

Certified Information System Auditor Training Program



This Program is ideally suited to following individuals who are:

- **Fresh University Graduates and like to develop their Career Information System Auditing.**
- **Already working class who are willing to update and learn the new methodologies of information System and Techniques.**
- **Firm's I.T. Manager, IS professionals and Director I.T.**

Program is offered by: 3D Educators – Trainers & Consultants

Table of Contents

Detail

Inauguration

Structure

Topics & Time Allocation

About the Program Designer & Instructor

Syllabus

3D EDUCATORS

TRAINERS & CONSULTANTS

Program Details

Inauguration

The Training Program will be inaugurated by a senior member of 3DEducators

Program Structure

Number of classes in a week	Two Class Per Week
Duration of each class	2-Hour
Total Duration	32 Hours

Other Learning Activities:

Classroom Assignments	6
Presentations by Trainees	1

3D EDUCATORS
About the Program Designer & Instructor

TRA

The "CISA" Program has been designed by the International body ISACA (USA) and will be conducted by Senior most Auditors and consultants who having the huge experience of training and auditing. They have worked with various large multinational organizations and provide the trainings in local and abroad.

The Trainers who are conducting this program have the following positions in the different organization:

- ✓ Information System Auditors
- ✓ Director I.T

They trainers are foreign qualified and having the degrees of PhD, MBA (MIS), Msc. Applied Physics, MCSE + I, MCDBA, A+ Certified and CISA Certified. More they are also the member of CITTA and its Society.

Program Syllabus

COURSE CONTENTS:

Content Area 1: IS Audit Process

(Content Area, Approximately 10% of exam)

1.1 Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.

1.2 Plan specific audits to ensure that IT and business systems are protected and controlled.

1.3 Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.

1.4 Communicate emerging issues, potential risks, and audit results to key stakeholders.

1.5 Advise on the implementation of risk management and control practices within the organization, while maintaining independence.

Knowledge Statements

1.1 Knowledge of ISACA IS Auditing Standards, Guidelines and Procedures and Code of Professional Ethics

1.2 Knowledge of IS auditing practices and techniques

1.3 Knowledge of techniques to gather information and preserve evidence (e.g., observation, inquiry, interview, CAATs, electronic media)

1.4 Knowledge of the evidence life cycle (e.g., the collection, protection, chain of custody)

1.5 Knowledge of control objectives and controls related to IS (e.g., CoBIT)

1.6 Knowledge of risk assessment in an audit context

1.7 Knowledge of audit planning and management techniques

1.8 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution)

1.9 Knowledge of control self-assessment (CSA)

1.10 Knowledge of continuous audit techniques

Content Area 2: IT Governance

(Content Area, Approximately 15% of exam)

2.1 Evaluate the effectiveness of IT governance structure to ensure adequate board control over the decisions, directions, and performance of IT so that it supports the organization's strategies and objectives.

2.2 Evaluate IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.

2.3 Evaluate the IT strategy and the process for its development, approval, implementation, and maintenance to ensure that it supports the organization's strategies and objectives.

2.4 Evaluate the organization's IT policies, standards, and procedures; and the processes for their development, approval, implementation, and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.

2.5 Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standards, and procedures.

2.6 Evaluate IT resource investment, use, and allocation practices to ensure alignment with the organization's strategies and objectives.

2.7 Evaluate IT contracting strategies and policies, and contract management practices to ensure that they support the organization's strategies and objectives.

2.8 Evaluate risk management practices to ensure that the organization's IT related risks are properly managed.

2.9 Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.

Knowledge Statements

2.1 Knowledge of the purpose of IT strategies, policies, standards and procedures for an organization and the essential elements of each

2.2 Knowledge of IT governance frameworks

2.3 Knowledge of the processes for the development, implementation and maintenance of IT strategies, policies, standards and procedures (e.g., protection of information assets, business continuity and disaster recovery, systems and infrastructure lifecycle management, IT service delivery and support)

2.4 Knowledge of quality management strategies and policies

2.5 Knowledge of organizational structure, roles and responsibilities related to the use and management of IT

2.6 Knowledge of generally accepted international IT standards and guidelines

2.7 Knowledge of enterprise IT architecture and its implications for setting long-term strategic directions

2.8 Knowledge of risk management methodologies and tools

2.9 Knowledge of the use of control frameworks (e.g., CobiT, COSO, ISO 17799)

2.10 Knowledge of the use of maturity and process improvement models (e.g., CMM, CobiT)

2.11 Knowledge of contracting strategies, processes and contract management practices
2.12 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI])

2.13 Knowledge of relevant legislative and regulatory issues (e.g., privacy, intellectual property, corporate governance requirements)

2.14 Knowledge of IT human resources (personnel) management

2.15 Knowledge of IT resource investment and allocation practices (e.g., portfolio management return on investment (ROI))

Content Area 3: Systems and Infrastructure Lifecycle Management

(Content Area, Approximately 16% of exam)

- 3.1 Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organization's business goals.
- 3.2 Evaluate the project management framework and project governance practices to ensure that business objectives are achieved in a cost-effective manner while managing risks to the organization.
- 3.3 Perform reviews to ensure that a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- 3.4 Evaluate proposed control mechanisms for systems and/or infrastructure during specification, development/acquisition, and testing to ensure that they will provide safeguards and comply with the organization's policies and other requirements.
- 3.5 Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organization's objectives.
- 3.6 Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.
- 3.7 Perform post-implementation review of systems and/or infrastructure to ensure that they meet the organization's objectives and are subject to effective internal control.
- 3.8 Perform periodic reviews of systems and/or infrastructure to ensure that they continue to meet the organization's objectives and are subject to effective internal control.
- 3.9 Evaluate the process by which systems and/or infrastructure are maintained to ensure the continued support of the organization's objectives and are subject to effective internal control.
- 3.10 Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organization's policies and procedures.

Knowledge Statements

- 3.1 Knowledge of benefits management practices, (e.g., feasibility studies, business cases)
- 3.2 Knowledge of project governance mechanisms (e.g., steering committee, project oversight board)
- 3.3 Knowledge of project management practices, tools, and control frameworks
- 3.4 Knowledge of risk management practices applied to projects
- 3.5 Knowledge of project success criteria and risks
- 3.6 Knowledge of configuration, change and release management in relation to development and maintenance of systems and/or infrastructure
- 3.7 Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity, and authorization of transactions and data within IT systems applications
- 3.8 Knowledge of enterprise architecture related to data, applications, and technology (e.g., distributed applications, web-based applications, web services, n-tier applications)
- 3.9 Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis)

3.10 Knowledge of acquisition and contract management processes (e.g., evaluation of vendors, preparation of contracts, vendor management, escrow)

3.11 Knowledge of system development methodologies and tools and an understanding of their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)

3.12 Knowledge of quality assurance methods

3.13 Knowledge of the management of testing processes (e.g., test strategies, test plans, test environments, entry and exit criteria)

3.14 Knowledge of data conversion tools, techniques, and procedures

3.15 Knowledge of system and/or infrastructure disposal procedures

3.16 Knowledge of software and hardware certification and accreditation practices

3.17 Knowledge of post-implementation review objectives and methods (e.g., project closure, benefits realization, performance measurement)

3.18 Knowledge of system migration and infrastructure deployment practices

Content Area 4: IT Service Delivery and Support

(Content Area, Approximately 14% of exam)

4.1 Evaluate service level management practices to ensure that the level of service from internal and external service providers is defined and managed.

4.2 Evaluate operations management to ensure that IT support functions effectively meet business needs.

4.3 Evaluate data administration practices to ensure the integrity and optimization of databases.

4.4 Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives.

4.5 Evaluate change, configuration, and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented.

4.6 Evaluate problem and incident management practices to ensure that incidents, problems, or errors are recorded, analyzed, and resolved in a timely manner.

4.7 Evaluate the functionality of the IT infrastructure (e.g., network components, hardware, system software) to ensure that it supports the organization's objectives.

Knowledge Statements

4.1 Knowledge of service level management practices

4.2 Knowledge of operations management best practices (e.g., workload scheduling, network services management, preventive maintenance)

4.3 Knowledge of systems performance monitoring processes, tools, and techniques (e.g., network analyzers, system utilization reports, load balancing)

4.4 Knowledge of the functionality of hardware and network components (e.g., routers, switches, firewalls, peripherals)

4.5 Knowledge of database administration practices

4.6 Knowledge of the functionality of system software including operating systems, utilities, and database management systems

4.7 Knowledge of capacity planning and monitoring techniques

4.8 Knowledge of processes for managing scheduled and emergency changes to the production systems and/or infrastructure including change, configuration, release, and patch management practices

4.9 Knowledge of incident/problem management practices (e.g., help desk, escalation procedures, tracking)

4.10 Knowledge of software licensing and inventory practices

4.11 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)

Content Area 5: Protection of Information Assets

(Content Area, Approximately 31% of exam)

5.1 Evaluate the design, implementation, and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.

5.2 Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.

5.3 Evaluate the design, implementation, and monitoring of environmental controls to prevent or minimize loss.

5.4 Evaluate the design, implementation, and monitoring of physical access controls to ensure that information assets are adequately safeguarded.

5.5 Evaluate the processes and procedures used to store, retrieve, transport, and dispose of confidential information assets.

Knowledge Statement

5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment)

5.2 Knowledge of logical access controls for the identification, authentication, and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus, profiles)

5.3 Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies, identity management)

5.4 Knowledge of attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service, spamming)

5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

5.6 Knowledge of network and Internet security devices, protocols, and techniques (e.g., SSL, SET, VPN, NAT)

5.7 Knowledge of intrusion detection systems and firewall configuration, implementation, operation, and maintenance

- 5.8 Knowledge of encryption algorithm techniques (e.g., AESRSA)
- 5.9 Knowledge of public key infrastructure (PKI) components (e.g., certification authorities, registration authorities) and digital signature techniques
- 5.10 Knowledge of virus detection tools and control techniques
- 5.11 Knowledge of security testing and assessment tools (e.g., penetration testing, vulnerability scanning)
- 5.12 Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems, water sensors)
- 5.13 Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks, tokens)
- 5.14 Knowledge of data classification schemes (e.g., public, confidential, private, and sensitive data)
- 5.15 Knowledge of voice communications security (e.g., voice over IP)
- 5.16 Knowledge of the processes and procedures used to store, retrieve, transport, and dispose of confidential information assets
- 5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., PDAs, USB devices, Bluetooth devices)

Content Area 6: Business Continuity and Disaster Recovery

(Content Area, Approximately 14% of exam)

- 6.1 Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing.
- 6.2 Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.
- 6.3 Evaluate the organization's business continuity plan to ensure its ability to continue essential business operations during the period of an IT disruption.

Knowledge Statements

- 6.1 Knowledge of data backup, storage, maintenance, retention and restoration processes, and practices
- 6.2 Knowledge of regulatory, legal, contractual, and insurance issues related to business continuity and disaster recovery
- 6.3 Knowledge of business impact analysis (BIA)
- 6.4 Knowledge of the development and maintenance of the business continuity and disaster recovery plans
- 6.5 Knowledge of business continuity and disaster recovery testing approaches and methods
- 6.6 Knowledge of human resources management practices as related to business continuity and disaster recovery (e.g., evacuation planning, response teams)

6.7 Knowledge of processes used to invoke the business continuity and disaster recovery plans

6.8 Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites)

3D EDUCATORS

TRAINERS & CONSULTANTS
