Security & Compliances

Ensuring Security, Integrity, and Compliance in IT Systems

Presented by Urvi Chheda At Hack-X MIT WPU

Who Am I

- ISO 27001: Lead Auditor
- Certified Ethical Hacker
- Certified Network Defender
- Subject Matter Expert,HTB

Urvi Chheda

Urvi

Agenda

- What is IT Audit?
- Key Objectives of IT Audits
- Compliance in IT
- Types of IT Audits
- IT Frameworks and Standards
- IT Audit Process
- Compliance and Risk Management
- Conclusion

What is IT Audit?

Definition: An IT audit is an examination of the controls within an entity's IT infrastructure. It evaluates the systems' ability to protect the organization's information and ensure the integrity and confidentiality of data.

Importance:

- Verifies data accuracy
- Ensures compliance with regulations and standards
- Assesses IT controls and processes

Key Objectives of IT Audits

Data Integrity: Ensuring the accuracy and consistency of data.

Confidentiality: Protecting sensitive information from unauthorized access.

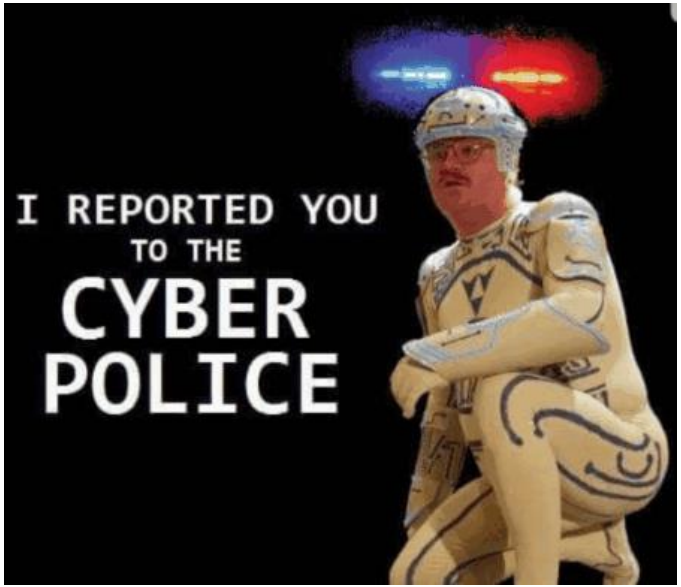
Availability: Ensuring IT systems and data are available when needed.

Compliance: Adhering to legal, regulatory, and organizational policies.

Risk Management: Identifying and mitigating risks to IT assets and infrastructure.

Compliance in IT

Definition: IT compliance refers to adhering to legal, regulatory, and organizational requirements regarding information technology usage.



Importance:

- Avoids legal penalties
- Protects brand reputation
- Prevents security breaches
- Aligns with best practices

Key Compliance Regulations:

- GDPR (General Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI-DSS (Payment Card Industry Data Security Standard)
- ISO 27001 (Information Security Management Systems)

Types of IT Audits

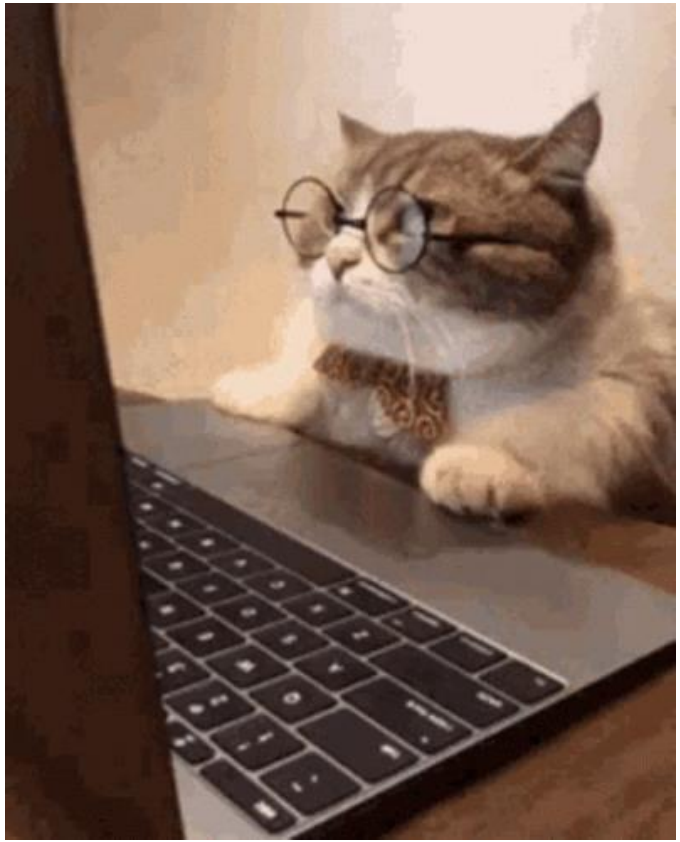
General Control Audits: Assess overall IT environment and controls.

Application Control Audits: Examine specific software applications for data integrity, security, and access controls.

Compliance Audits: Check compliance with laws, regulations, and policies.

Operational Audits: Evaluate the effectiveness and efficiency of IT processes.

Security Audits: Focus on cybersecurity measures, controls, and policies.



IT Frameworks and Standards

COBIT (Control Objectives for Information and Related Technology):

- Framework for developing, implementing, and monitoring IT governance and management practices.

ITIL (Information Technology Infrastructure Library):

- Best practice framework for delivering IT services.

ISO 27001:

- Standard for establishing, implementing, maintaining, and improving an ISMS (Information Security Management System).

NIST (National Institute of Standards and Technology):

- Cybersecurity Framework for managing and reducing IT risk.

IT Audit Process

1. **Planning:** Define audit scope, objectives, and resources.

2. **Risk Assessment**: Identify potential threats and vulnerabilities.

3. **Audit Execution:** Evaluate IT controls, gather data, and analyze findings.

4. **Reporting:** Compile audit findings and recommend corrective actions.

5. **Follow-up:** Review action plan and ensure the implementation of recommendations.

Compliance and Risk Management

Compliance Activities:

- Regular audits and assessments
- Policy reviews and updates
- Employee training

Risk Management:

- Identifying IT risks (cybersecurity, data integrity, operational risks)
- Implementing controls to mitigate risks
- Continuous monitoring and improvement
- Integrating compliance with risk management frameworks

Conclusion

- IT audit and compliance ensure the security, integrity, and availability of information systems.

- Effective audits help organizations adhere to standards, manage risks, and improve operations.

- Compliance with regulations protects organizations from legal, financial, and reputational damage.

- Continuous monitoring and updating are key to maintaining IT governance and security.


THANK
YOU