Global Information Security Society for Professionals of Pakistan

Certified Information System Auditor-CISA

Trainer: Ali Nouman

How to use Zoom Client

If you are using Zoom for the first time than these points will be useful for you .

- If you are unable to hear audio than you need to connect via device audio . Look at the bottom left corner .
- Kindly turn off your camera while connecting to Zoom as we respect your privacy .
- The Speaker will keep you muted during the session however if you want to ask any question during QA session ,you can click on the three dots and “raise hand” so that the speaker can unmute you .
- You can click on the participants tab to chat with host or to send a member to all participants
- If you are attending the session while doing some other work ,kindly mute yourself in case if the host unmutes all users during QA session

Trainer Profile

- Ali Nouman is Working as Manager IT Security in one of the top Bank, based in Qatar. Over 15 years of IT experience and focus on Information Security for the last 10 years. He is CISA, CISSP, CISM, COBIT-5, IRCA registered Lead Auditor of ISO ISMS, AWS and ITIL certified as well as founding member of (ISC)² Qatar Chapter. He is visiting faculty member and CISA Trainer at SKANS, ISACA Lahore Chapter and Audit General of Pakistan, He has previously worked in Teradata, ABL, BOP and Samba Bank. He is a Corporate trainer of different area of information security, governance and CISA. LinkedIn :
- https://www.linkedin.com/in/ali-nouman-cissp-aws-cisa-cism-isms-itil-ba3a8225/

Welcome!

- This program is designed to prepare you for success on the CISA exam, one step in the process of becoming certified.
- The program will include:
  - Information about the CISA exam and certification
  - Detailed coverage of the body of knowledge required by CISA
  - Activities, exam discussion questions, and group discussions
  - Real-world examples of CISA subject matter

Domain 1

The Process of Auditing Information Systems

Domain 1

The Process of Auditing Information Systems

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

Domain 1

The Process of Auditing Information Systems: Task 1

Task 1:

Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited

Domain 1

The Process of Auditing Information Systems: Task 1

IS Audit Function

- IS auditing is the formal examination, interview and/or testing of information systems to determine whether:
  - Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines.
  - IS data and information have appropriate levels of confidentiality, integrity and availability.
  - IS operations are being accomplished efficiently, and effectiveness targets are being met.

Domain 1

The Process of Auditing Information Systems: Task 1

IS Auditor Skills

- ISACA IS Audit and Assurance Standards require that the IS auditor be technically competent (1006 Proficiency).
- This is achieved through continuing education.
- CISA candidates do NOT need to memorize the ISACA IS Audit and Assurance Standards, Guidelines, and Tools and Techniques, but they must be able to apply the standard, guideline or ISACA Code of Professional Ethics in a given situation.

Domain 1

The Process of Auditing Information Systems: Task 1

Code of Professional Ethics: i

- Support the implementation of, and encourage compliance with, appropriate standards, procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
- Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.

Domain 1

The Process of Auditing Information Systems: Task 1

Code of Professional Ethics: ii

- Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
- Maintain competency in their respective fields, and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence

Domain 1

The Process of Auditing Information Systems: Task 1

Code of Professional Ethics: iii

- Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
- Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security and risk management.

Domain 1

The Process of Auditing Information Systems: Task 1

Standards :

- Standards contain statements of mandatory requirements.
- These standards inform:
  - IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the CISA designation of their requirements

Domain 1

The Process of Auditing Information Systems: Task 1

Guidelines :

- The objective of the ISACA IS Audit and Assurance Guidelines is to provide guidance and additional information on how to comply with the ISACA IS Audit and Assurance Standards.
- The IS auditor and assurance professional should:
  - Consider these guidelines in determining how to implement the standards.
  - Use professional judgment in applying the guidelines to specific audits.
  - Be able to justify any departure from the ISACA IS Audit and Assurance Standards.

Domain 1

The Process of Auditing Information Systems: Task 1

Documents and their interpretation

- Policy:
- Standard
- Procedure(SOP):
- Law & Regulations
- Guidelines
- Baseline
- Bench Mark

Domain 1

The Process of Auditing Information Systems: Task 1

Tool and Techniques:

- The tools and techniques documents provide information on how to meet the standards when performing IS auditing work but do not set requirements.
- Tools and techniques documents include:
  - White papers
  - Audit/Assurance programs
  - COBIT 5 family of products
  - Technical and Risk Management Reference series
  - ISACA Journal IT Audit Basics

Domain 1

The Process of Auditing Information Systems: Task 1

Laws and Regulations:

- Certain industries, such as banks and internet service providers (ISPs), are closely regulated. These legal regulations may pertain to financial, operational and IS audit functions.
- There are two areas of concern that impact the audit scope and objectives:
  - Legal requirements placed on the audit
  - Legal requirements placed on the auditee and its systems, data management, reporting, etc.
- **Examples include:**
  - US Health Insurance Portability and Accountability Act (HIPAA)
  - US Sarbanes-Oxley Act of 2002
  - Basel Accords
  - Protection of Personal Data Directives and Electronic Commerce within the European Community

Domain 1

The Process of Auditing Information Systems: Task 1

Control Self Assessment-CSA:

- Control self-assessment (CSA) is an assessment of controls made by the staff and management to assure stakeholders, customers and other parties of the reliability of the organization's internal controls.
- It can consist of simple questionnaires to facilitated workshops.
- **Tools include:**
  - Management meetings
  - Client workshops
  - Worksheets
  - Rating sheets

Domain 1

The Process of Auditing Information Systems: Task 1

CSA Objectives:

- The primary objective is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas.
- CSA empowers workers to assess or even design the control environment.
- An IS auditor's role is to facilitate and guide the auditees in assessing their environment by providing insight about the objectives of controls based on the risk assessment

Domain 1

The Process of Auditing Information Systems: Task 1

CSA Pros and & Cons:

Advantages	Disadvantages
• Early detection of risk • More effective and improved internal controls • Creation of cohesive teams through employee involvement • Developing sense of ownership • Increased employee awareness • Increased communication • Improved audit rating process • Reduction in control cost • Assurance provided to stakeholders and customers	• Mistaken as an audit function replacement • Regarded as an additional workload • Failure to act on improvement suggestions could damage employee morale • Lack of motivation may limit effectiveness in the detection of weak controls

Traditional vs. CSA

Traditional	CSA
Assigns duties/supervises staff	Empowered/accountable employees
Policy/rule-driven	Continuous improvement/learning curve
Limited employee participation	Extensive employee participation and training
Narrow stakeholder focus	Broad stakeholder focus
Auditors and other specialists	Staff at all levels, in all functions, are the primary control analysts.

GISSP

THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman