

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

TRF

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:

Domain 1—The Process of Auditing Information Systems (14%)

Provide audit services in accordance with IT audit standards to assist the organization in protecting and controlling information systems.

Domain 1—Task Statements:

- 1.1 Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- 1.2 Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- 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.

Domain 1—Knowledge Statements:

- 1.1 Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
- 1.2 Knowledge of risk assessment concepts, tools and techniques in an audit context
- 1.3 Knowledge of control objectives and controls related to information systems
- 1.4 Knowledge of audit planning and audit project management techniques, including follow-up
- 1.5 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT
- 1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits
- 1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis) used to gather, protect and preserve audit evidence
- 1.8 Knowledge of different sampling methodologies
- 1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure)
- 1.10 Knowledge of audit quality assurance systems and frameworks

Domain 2—Governance and Management of IT (14%)

Provide assurance that the necessary leadership and organization structure and processes are in place to achieve objectives and to support the organization's strategy.

Domain 2—Task Statements:

- 2.1 Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
- 2.2 Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
- 2.3 Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with 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, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.

2.5 Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.

2.6 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures.

2.7 Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.

2.8 Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.

2.9 Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.

2.10 Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.

2.11 Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

Domain 2—Knowledge Statements:

2.1 Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines, and practices

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

2.3 Knowledge of organizational structure, roles and responsibilities related to IT

2.4 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures

2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions

2.6 Knowledge of relevant laws, regulations and industry standards affecting the organization

2.7 Knowledge of quality management systems

2.8 Knowledge of the use of maturity models

2.9 Knowledge of process optimization techniques

2.10 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management)

2.11 Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships

2.12 Knowledge of enterprise risk management

2.13 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI])

2.14 Knowledge of IT human resources (personnel) management practices used to invoke the business continuity plan

2.15 Knowledge of business impact analysis (BIA) related to business continuity planning

2.16 Knowledge of the standards and procedures for the development and maintenance of the business continuity plan and testing methods

Domain 3—Information Systems Acquisition, Development, and Implementation (19%)

Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

Domain 3—Task Statements:

3.1 Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.

3.2 Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.

- 3.3 Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- 3.4 Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- 3.5 Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and organization's requirements are met.
- 3.6 Conduct post-implementation reviews of systems to determine whether project deliverables, controls and organization's requirements are met.

Domain 3—Knowledge Statements:

- 3.1 Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], ROI)
- 3.2 Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office)
- 3.3 Knowledge of project management control frameworks, practices and tools
- 3.4 Knowledge of risk management practices applied to projects
- 3.5 Knowledge of IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications)
- 3.6 Knowledge of acquisition practices (e.g., evaluation of vendors, vendor management, escrow)
- 3.7 Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)
- 3.8 Knowledge of project success criteria and risks
- 3.9 Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data
- 3.10 Knowledge of system development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)
- 3.11 Knowledge of testing methodologies and practices related to information systems development
- 3.12 Knowledge of configuration and release management relating to the development of information systems
- 3.13 Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures.
- 3.14 Knowledge of post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement)

Domain 4—Information Systems Operations, Maintenance and Support (23%)

Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

Domain 4—Task Statements:

- 4.1 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
- 4.2 Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- 4.3 Evaluate third party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
- 4.4 Evaluate operations and end-user procedures to determine whether scheduled and non-scheduled processes are managed to completion.
- 4.5 Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
- 4.6 Evaluate data administration practices to determine the integrity and optimization of databases.
- 4.7 Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT

services meet the organization's objectives.

4.8 Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.

4.9 Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the organization's production environment are adequately controlled and documented.

4.10 Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing.

4.11 Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

Domain 4—Knowledge Statements:

4.1 Knowledge of service level management practices and the components within a service level agreement

4.2 Knowledge of techniques for monitoring third party compliance with the organization's internal controls

4.3 Knowledge of operations and end-user procedures for managing scheduled and non-scheduled processes

4.4 Knowledge of the technology concepts related to hardware and network components, system software and database management systems

4.5 Knowledge of control techniques that ensure the integrity of system interfaces

4.6 Knowledge of software licensing and inventory practices

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

4.8 Knowledge of database administration practices

4.9 Knowledge of capacity planning and related monitoring tools and techniques

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

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

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

4.13 Knowledge of data backup, storage, maintenance, retention and restoration practices

4.14 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery

4.15 Knowledge of business impact analysis (BIA) related to disaster recovery planning

4.16 Knowledge of the development and maintenance of disaster recovery plans

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

4.18 Knowledge of processes used to invoke the disaster recovery plans

4.19 Knowledge of disaster recovery testing methods

Domain 5—Protection of Information Assets (30%)

Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

Domain 5—Task Statements:

5.1 Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.

5.2 Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.

5.3 Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.

5.4 Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.

5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

Domain 5—Knowledge Statements:

- 5.1 Knowledge of the techniques for the design, implementation, and monitoring of security controls, including security awareness programs
- 5.2 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
- 5.3 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data
- 5.4 Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems), and database management systems.
- 5.5 Knowledge of risks and controls associated with virtualization of systems
- 5.6 Knowledge of the configuration, implementation, operation and maintenance of network security controls
- 5.7 Knowledge of network and Internet security devices, protocols, and techniques
- 5.8 Knowledge of information system attack methods and techniques
- 5.9 Knowledge of detection tools and control techniques (e.g., malware, virus detection, spyware)
- 5.10 Knowledge of security testing techniques (e.g., intrusion testing, vulnerability scanning)
- 5.11 Knowledge of risks and controls associated with data leakage
- 5.12 Knowledge of encryption-related techniques
- 5.13 Knowledge of public key infrastructure (PKI) components and digital signature techniques
- 5.14 Knowledge of risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs)
- 5.15 Knowledge of controls and risks associated with the use of mobile & wireless devices
- 5.16 Knowledge of voice communications security (e.g., PBX, VoIP)
- 5.17 Knowledge of the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody)
- 5.18 Knowledge of data classification standards and supporting procedures
- 5.19 Knowledge of physical access controls for the identification, authentication and restriction of users to authorized facilities
- 5.20 Knowledge of environmental protection devices and supporting practices
- 5.21 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

3D EDUCATORS

TRAINERS & CONSULTANTS
