IT Governance and Audit Practices

Standards and Guidelines for IS Auditing

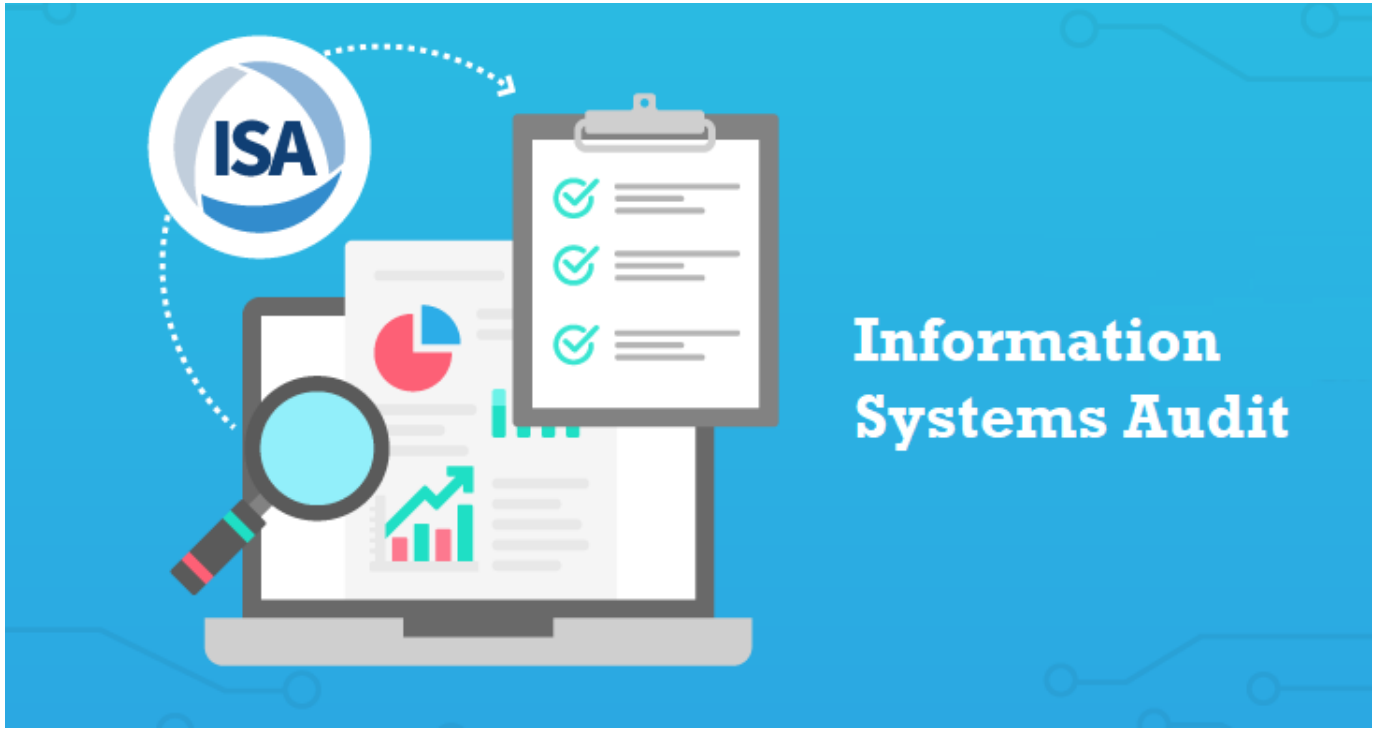
Course: IT Governance and Audit Practices

Program: Master of Science in Information Technology (MSIT)

Prepared by: Paolo Jon B. Caraig

Introduction

- Information Systems (IS) auditing ensures IT systems are secure, reliable, and compliant.
- Organizations rely heavily on IT for operations and decision-making.
- Governance frameworks and standards guide auditors in evaluating IT controls.
- This report covers:
  - Code of Ethics
  - IS Audit Practices & Techniques
  - ISO/IEC 27001
  - ITIL Framework



Objectives

- Understand ethical standards in IS auditing.
- Identify common audit practices and techniques.
- Explain ISO/IEC 27001 information security standards.
- Discuss ITIL’s role in IT governance and service management.

Code of Ethics in IS Auditing

- A Code of Ethics defines professional conduct and responsibilities.
- Ensures trust, integrity, and accountability in auditing.
- Promoted by professional bodies like ISACA.

Core Principles of IS Audit Ethics

- **Integrity** – Honest and responsible performance.
- **Objectivity** – Unbiased audit judgments.
- **Confidentiality** – Protect sensitive information.
- **Competency** – Maintain professional knowledge and skills.

Importance of Ethical Compliance

- Builds stakeholder trust.
- Prevents conflicts of interest.
- Ensures legal and regulatory compliance.
- Protects organizational reputation.

IS Audit Practices Overview

- Systematic evaluation of IT systems and controls.
- Determines effectiveness, efficiency, and security.
- Aligns IT operations with business objectives.

Types of IS Audits

- **Compliance Audit** – Adherence to laws/policies.
- **Operational Audit** – Efficiency of IT operations.
- **Financial Audit** – Accuracy of financial systems.
- **Security Audit** – Protection of information assets.

IS Audit Techniques

- **Risk Assessment** – Identify vulnerabilities.
- **Control Testing** – Evaluate internal controls.
- **Substantive Testing** – Validate data accuracy.
- **Analytical Procedures** – Compare trends/patterns.

Audit Tools & Methods

- Computer-Assisted Audit Techniques (CAATs).
- Data analytics software.
- Network security scanners.
- Log analysis tools.

Overview of ISO/IEC 27001

- International standard for Information Security Management Systems (ISMS).
- Published by ISO and IEC.
- Provides framework for managing sensitive information securely.

Objectives of ISO 27001

- Ensure confidentiality, integrity, availability (CIA triad).
- Manage security risks systematically.
- Protect customer and organizational data.

Key Components of Information Security Management Systems (ISMS)

- Security policies
- Risk assessment & treatment
- Asset management
- Access control
- Incident management
- Business continuity planning

Benefits of ISO 27001 Certification

- Regulatory compliance.
- Reduced cyber risk.
- Improved customer confidence.
- Competitive advantage.

What is ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)?

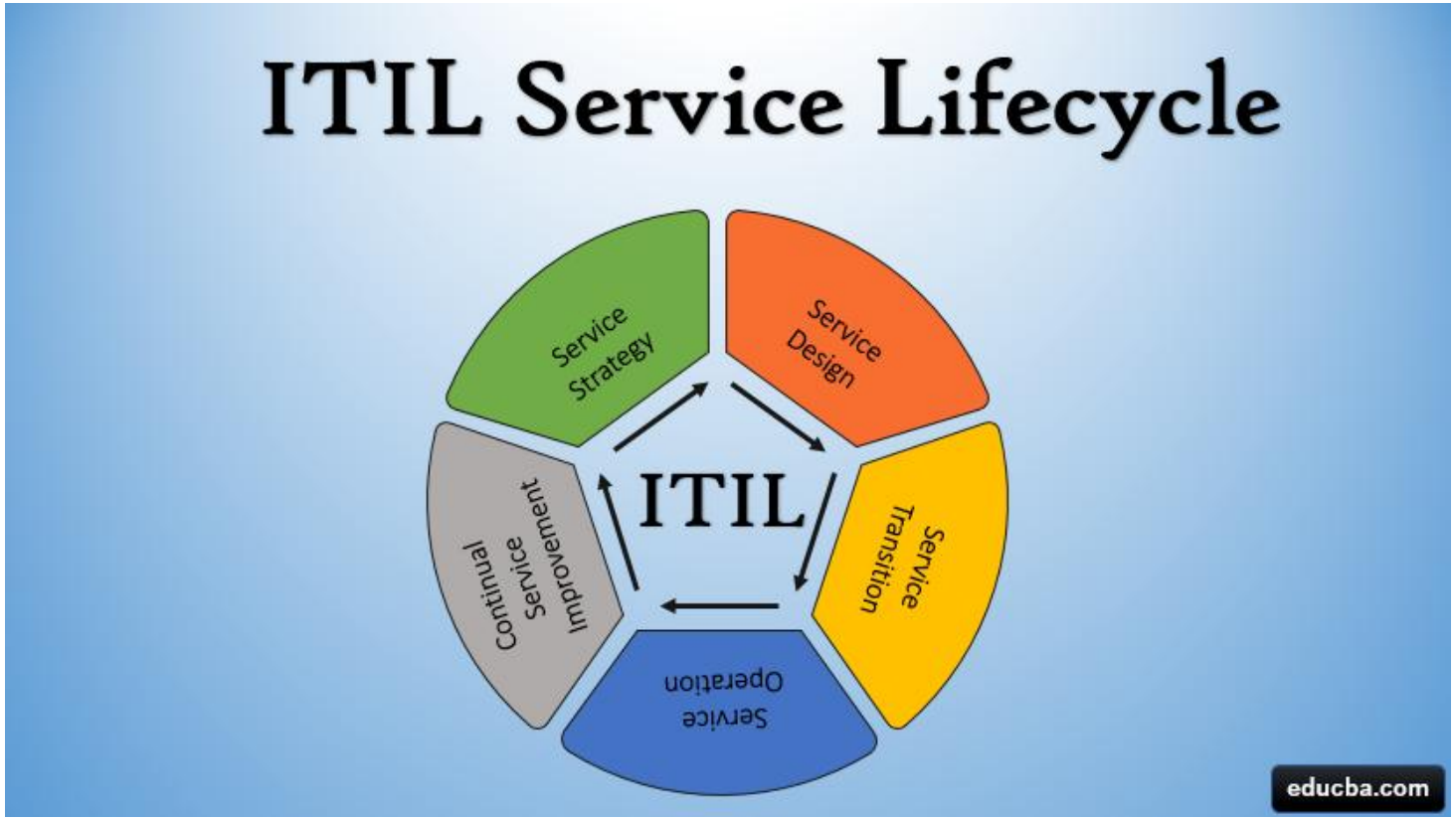
- A globally recognized IT Service Management (ITSM) framework.
- Focuses on aligning IT services with business needs.
- Developed by the UK government (AXELOS ownership now under PeopleCert).

ITIL Framework

ITIL Service Lifecycle (ITIL v3 / concepts still referenced)

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

(ITIL 4 now uses Service Value System but lifecycle is still widely taught.)



Key Benefits of ITIL

- Improved service delivery.
- Better incident/problem management.
- Cost efficiency.
- Enhanced customer satisfaction.
- Stronger IT governance.

Conclusion

- IS auditing ensures IT accountability and risk control.
- Ethical standards guide auditor professionalism.
- ISO 27001 strengthens information security governance.
- ITIL improves IT service quality and operational alignment.
- Together, these frameworks enhance organizational IT governance.

References:

Code of Ethics & IS Auditing
ISACA. (n.d.). *Code of professional ethics*.
https://www.isaca.org/code-of-professional-ethics

ISACA. (n.d.). *IT audit and assurance standards, guidelines, and tools and techniques*.
https://www.isaca.org/resources

IS Audit Practices & Techniques
National Institute of Standards and Technology. (2017). *Guide to computer security log management (Special Publication 800-92)*.
https://csrc.nist.gov/pubs/sp/800/92/final

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*.
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

ISO/IEC 27001
International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security management systems — Requirements*.
https://www.iso.org/isoiec-27001-information-security.html

IT Governance Ltd. (n.d.). *ISO 27001 explained*.
https://www.itgovernance.co.uk/iso27001

ITIL Framework
AXELOS. (2019). *ITIL foundation: ITIL 4 edition*. AXELOS Limited.
https://www.axelos.com/best-practice-solutions/itil

PeopleCert. (n.d.). *ITIL® 4 framework overview*.
https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1