Cyber Security Audit & Compliance: Ensuring Robust Protection

Exploring the significance of audits and compliance in cyber security.

Sansrujan

Agenda

Cyber Security Audit & Compliance: Ensuring Robust Protection

01 **Introduction to Cyber Security Audits**

Overview of cyber security audits and their significance.

02 **Defining the Scope for Audit**

Identifying the boundaries and focus areas for the audit.

03 **Identifying Critical Requirements**

Determining essential security requirements for compliance.

04 **Assessing IT Security**

Evaluating current IT security measures and their effectiveness.

05 **Gathering Information & Resources**

Collecting necessary data and resources for the audit.

06 **Mapping the IT Security Framework**

Creating a comprehensive map of the existing security framework.

07 **Goal-Based Security Control**

Establishing security controls aligned with organizational goals.

08 **Implementation-Based Security Control**

Focusing on practical implementation of security measures.

09 **Security Control Formulation**

Developing robust security controls to mitigate risks.

Introduction to Cyber Security Audits

Cyber Security Audit & Compliance: Ensuring Robust Protection

Critical Evaluations

Cyber security audits evaluate IT infrastructure for security compliance.

Identifying Vulnerabilities

Audits help pinpoint weaknesses in systems that could be exploited.

Mitigating Risks

Through audits, organizations can implement measures to reduce potential risks.

Ensuring Compliance

Regular audits ensure adherence to security policies and industry standards.

Continuous Improvement

Audits facilitate ongoing enhancements in security protocols and practices.

Defining the Scope for Audit

Establishing Focus in Cyber Security Audits

Initial Step in Audit Process

Defining the scope is crucial as it sets the boundaries for the audit's focus.

Critical Areas Identification

It ensures that the audit targets essential components of the IT infrastructure.

Infrastructure Review

Decide which parts of the IT infrastructure will be included in the audit.

Example of Scope Definition

For office audits, choose between reviewing just computers or the entire network.

Comprehensive Coverage

Consider including servers, applications, and storage systems for thorough assessment.

Identifying Critical Requirements

Essential standards for compliance in cybersecurity

Must-Have Elements

Critical requirements are essential for organizational compliance, covering legal, regulatory, and security standards.

HIPAA Compliance

Healthcare organizations must comply with HIPAA regulations to safeguard sensitive patient information.

PCI DSS Compliance

For organizations handling payment data, adhering to PCI DSS standards is vital to ensure data protection.

Assessing IT Security

Evaluating Measures for Risk Management in Cyber Security

Evaluate Current Security Measures

Assess existing protocols to identify vulnerabilities that could expose sensitive data.

Identify Potential Risks

Recognize gaps in security that may allow unauthorized access to systems and information.

Utilize Effective Tools

Check the implementation of firewalls, antivirus software, and encryption technologies.

Enhance Data Protection

Develop strategies based on assessments to strengthen defenses against cyber threats.

Gathering Information & Resources

Essential steps for a comprehensive cyber security audit

Collect Security Policies

Gather all relevant security policies that govern the organization's data protection strategies.

Access Logs Review

Compile access logs to monitor user activity and identify potential security breaches.

Inventory Software Assets

Create an inventory of all software applications to ensure compliance and security standards.

Network Diagrams Compilation

Draw network diagrams to visualize the network architecture and identify

Collect System Logs

Accumulate system logs for a detailed examination of system performance and security-related events.

Firewalls Rules Documentation

Document firewall rules to assess the effectiveness of network defenses against unauthorized access.

User Access Lists

Gather user access lists to ensure that only authorized personnel have access to sensitive information.

Policy Documents Review

Review policy documents to ensure that they are up-to-date and aligned with current security practices.

Certifications and Standards:

01

ISO 27001 (Information Security Management System)

This is the most widely recognized international standard for managing information security. It provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

02

SOC 1 & 2 (Service Organization Controls)

These are reports and certifications provided after an audit of an organization's internal controls. SOC 1 focuses on financial reporting, while SOC 2 is related to IT security, privacy, and confidentiality.

03

PCI DSS (Payment Card Industry Data Security Standard)

This is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Certifications and Standards:

01 **COBIT (Control Objectives for Information and Related Technology)**

COBIT is a framework for the governance and management of IT. It helps organizations develop, implement, monitor, and improve IT governance and management practices.

02 **GDPR (General Data Protection Regulation)**

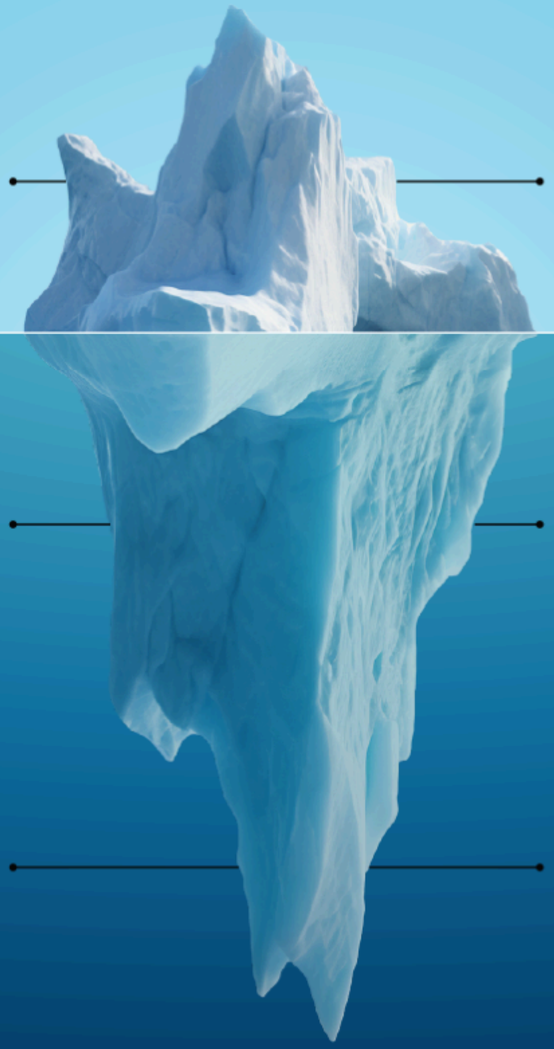
A European regulation on data protection and privacy for individuals within the EU, it requires companies to protect personal data and privacy for European citizens and residents.

03 **PCI DSS (Payment Card Industry Data Security Standard)**

Primarily used in the healthcare sector in the United States, this law mandates the protection of sensitive patient health information.

Mapping the IT Security Framework - The Seven Domains of IT Infrastructure

Cyber Security Audit & Compliance: Ensuring Robust Protection



User

Focus on user authentication and access controls to protect sensitive data.

Workstation

Implement data encryption and antivirus software on workstations.

LAN

Secure local area networks with firewalls and intrusion detection systems.

LAN-to-WAN

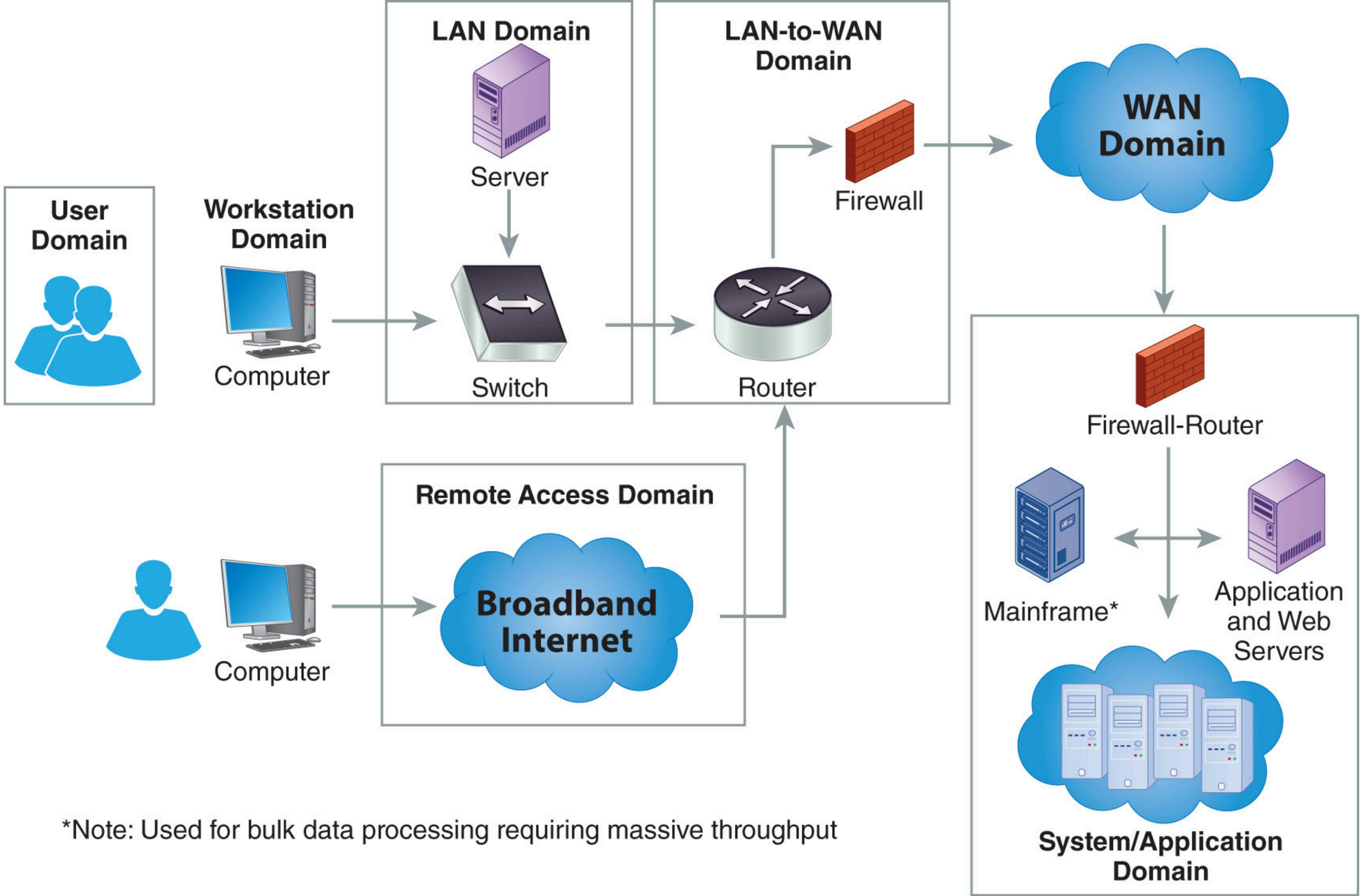
Ensure data encryption during transit between LAN and WAN for added security.

Remote Access

Utilize VPNs for secure remote access to the IT infrastructure.

WAN

Protect wide area networks with robust security policies and monitoring.



*Note: Used for bulk data processing requiring massive throughput

Companies that failed IT Audit

Facebook/Cambridge Analytica (2018)

Facebook's IT audit revealed improper data-sharing practices, specifically the sharing of personal user data with third parties like Cambridge Analytica without proper user consent. It failed to adhere to security, privacy, and compliance standards.

Sony Pictures (2014)

Sony failed an IT security audit when it was hacked by the group known as "Guardians of Peace," leading to leaked confidential information, employee data, and unreleased films. The audit revealed weaknesses in encryption, network segregation, and user access controls.

Uber (2016)

Uber failed in its IT audit when it was found that hackers accessed the personal data of 57 million customers and drivers. The company also attempted to cover up the breach by paying hackers to delete the data.

Satyam Computers (2009)

Satyam's financial statements were heavily falsified. They inflated cash reserves, profits, and revenues to deceive shareholders and stakeholders about the company's financial health.

Common Reasons for Failing IT Audits

Weak Security Controls

01

Failure to implement patches, weak passwords, lack of multi-factor authentication (MFA), and poor encryption.

Non-Compliance with Regulations

02

Not adhering to laws like GDPR, HIPAA, or SOX can result in audit failure.

Poor Data Governance

03

Lack of policies for handling, storing, and deleting data.

Insufficient Monitoring and Incident Response

04

Not having proper monitoring tools or an incident response plan in case of a breach.

Unauthorized Access

05

Weak access controls, leading to data breaches or insider threats.

Enhancing Operational Efficiency

The Importance of Security Controls in IT Audits

Ensuring Data Security and Integrity

Controls safeguard data confidentiality, integrity, and availability, preventing unauthorized access and ensuring accuracy.

Risk Management

Effective controls identify vulnerabilities and mitigate risks, minimizing potential security threats and ensuring a secure IT environment.

Compliance

Controls help organizations adhere to regulations like GDPR and HIPAA, avoiding legal penalties through proper policy implementation.

Operational Efficiency

Regular updates and patch management reduce downtime and improve productivity, ensuring smooth IT system functionality.

Detecting and Responding to Threats

Detective controls monitor for unusual activities, allowing quick response to potential breaches, thus maintaining security.

Maintaining Accountability

Audit logs and access control mechanisms track user activity, ensuring that only authorized personnel access sensitive data.

Ensuring Business Continuity

Disaster recovery plans and backup procedures are critical for maintaining operations during disruptions, ensuring quick recovery.

Preventing Financial Losses

Strong controls reduce the risk of financial damage from breaches and outages, protecting the organization's financial health.

Case Study: Security Control Examples

Examining vital security controls in IT audits for data protection.

Control Type	Description	Role in IT Audit	Impact on Data Security
Password Policy	Requires strong, regularly changed passwords.	Evaluates compliance with security best practices.	Reduces risk of unauthorized access.
Firewall	Monitors and filters network traffic.	Assesses effectiveness in preventing unauthorized access.	Protects network from external threats.
Data Encryption	Encrypts sensitive data in transit and at rest.	Checks for adherence to data protection regulations.	Safeguards data from unauthorized access.
Incident Response Plan	Outlines steps for responding to security breaches.	Reviews readiness and effectiveness of response strategies.	Ensures quick recovery from incidents.
Audit Logs	Tracks system activities to detect suspicious behavior.	Evaluates monitoring and alerting capabilities.	Maintains accountability and traces unauthorized access.

Goal-Based Security Control

Ensuring Robust Protection Through Strategic Measures

Focus on Security Objectives

Goal-based security controls are centered around achieving specific security goals, such as protecting sensitive data.

Protection of Customer Data

A primary aim is safeguarding customer information against breaches and unauthorized access.

Ensuring System Availability

Controls are designed to maintain system uptime and functionality, ensuring continuous service.

Preventing Unauthorized Access

Implementing strong password policies and multi-factor authentication to thwart unauthorized access.

Access Monitoring

Regular monitoring of access points to ensure compliance with security policies and detect anomalies.

Implementation-Based Security Control

Focusing on Specific Steps and Techniques for Security

Defined Controls

Implementation-based controls detail specific actions needed for security.

Use of Tools

Employing various tools to enforce security measures effectively.

Techniques in Security

Applying proven techniques to address potential security vulnerabilities.

Encryption Standards

Specifying encryption methods, such as AES-256, for data protection.

Communication Security

Securing communication channels between servers to prevent data breaches.

Security Control Formulation

Designing robust security controls to mitigate risks effectively.

01

Identify potential threats and vulnerabilities to determine the necessary protections.

Risk Assessment

02

Establish clear security objectives aligned with organizational goals and compliance requirements.

Objective Setting

03

Develop effective security controls tailored to mitigate identified risks and meet objectives.

Control Design

Security Control Formulation

Designing robust security controls to mitigate risks effectively.

04

Deploy the designed security controls across the organization to enhance protection.

Implementation

05

Evaluate the effectiveness of implemented controls through regular testing and updates.

Testing

Security Architecture Design

Cyber Security Audit & Compliance: Ensuring Robust Protection

Framework for Security Controls

Establishes a systematic approach to implement security measures across the organization.

Access Controls

Ensures that only authorized users can access sensitive information, enhancing data protection.

Encryption Protocols

Incorporates encryption methods to protect data in transit and at rest, preventing unauthorized access.

Monitoring Systems

Includes continuous monitoring mechanisms to detect and respond to security incidents promptly.

Design Considerations

Emphasizes the importance of integrating security measures from the initial design phase, akin to building safety features.

Governance & Control Framework

A Multitiered Approach to Cyber Security Oversight

Strategic Tier

The board of directors establishes high-level policies for security control.

Management Tier

The IT security team formulates procedures to implement the strategic policies.

Operational Tier

System administrators are responsible for the day-to-day management of security controls.