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 Auditor 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/

Domain 2

Governance and Management of IT

Session 1.4

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

HR Management

Recruiting	Selecting	Training
Promoting	Measuring performance	Discipline
Staff retention	Mandatory leave	Succession planning

Discussion Question-1

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.
B. inadequate succession planning.
C. one person knowing all parts of a system.
D. a disruption of operations.

IT Organizational Structure

- Within an organization, the IT department can be structured in a variety of ways.
- An organizational chart provides a clear definition of a department's hierarchy and lines of authority.
- The IS auditor should compare observed roles and responsibilities with formal organizational structures and job descriptions.

IT Functions

- Generally, the following IT functions should be reviewed by the IS auditor:
  - Systems development management
  - Project management
  - Help or service desk administration
  - End-user activities and their management
  - Data management
  - Quality assurance management
  - Information security management

IT Functions (cont'd)

- Additionally, these functions should be reviewed by the IS auditor:
  - Vendor and outsourcer management
  - Infrastructure operations and maintenance
  - Removable media management
  - Data entry
  - Supervisory control and data acquisition
  - Systems and security administration
  - Database administration
  - Applications and infrastructure development and maintenance
  - Network management

Discussion Question-2

When auditing the IT governance framework and IT risk management practices that exist within an organization, the IS auditor identified some undefined responsibilities regarding IT management and governance roles. Which of the following recommendations is the **MOST** appropriate?

A. Review the strategic alignment of IT with the business.
B. Implement accountability rules within the organization.
C. Ensure that independent IS audits are conducted periodically.
D. Create a chief risk officer (CRO) role in the organization.

Discussion Question-3

When auditing the archiving of the company's email communications, the IS auditor should pay the **MOST** attention to:

A. the existence of a data retention policy.
B. the storage capacity of the archiving solution.
C. the level of user awareness concerning email use.
D. the support and stability of the archiving solution manufacturer.

Segregation of IT Duties

- While actual job titles and organizational structures vary across enterprises, an IS auditor must obtain enough information to understand and document the relationships among various job functions, responsibilities and authorities.
- The IS auditor must also assess the adequacy of SoD.
- SoD limits the possibility that a single person will be responsible for functions in such a way that errors or misappropriations could occur undetected.
- SoD is an important method to discourage and prevent fraudulent or malicious acts.

SoD Guidelines

- Duties that should be segregated include:
  - Asset custody
  - Authorization capability
  - Transaction recording
- Both IS and end-user departments should be organized to meet SoD policies.

SoD Guidelines (cont'd)

- If adequate SoD does not exist, the following may occur with a lower likelihood of detection:
  - Misappropriation of assets
  - Misstated financial statements
  - Inaccurate financial documentation (due to errors or irregularities)
  - Improper use of funds or modification of data
  - Unauthorized or inaccurate modification of programs

Discussion Question-4

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls

Change Management

- Organizational change management uses a defined and documented process to identify and apply technology improvements at both the infrastructure and application levels.
- The IT department is the focal point for such changes and leads or facilitates the changes with senior management support.
- Communication is an important component of change management, and end-users must be informed of the impact and benefits of changes.

Discussion Question-5

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.

B. inadequate succession planning.

C. one person knowing all parts of a system.

D. a disruption of operations.

IT Balanced Scorecard

- The IT balanced scorecard (BSC) is a management evaluation technique that can be applied to the GEIT process.
- It goes beyond traditional financial evaluation by measuring:
  - Customer (or user) satisfaction
  - Internal operational processes
  - The ability to innovate

GISSP

THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman