€TRAINING

CISA Certified Information Systems Auditor

CISA Certified Information Systems Auditor

Introduction:

This program is designed to prepare participants for the certification exam only.

This training program provides comprehensive training on information systems audit and governance. It empowers participants to become prepared for the certification of Information Systems Auditors and contribute to the assurance and governance of information systems within their organizations.

Program Objectives:

At the end of this program, participants will be able to:

- Understand and apply the principles and best practices of information systems audit.
- Assess IT governance, risk management, and compliance processes.
- Evaluate information systems acquisition, development, and implementation practices.
- Review information systems operations, business resilience, and continuity planning.
- Assess the protection of information assets and ensure compliance with security standards.
- Prepare for the certification exam.

Targeted Audience:

- IT auditors and compliance professionals.
- Information security managers and analysts.
- IT risk management professionals.
- System administrators and network engineers.

Program Outline:

Unit 1:

Introduction to Information Systems Audit:

- Overview of information systems audit and its significance in modern organizations.
- Understanding the role and responsibilities of a Certified Information Systems Auditor CISA.

- Key concepts and principles of information systems auditing.
- Relationship between information systems audit and organizational governance.
- Regulatory requirements and industry standards governing information systems audit.

Unit 2:

Governance and Management of IT:

- Understanding IT governance frameworks and best practices.
- Assessing IT strategy, policies, and procedures.
- Evaluating IT organizational structure and resource management.
- Reviewing IT risk management processes and controls.
- Examining IT performance monitoring and assurance mechanisms.

Unit 3:

Information Systems Acquisition, Development, and Implementation:

- Assessing the effectiveness of information systems acquisition processes.
- Evaluating project management practices for information systems development.
- Reviewing system development methodologies and life cycle management.
- Examining system implementation practices and change management processes.
- Ensuring compliance with regulatory requirements and security standards.

Unit 4:

Information Systems Operations and Business Resilience:

- Evaluating information systems operations and service management practices.
- Assessing the effectiveness of IT service delivery and support mechanisms.
- Reviewing IT asset management and data management practices.
- Examining business continuity and disaster recovery planning processes.
- Ensuring compliance with regulatory requirements and industry standards.

Unit 5:

Protection of Information Assets:

- Assessing the effectiveness of information security governance frameworks.
- Evaluating information security policies, procedures, and standards.
- Reviewing access controls and identity management practices.
- Examining security architecture and design principles.
- Ensuring compliance with regulatory requirements and privacy laws.

- Preparation for the certification exam.

Note: This program is designed to prepare participants for the certification exam only.