Cyber Audit

By –Prakash Khasor,
Assistant Professor(Cyber Security),
National Forensic Sciences University

Basic Terms for Audit

- Policies: Policies are a set of principles, guidelines, or rules established by organizations or institutions to guide decision-making and behavior within their jurisdiction. Policies can cover a wide range of topics, from human resources and security to environmental sustainability and financial management.
- Scenario: A company aims to protect its sensitive digital data.

Example Policy: "Data Security Policy" - This policy outlines how employees should handle, store, and transmit sensitive data. It includes requirements for strong passwords, encryption, and guidelines for reporting security incidents.

Basic Terms for Audit

- Rules: Rules are specific directives or instructions that prescribe certain actions or behaviors and may be part of policies or regulations. They are typically more detailed and specific than policies and are often used to enforce compliance with broader policies and laws.
- Scenario: An online gaming community wants to maintain fair play.

Example Rule: "No cheating or exploiting game glitches" - This rule is part of the community's code of conduct. It prohibits players from gaining unfair advantages by cheating or exploiting software vulnerabilities.

Basic Terms for Audit

- Framework: A framework is a structured approach or system that provides a foundation for developing policies, rules, or guidelines. Frameworks help organizations or governments create consistent and cohesive regulations in various areas. For example, a cybersecurity framework might outline best practices for protecting digital assets.
- Scenario: A national cybersecurity agency is working to enhance the country's cybersecurity posture.

Example Framework: "National Cybersecurity Framework" - This framework establishes a comprehensive approach to cybersecurity, including risk assessment, incident response protocols, and collaboration between government agencies and the private sector.

Basic Terms for Audit

- Laws: Laws are formal, binding rules and regulations established by governments or legislative bodies. They are enforced by legal authorities and carry penalties for non-compliance. Laws can cover a wide range of issues, such as criminal behavior, property rights, taxation, and more.
- Scenario: A nation wants to combat cybercrime.

Example Law: "Cybercrime Prevention Act" - This law defines various cybercrimes, such as hacking, identity theft, and online fraud, and prescribes penalties for offenders. It empowers law enforcement agencies to investigate and prosecute cybercriminals.

Basic Terms for Audit

- Guidelines: Guidelines are non-binding recommendations or suggestions that provide advice or best practices for specific activities or industries. While they are not legally enforceable on their own, guidelines are often used as references to inform decision-making or to establish standards within a particular field.
- Scenario: A social media platform aims to combat the spread of misinformation.

Example Guideline: "Content Moderation Guidelines" - These guidelines provide instructions to content moderators on how to identify and remove fake news, hate speech, and other harmful content. They help maintain a safe and informative online environment

Scope of IT Compliance Audit

- The scope of an IT compliance audit refers to the specific boundaries and objectives of the audit process.

- It defines what areas, systems, processes, and controls will be assessed to ensure compliance with relevant regulations, standards, policies, and best practices in the field of information technology (IT).

Scope of IT Compliance Audit

- The scope of an IT compliance audit refers to the specific boundaries and objectives of the audit process.

- It defines what areas, systems, processes, and controls will be assessed to ensure compliance with relevant regulations, standards, policies, and best practices in the field of information technology (IT).

Regulatory Compliance

- Ensuring that the organization adheres to relevant laws and regulations that govern IT operations, such as data protection laws (e.g., GDPR, HIPAA), financial regulations (e.g., Sarbanes-Oxley Act), or industry-specific standards (e.g., PCI DSS for payment card data security).

Policy Compliance

- Assessing whether the organization's IT policies and procedures align with internal guidelines and industry best practices. This may include policies related to data security, access controls, incident response, and more.
- Information Security Policy Compliance:
- Password Policies:-
- Data Encryption: -
- Access Control:-

Data Security

- Evaluating the measures in place to protect sensitive data, including data encryption, access controls, data backup, and disaster recovery plans.
- Data Backup and Recovery:-
- Authentication and Authorization:-
- Data Encryption:-
- Security Patch Management:-
- Incident Response Management:

Access Controls

- Verifying that access to IT systems and data is restricted appropriately based on user roles and responsibilities. This includes user authentication, authorization, and audit trails.
- Role-Based Access Control (RBAC):
- Access Control Lists (ACLs):
- Mandatory Access Control (MAC):
- Discretionary Access Control (DAC):
- Biometric Access Control:
- Time-Based Access Control:
- Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA):

Change Management

- Examining the processes for making changes to IT systems, software, and configurations to ensure that changes are documented, tested, and approved to prevent unauthorized or risky alterations.
- Change Request Process:
- Change Review and Approval:
- Testing and Validation:
- Rollback Plans:
- Documentation and Tracking:
- Compliance with Policies and Standards:
- Communication and Training:

Incident Response

- Assessing the organization's readiness to respond to IT security incidents, including the detection, containment, and recovery processes.
- Incident Identification
- Incident Classification and Prioritization
- Containment and Eradication
- Communication and Reporting
- Evidence Preservation
- Recovery and Remediation
- Post-incident review and Lessons Learned
- Continuous Improvement

Network and Infrastructure Security

- Evaluating the security of the organization's network infrastructure, including firewalls, intrusion detection/prevention systems, and network segmentation.
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)
- Access Control and Authentication
- Network Segmentation
- Patch Management
- Network Monitoring and Logging
- Data Encryption
- Disaster Recovery and Redundancy
- Physical Security
- Incident Response Preparedness

Vendor and Third-Party Management

- Ensuring that third-party vendors and service providers are also in compliance with relevant IT standards and regulations when they handle the organization's data or IT processes.
- Vendor Assessment and Due Diligence
- Contractual Agreements and SLAs
- Security Controls and Compliance
- Access Control and Monitoring
- Incident Response and Reporting
- Business Continuity and Disaster Recovery
- Exit Strategy
- Ongoing Monitoring and Auditing

Audit Trails and Logging

- Reviewing the adequacy of audit trails and logs to track and monitor user activities, system changes, and security events.
- Logging Policies and Standards
- Log Generation and Collection
- Time Synchronization
- Log Retention and Storage
- Log Review and Analysis
- Access Controls to Logs
- Integration with SIEM Systems
- Log Encryption
- Alerting and Notification
- Incident R

Physical Security

- Assessing physical security measures in place, such as access controls to data centers and server rooms, surveillance, and environmental controls..
- Access Control Systems
- Perimeter Security
- Video Surveillance
- Intrusion Detection and Alarm Systems
- Visitor Management
- Biometric Access Control
- Locks and Keys
- Environmental Controls
- Data Center Security
- Security Personnel and Training

Disaster Recovery and Business Continuity:

- Verifying that the organization has plans and procedures in place to recover IT systems and maintain critical business functions in the event of a disaster.
- Risk Assessment
- Business Impact Analysis (BIA)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Testing and Exercises
- Data Backup and Recovery
- Alternate Sites and Facilities
- Communication and Notification
- Training and Awareness
- Compliance and Documentation

Thank you!