Information System Auditing Process

Learning Objective:

Get a firm grasp of the primary processes for information systems audit.

Topics:

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Audit in accordance with IS audit standards and a risk based IS audit strategy.
- Communicate audit progress, findings, results and recommendations to stakeholders.
- Conduct audit follow-up to evaluate risk-addressal.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting and guidance to improve the quality and control of information systems.
- Identify opportunities for process improvement in IT policies and practices.

Governance & Management of IT

Learning Objective:

Learn about the principles of governance and management of IT for an enterprise.

Topics:

- Evaluate IT strategy for alignment with the organization's objectives.
- Evaluate the effectiveness of IT governance & organizational structure.
- Evaluate the organization's management of IT policies and practices.
- Evaluate the organization's IT policies and practices for regulatory & legal compliance.
- Evaluate IT resources and portfolio management.
- Evaluate the organization's risk management policies and practices.
- Evaluate IT management and monitoring of controls.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate IT supplier selection and contract management processes.
- Evaluate IT service management practices' alignment with business requirements.

- Periodic review of information systems and enterprise architecture.
- Evaluate data governance policies and practices.
- Evaluate the information security program for effectiveness.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Information Systems Acquisition, Development, & Implementation

Learning Objective:

Know how to acquire, develop, and implement information systems for an enterprise.

Topics:

- Evaluate proposed changes to information systems.
- Evaluate the organization's project management policies and practices.
- Evaluate controls at all stages of the information systems' development life cycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Post-implementation review of systems to determine whether project deliverables, controls and requirements are met.
- Evaluate change, configuration, release, and patch management policies and practices.

Information Systems Operations and Business Resilience

Learning Objective:

Gain mastery of how to evaluate enterprise information systems for optimizing business continuity and resilience.

Topics:

- Evaluate the organization's ability to continue business operations.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.

- Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.
- Evaluate problem and incident management policies and practices.
- Evaluate change, configuration, release, and patch management policies and practices.
- Evaluate end-user computing to determine whether the processes are effectively controlled.

Protection of Information Assets

Learning Objective:

Learn to apply IS audit frameworks to ensure that the enterprise's information systems are secure and optimized to meet business objectives.

Topics:

- Audit in accordance with IS audit standards and a risk based IS audit strategy.
- Evaluate problem and incident management policies and practices.
- Evaluate the organization's information security and privacy policies and practices.
- Evaluate physical and environmental controls for safeguarding information assets.
- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
- Evaluate data classification practices for alignment with the organization's policies and applicable external requirements.
- Evaluate policies and practices related to asset life cycle management.
- Evaluate the information security program for effectiveness.
- Perform technical security testing to identify potential threats and vulnerabilities.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.