comply with Compliance Laws?

9.2 Auditing Standards and Frameworks

- 9.2.1. Why Frameworks Are Important for Auditing?
- 9.2.2. The Importance of Using Standards in Compliance Auditing

Overview

9.3 Planning an IT Infrastructure Audit

9.3.1 Defining the Scope, Objectives, Goals, and Frequency of an Audit

9.3.2 Identifying Critical Requirements for the Audit

9.3.3 Assessing IT Security

9.3.4 Obtaining Information, Documentation, and Resources

9.3.5 Mapping the IT Security Policy Framework Definitions to the Seven Domains of a Typical IT Infrastructure

9.3.6 Identifying and Testing Monitoring Requirements

9.3.7 Identifying Critical Security Control Points That Must Be Verified Throughout the IT Infrastructure

9.3.8 Building a Project Plan

Overview

9.4 Conducting and IT Infrastructure Audit

9.4.1 Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions

9.4.2 Identifying All Documented IT Security Policies, Standards, Procedures, and Guidelines

9.4.3 Conducting the Audit in a Layered Fashion

9.4.4 Performing a Security Assessment for the Entire IT Infrastructure and Individual Domains

9.4.5 Incorporating the Security Assessment into the Overall Audit Validating Compliance Process

9.4.6 Using Audit Tools to Organize Data Capture

9.4.7 Using Automated Audit Reporting Tools and Methodologies

9.4.8 Reviewing Configurations and Implementations

9.4.9 Verifying and Validating Proper Configuration and the Implementation of Security Controls and Countermeasures

9.4.10 Identifying Common Problems When Conducting an IT Infrastructure Audit

9.4.11 Validating Security Operations and Administration Roles, Responsibilities, and Accountabilities Throughout the IT Infrastructure

9.5. Writing IT infrastructure audit report

9.1. The Need for Information Systems Security Compliance

- Compliance goes beyond just conforming to internal policies and standards. Compliance extends outside of the organization, mapping to external regulations and industry standards.
- Regular assessments and audits of the IT environment are important for ensuring compliance.
- Failure to comply with external regulations and industry standards can carry severe penalties.

9.1. The Need for Information Systems Security Compliance

- 9.1.1. What Is an IT Security Assessment?
  - Assessing IT security is typically part of a larger security program within an organization. Specifically, an IT security assessment is a key activity that involves the management of risk
  - A risk-based approach to managing information security involves the following:
    - Identifying and categorizing the information and the information systems
    - Selecting and implementing appropriate security controls
    - Assessing the controls for effectiveness
    - Authorizing the systems by accepting the risk based upon the selected security controls
    - Monitoring the security controls on a continual basis
  - This approach is a continual cycle

9.1. The Need for Information Systems Security Compliance

- 9.1.1. What Is an IT Security Assessment?
  - Security controls include the physical, procedural, and technical mechanisms to safeguard systems
  - To understand their effectiveness, organizations must assess security controls
  - A security assessment should produce information required to do the following
    - Identify weaknesses within the controls implemented on information systems
    - Confirm that previously identified weaknesses have been remediated or mitigated
    - Prioritize further decisions to mitigate risks.
    - Provide assurance, a level of confidence that effective controls are in place and that associated risks are accepted and authorized.
    - Provide support and planning for future budgetary requirements.

9.1. The Need for Information Systems Security Compliance

- 9.1.1. What Is an IT Security Assessment?
  - The personnel who conduct security assessments can be internal or external to an organization
  - National Institute of Standards and Technology (NIST) provides a framework for effective security assessment plans in NIST Special Publication 800-53A
    - assessment objectives - Each objective has a set of assessment methods, including examination, interview, and test; and each objective has a set of assessment objects, including specification, mechanism, activity, and individual.
    - <Take Unsuccessful Logon Attempts as an example to explain the assessment plan>

9.1. The Need for Information Systems Security Compliance

- 9.1.2. What Is an IT Security Audit?
  - An IT security audit is an independent assessment of an organization's internal policies, controls, and activities
  - What is the importance of IT Security Audit?
  - The scope of an IT audit often varies, but can involve any combination of the following:
    - **Organizational**—This examines the management control over IT and related programs, policies, and processes.
    - **Compliance**—This pertains to ensuring that specific guidelines, laws, or requirements have been met.
    - **Application**—This involves the applications that are strategic—for example, those typically used by finance and operations.
    - **Technical**—This examines the IT infrastructure and data communications.

9.1. The Need for Information Systems Security Compliance

- 9.1.2. What Is an IT Security Audit?
  - An effective IT security audit program should ultimately accomplish three goals:
    - Provide an objective and independent review of an organization's policies, information systems, and controls.
    - Provide reasonable assurance that appropriate and effective IT controls are in place.
    - Provide audit recommendations for both corrective actions and improvement to controls.

9.1. The Need for Information Systems Security Compliance

- 9.1.2. What Is an IT Security Audit?
  - External or internal auditors typically perform IT security audits
  - **External auditors**
    - An external auditor is independent of the organization and is often engaged from one of the big accounting and consulting firms
    - External auditors are typically limited to providing information about gaps discovered and leading the client to accepted principles
  - **Internal auditors**
    - Internal auditors are employed by the organization that they audit.
    - Unlike external auditors, internal auditors are not independent of the organization they audit. They directly report to the board of directors or a subcommittee of the board of directors
    - This is important so as not to be influenced by management and to ensure the integrity and honesty of their findings.
    - Internal auditors can provide recommendations for improvements; however, they should never be involved in the design or implementation of any system or control.

9.1. The Need for Information Systems Security Compliance

- 9.1.3. What Is Compliance?
  - **Internal compliance** refers to an organization's ability to follow its own rules, which are typically based on defined policies
  - **External compliance** refers to the need or desire for an organization to follow rules and guidelines set forth by external organizations and initiatives
  - The general steps to meeting compliance include the following:
    - Interpret the regulation and how it applies to the organization.
    - Identify the gap or determine where the organization stands with the compliance mandate.
    - Devise a plan to close the gap.
    - Execute the plan.
- Compliance is closely related to risk management and governance on all levels, be it technical, procedural, or strategic.

9.1. The Need for Information Systems Security Compliance

- 9.1.4. How Does an Audit Differ from an Assessment?
  - Security auditing, in general, must follow a more rigid approach and process over a security assessment.
  - An audit contains the following unique characteristics:
    - Auditors should never be involved in the auditing of processes, systems, or applications that they themselves designed or implemented.
    - Audits are an independent evaluation. A security assessment may also be conducted independently, but it is not necessary. Many organizations use a combination of both.
    - Audits follow a rigorous approach and are conducted according to accepted principles. This also requires that auditors be qualified. The approach taken for an assessment can fall across a wide spectrum, but in many cases, they have taken a cue from audits with well-defined approaches and frameworks.
    - In the event an organization passes an audit, the organization typically receives some type of certification or confirmation. This is not the case for assessments.
    - An audit is concerned about past results and performance, whereas an assessment considers previous and current results as well as expected performance.

9.1. The Need for Information Systems Security Compliance

- 9.1.5. What If an Organization Does Not Comply with Compliance Laws?
  - Consequences of noncompliance could be:
    - financial
    - reputational
    - operational
  - Consider the following categories from where costs can occur following a security breach:
    - Discovery, notification, and response
    - Lost productivity
    - Opportunity cost
    - Regulatory fines
    - Restitution
    - Additional security and audit requirements
    - Other liabilities

9.2. Auditing Standards and Frameworks

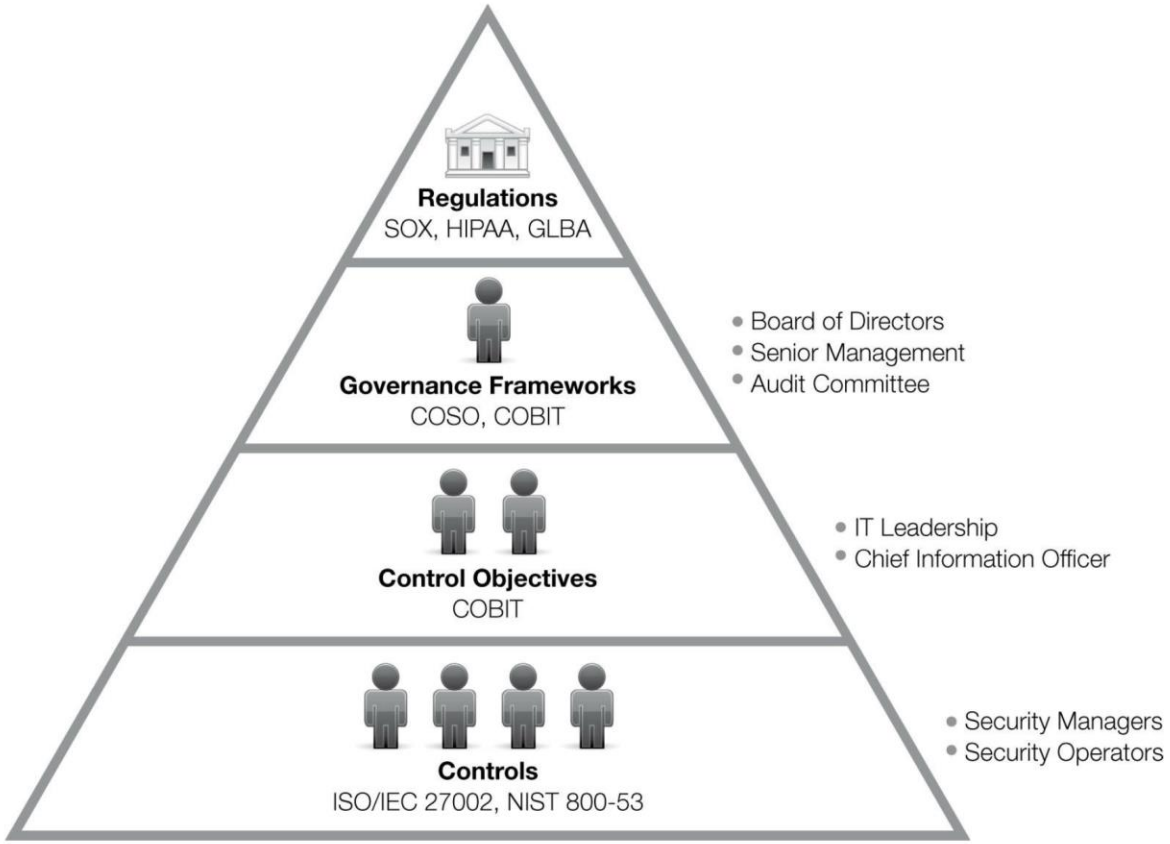
- 9.2.1. Why Frameworks Are Important for Auditing?
  - A framework is a conceptual set of rules and ideas that provide structure to a complex and tough situation.
  - A framework, provides a consistent system of controls to which IT departments can adhere.
  - This system of controls also provides an auditor a consistent approach for conducting audits.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - Different standards and frameworks would have different attributes:
    - Depth and breadth
    - Flexibility
    - Reasoning
    - Prioritization
    - Industry acceptance
  - Auditing against standards works best when the auditor and the organization agree on a specific standard.
  - The following are some key recommendations when selecting a standard:
    - Select a standard that can be followed
    - Employ the standard
    - Select a flexible standard

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - The hierarchy of standers and compliance



9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - Following are the high-level steps an organization may take to apply the use of standards:
    - Educate personnel, beginning with senior management.
    - Choose the standards that the organization will follow.
    - Put the people in place and provide the needed resources to apply and meet the standard.
    - Confirm the standards are being met by using an internal audit and outside resources as needed.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *COSO (Committee of Sponsoring Organizations)*
  - COSO provides the structure to examine risk within the organization and apply risk-based processes.
  - The COSO enterprise risk management (ERM) framework consists of eight components across four objectives.
  - The framework is geared to achieving an organization's objectives as defined by the following:
    - Strategic
    - Operations
    - Reporting
    - Compliance

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - The COSO framework identifies eight interrelated parts in connection with the management processes of an organization.
    - Internal environment
    - Objective setting
    - Event identification
    - Risk assessment
    - Risk response
    - Control activities
    - Information and communication
    - Monitoring

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *COBIT (Control Objectives for Information and Related Technology)*
  - COBIT helps to align IT with the business or enterprise requirements by doing the following:
    - Mapping controls to key business requirements
    - Classifying IT activities into a process model
    - Identifying the key IT resources to be controlled
    - Defining the framework for control objectives

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles
    - Meeting stakeholder needs
    - Covering the enterprise End to End
    - Applying a single integrated framework
    - Enabling a holistic approach
    - Separating governance from management

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Meeting stakeholder needs
  - These needs are broadly defined in the following three categories:
    - Benefits realization
    - Risk optimization
    - Resource optimization

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Meeting stakeholder needs
    - Meeting stakeholder needs
    - Covering the enterprise End to End
    - Applying a single integrated framework
    - Enabling a holistic approach
    - Separating governance from management

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Covering the enterprise End to End
  - Enable interaction with the system through three elements
    - Governance enablers
    - Governance scope
    - Roles, activities, and relationships

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Applying a Single Integrated Framework
  - COBIT 5 is a collective framework and content filters can be applied to provide for varying degrees of guidance

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Enabling a Holistic Approach
  - COBIT 5 provides a holistic approach through enablers
  - COBIT 5 defines the following seven categories of enablers:
    - Principles, policies, and frameworks
    - Processes
    - Organizational structures
    - Culture, ethics, and behavior
    - Information
    - Services, infrastructure, and applications
    - People, skills, and competencies

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Enabling a Holistic Approach
  - To provide for a structured way to deal with enablers and to manage the interactions and ultimately facilitate a successful outcome, COBIT 5 defines four dimensions.
  - That is, each enabler has the following:
    - Stakeholders
    - Goals
    - Lifecycle
    - Good practices

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - COBIT 5 Principles - Separating Governance from Management
  - COBIT 5 makes a strong statement on the differences between governance and management.
  - According to COBIT 5, governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
  - management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *Service Organization Control (SOC) Reports*
  - Service organizations find it important to instill trust and confidence in their customers.
  - Service Organization Control (SOC) reports provide such assurance.
  - The primary stakeholders for SOC reports include the following:
    - User entities
    - Service organizations
    - Auditors

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *Service Organization Control (SOC) Reports*
  - SOC reports take the form of three different engagements, which product three different reports. The following are the three types of engagements and associated SOC reports:
    - SOC 1, Report on Controls at a Service Organization Relevant to User Entities' Internal Controls over Financial Reporting
    - SOC 2, Report on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
    - SOC 3, Trust Services Report for Service Organizations

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *ISO/IEC Standards*
  - The International Organization for Standardization (ISO) is a nongovernment group that brings both the private and public sectors together and creates solutions for business and society
  - ISO/IEC 27000 is a series of standards and related terms that provide guidance on matters of information security.
  - This includes implementing, designing, and auditing an information security management system (ISMS). An ISMS describes the policies, standards, and programs related to information security.
  - Other popular series include ISO 9000 and ISO 14000, which deal with quality management and environmental management, respectively.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *ISO/IEC 27001 Standard*
  - ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *ISO/IEC 27002 Standard*
  - ISO/IEC 27002:2013 Information Technology— Security Techniques—Code of Practice for Information Security Management.

9.2. Auditing Standards and Frameworks

- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *NIST 800-53*
  - NIST 800-53 provides a comprehensive catalog of security controls.
  - The catalog of controls is grouped into 17 families of controls, which include the following:
    - Access Control
    - Awareness and Training
    - Audit and Accountability
    - Configuration Management
    - Contingency Planning
    - Identification and Authentication
    - IncidentResponse
    - Maintenance
    - Media Protection
    - Physical and Environmental Protection • Planning
    - PersonnelSecurity
    - Risk Assessment
    - Security Assessment and Authorization • System and Services Acquisition
    - System and Communication Protection
    - System and Information Integrity

9.2. Auditing Standards and Frameworks

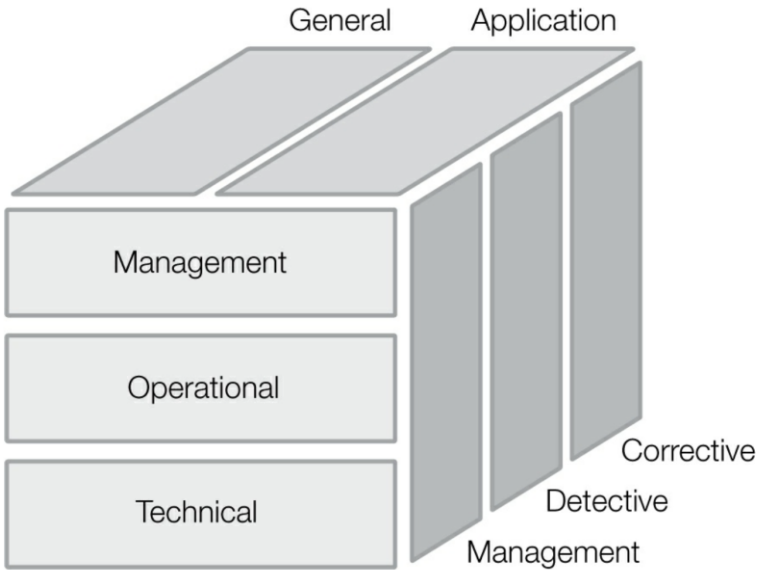
- 9.2.2. The Importance of Using Standards in Compliance Auditing
  - *Cybersecurity Framework*
  - The Cybersecurity Framework is made up of three components:
    - The Framework Core
    - The Framework Profile
    - The Framework Implementation Tiers
  - The framework includes various categories across five different functions.
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover

9.3. Planning an IT Infrastructure Audit

- 9.3.1 Defining the Scope, Objectives, Goals, and Frequency of an Audit
  - When defining the scope, the auditor should consider the controls and processes across the seven domains of IT infrastructure.
  - This includes relevant resources such as the following:
    - Data
    - Applications
    - Technology
    - Facilities
    - Personnel

9.3. Planning an IT Infrastructure Audit

- 9.3.2 Identifying Critical Requirements for the Audit
  - Implementing Security Controls
    - Management controls
    - Operational controls
    - Technical controls
  - Protecting Privacy Data



9.3. Planning an IT Infrastructure Audit

- 9.3.3 Assessing IT Security
  - Risk Management
  - Threat Analysis
  - Vulnerability Analysis
  - Risk Assessment Analysis: Defining an Acceptable Security Baseline Definition

9.3. Planning an IT Infrastructure Audit

- 9.3.4 Obtaining Information, Documentation, and Resources
  - Existing IT Security Policy Framework Definition
  - Configuration Documentation for IT Infrastructure
  - Interviews with Key IT Support and Management Personnel: Identifying and Planning

9.3. Planning an IT Infrastructure Audit

- 9.3.5 Mapping the IT Security Policy Framework Definitions to the Seven Domains of a Typical IT Infrastructure
  - The seven domains of a typical IT infrastructure are as follows:
    - User Domain
    - Workstation Domain
    - LAN Domain
    - LAN-to-WAN Domain
    - WAN Domain
    - Remote Access Domain
    - System/Application Domain

9.3. Planning an IT Infrastructure Audit

- 9.3.6 Identifying and Testing Monitoring Requirements
  - COBIT states that continuous monitoring and evaluation of a the control environment helps provide answers to the following questions:
    - Is IT performance measured to detect problems before it is too late?
    - Does management ensure that internal controls are effective and efficient?
    - Can IT performance be linked back to business goals?
    - Are adequate confidentiality, integrity, and availability controls in place for information security?

9.3. Planning an IT Infrastructure Audit

- 9.3.7 Identifying Critical Security Control Points That Must Be Verified Throughout the IT Infrastructure
  - Consensus Audit Guidelines (CAG) published by SANS in 2009.

<knowing the existence of such guideline is sufficient for the module>

9.3. Planning an IT Infrastructure Audit

- 9.3.8 Building a Project Plan
  - Having the appropriate people assigned to perform an audit
  - Tools to support the IT auditing process
  - The IIA lists several types of tools that can facilitate an audit. These include the following:
    - Electronic work papers
    - Project management software
    - Flowcharting software
    - Open issue tracking software
    - Audit department Web site

9.4. Conducting and IT Infrastructure Audit

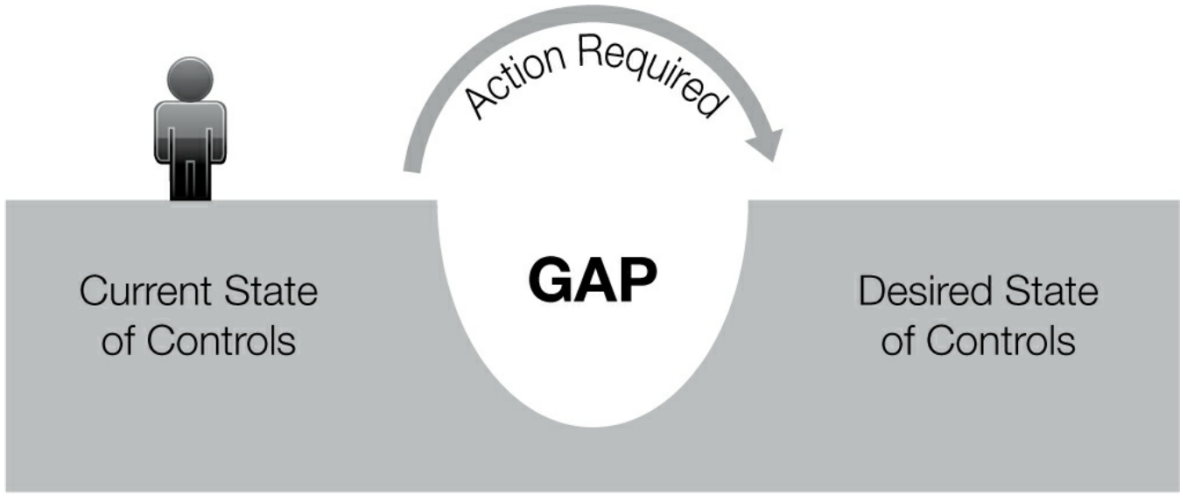
- 9.4.1 Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions
  - The following questions are helpful in determining an appropriate set of baseline controls:
    - Does the organization have a program for IT governance and security management?
    - Do IT policies exist?
    - Are there tools and processes for assessing risk in place?
    - Is the IT environment physically secured?
    - Are authentication and access control mechanisms in place?
    - Is software to prevent, detect, and respond to malicious code in place?
    - Are firewalls used?
    - Has a program for configuration and change management been put in place?
    - Are systems automatically monitored and reviewed by IT staff?
    - Do personnel have the appropriate skills to perform their job, and is an ongoing training and awareness program in place?

9.4. Conducting and IT Infrastructure Audit

- 9.4.1 Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions
  - Organization-Wide
    - Establishing a baseline based on a control framework needs to be relative to the risk appetite of the organization
  - Seven Domains of a Typical IT Infrastructure
    - The seven domains of a typical IT infrastructure are composed of people, processes, and technology.
    - Gathering the appropriate documents can provide an immediate view into the domains and inventory of the IT infrastructure.
    - Reducing the risk depends on what controls are available, how much they cost, and if they are cost efficient.
    - Risk mitigation strategies include:
      - Accept the risk
      - Avoid the risk
      - Share the risk
      - Control the risk

9.4. Conducting and IT Infrastructure Audit

- 9.4.1 Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions
  - Gap Analysis for the Seven Domains



9.4. Conducting and IT Infrastructure Audit

- 9.4.2 Identifying All Documented IT Security Policies, Standards, Procedures, and Guidelines
  - The organizational security policy framework is the foundation for the management of information security.
  - ISO/IEC 27002 has a control objective dedicated to security policies, it references individual policies, standards, and procedures throughout all the other controls as well.

9.4. Conducting and IT Infrastructure Audit

- 9.4.3 Conducting the Audit in a Layered Fashion
  - The auditor should conduct the audit according to the scope of the plan.
  - A layered audit approach across the domains of the IT infrastructure will be necessary when systems span the domains.
  - A company's financial system can span multiple domains and even include third-party providers such as payroll service providers.

9.4. Conducting and IT Infrastructure Audit

- 9.4.4 Performing a Security Assessment for the Entire IT Infrastructure and Individual Domains
  - There are different approaches to identify security weaknesses within an organization. Some of the approaches include the following:
    - Network scan
    - Vulnerability scan
    - Penetration test

9.4. Conducting and IT Infrastructure Audit

- 9.4.5 Incorporating the Security Assessment into the Overall Audit Validating Compliance Process
  - ISACA produces a series of auditing standards, guidelines, and procedures for information systems auditors.
  - ISACA's suggested penetration test and vulnerability analysis procedures include the following:
    - Planning
    - Skills required
    - Agreements
    - Scope questions
    - Internet penetration testing
    - Dial-in penetration testing
    - Internal penetration testing
    - Physical access controls
    - Social engineering testing
    - Wireless
    - Web application
    - Report

9.4. Conducting and IT Infrastructure Audit

- 9.4.6 Using Audit Tools to Organize Data Capture
  - Auditors can increase their productivity through the use of computer assisted audit tools and techniques (CAATT)
  - CAATTs are used for many different functions, including the following:
    - Testing transactions in applications
    - Reviewing procedures
    - Testing system and application controls for compliance
    - Conducting automated vulnerability assessments
    - Performing penetration testing

9.4. Conducting and IT Infrastructure Audit

- 9.4.7 Using Automated Audit Reporting Tools and Methodologies
  - Many organizations use automated audit reporting tools.
  - These solutions aggregate all of this data centrally and provide mechanisms to correlate, alert, and report upon this data
  - From an organizational perspective, automated audit reporting tools or information and event management help simplify compliance, improve security, and optimize IT operations.

9.4. Conducting and IT Infrastructure Audit

- 9.4.8 Reviewing Configurations and Implementations
  - Configuration management has a direct impact on information security and compliance.
  - Configuration management as a program is made up of several pieces, such as the following:
    - Configuration change control board
    - Baseline configuration management
    - Configuration change control
    - Configuration monitoring and auditing
  - Monitoring configuration helps identify the following:
    - Unauthorized changes
    - Misconfigurations
    - Vulnerabilities
    - Unauthorized systems and software

9.4. Conducting and IT Infrastructure Audit

- 9.4.9 Verifying and Validating Proper Configuration and the Implementation of Security Controls and Countermeasures
  - Auditing security controls across the IT infrastructure involves testing the controls or countermeasures using available documents, interviews, and personal observation.
  - Each control to be tested should have an accompanying assessment objective
  - One or more assessment objectives are validated using a specific method.
  - Such methods include examination, interviews, and testing.
  - Using these methods against particular assessment objects will produce the results, which is a determination of the effectiveness of the controls.
  - Three broad categories of objects include the following:
    - Specification objects
    - Mechanism objects
    - Activity objects

9.4. Conducting and IT Infrastructure Audit

- 9.4.9 Verifying and Validating Proper Configuration and the Implementation of Security Controls and Countermeasures
  - The effort required to assess controls will vary not just across the objectives.
    - Depth
    - Coverage

9.4. Conducting and IT Infrastructure Audit

- 9.4.10 Identifying Common Problems When Conducting an IT Infrastructure Audit
  - NIST defines several areas of potential challenges when conducting security testing and assessments.
    - Time and resources
    - Resistance
    - Temporary behavior
    - Immediate response
    - Changing technology
    - Operational impact

9.4. Conducting and IT Infrastructure Audit

- 9.4.11 Validating Security Operations and Administration Roles, Responsibilities, and Accountabilities Throughout the IT Infrastructure
  - Security operations and administration are responsible for implementing the policy framework to protect the confidentiality, integrity, and availability of the company's information and supporting technologies.
  - Security operations and administration personnel are directly involved in the implementation and administration of controls designed to allow access only to those authorized.
  - They also maintain the systems that prevent fraud, violations, and other malicious and even unintentional breaches of confidentiality, integrity, and availability.
  - Those assigned to protect assets are not above committing irregular or illegal acts. In fact, without proper controls in place, such activities are easier to perform.

9.4. Conducting and IT Infrastructure Audit

- 9.4.11 Validating Security Operations and Administration Roles, Responsibilities, and Accountabilities Throughout the IT Infrastructure
  - Examples of safeguards that need to be verified include the to prevent such attacks are:
    - Security operation policies
    - Assignment of responsibilities
    - Maintenance procedures
    - Segregation of duties
    - Rotation of duties
    - Least privilege
    - Mandatory vacation
    - Screening
    - Training and awareness

9.5. Writing IT infrastructure audit report

- Executive Summary of an Audit Report
- Summary of Findings
- IT Security Assessment Results: Risk, Threats, and Vulnerabilities
- Reporting on Implementation of IT Security Controls and Countermeasures
- IT Security Controls and Countermeasure Gap Analysis
- Compliance Assessment Throughout the IT Infrastructure
- Presenting Compliance Recommendations