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




Enterprise Architecture

- Enterprise architecture (EA) is a practice focused on documenting an organization's IT assets in a structured manner.
- EA facilitates the understanding of, management of, and planning for IT investments through comparison of the current state and an optimized future state.

Enterprise Architecture (cont'd)

- EA can be approached from one of two differing perspectives, as follows:
  - Technology-driven EA — Seeks to clarify the complex technology choices faced by an organization in order to provide guidance on the implementation of various solutions.
  - Business-driven EA — Attempts to understand the organization in terms of its core processes, and derive the optimum mix of technologies needed to support these processes.

Discussion Question-1

Which of the following choices is the **PRIMARY** benefit of requiring a steering committee to oversee IT investment?

A. To conduct a feasibility study to demonstrate IT value
B. To ensure that investments are made according to business requirements
C. To ensure that proper security controls are enforced
D. To ensure that a standard development methodology is implemented

Discussion Question-2

As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirements.
B. baseline security following good practices.
C. institutionalized and commoditized solutions.
D. an understanding of risk exposure.

IT Governing Committees

- Organizations often have executive-level strategy and steering committees to handle organization-wide IT issues.
- The IS auditor should know the responsibilities of, authority possessed by and membership of such committees.

IT Committee Analysis

Level	IT Strategy Committee	IT Steering Committee
Responsibility	Provides insight and advice to the board across a range of IT topics	Decides the level and allocation of IT spending, aligns and approves the enterprise's IT architecture, and other oversight functions.
Authority	Advises the board and management on IT strategy, focusing on current and future strategic IT issues	Assists the executive in the delivery of IT strategy, overseeing management of IT service delivery, projects and implementation
Membership	Includes board members and specialist non-board members	Includes sponsoring executive, business executive (key users), chief information officer (CIO) and key advisors, as required

Source: ISACA, *CISA Review Manual 26th Edition*, figure 2.4

Security: *A Governance Issue*

- Information security has become a significant governance issue due to:
  - Global networking
  - Rapid technological innovation and change
  - Increase in threat agent sophistication
  - Extension of organizations beyond their traditional boundaries
- As a result of these, negligence in the area of information security will diminish an organization's ability to take advantage of IT opportunities while also mitigating risk.

Information Security

- Information security governance is the responsibility of the board of directors and executive management.
- Information security governance is a subset of corporate governance, providing strategic direction for security activities and ensuring that objectives are achieved.
- An information security program comprises the leadership, organizational structures and the processes that safeguard information.

Information Security (cont'd)

- The information security governance framework will generally consist of:
  - A security strategy linked with business objectives
  - Security policies that address strategy, controls and regulation
  - Standards to ensure that procedures and guidelines comply with policies
  - An effective security organizational structure without conflicts of interest
  - Monitoring procedures to ensure compliance and provide feedback on effectiveness

Sourcing Practices

- Sourcing practices relate to the way in which the enterprise obtains the IT functions required to support the business.
- These functions may be performed:
  - By the organization's staff in-house, or "insourced"
  - By staff of a vendor, or "outsourced"
  - By a mix of both insourced and outsourced methods

Sourcing Practices (cont'd)

- The functions may be performed across the globe in a variety of arrangements, including:
  - Onsite — Staff works onsite in the IT department.
  - Offsite — Staff works at a remote location in the same geographical region.
  - Offshore — Staff works at a remote location in a different geographical region.

Cloud Computing

- Cloud-based computing brings specific issues, including:
  - A lack of agreed-upon definitions.
  - Various models describing cloud computing result in differing risk and benefits.
  - Additional legal requirements may pertain to cloud storage.
- Several service models and deployment methods are applied to cloud computing; each of these raise specific considerations.

Issues in Service Models

Infrastructure as a Service (IaaS)

- Options to minimize the impact if the cloud provider has a service interruption

Platform as a Service (PaaS)

- Availability, confidentiality
- Privacy and legal liability in the event of a security breach
- Data ownership
- Concerns regarding e-discovery

Software as a Service (SaaS)

- Who owns the applications?
- Where do the applications reside?

Issues in Deployment Models

Private cloud — Operated solely for an organization

- Provides cloud services with minimum risk, but may not provide the scalability and agility of public cloud services

Community cloud — Shared by several organizations

- Same as private cloud services, plus data may be stored with the data of competitors

Public cloud — Owned by an organization selling cloud services

- Data may be stored with the data of competitors
- Data may be stored in unknown locations
- Data may not be easily retrievable

Hybrid cloud — Binding of two or more cloud deployment types

- Data labeling and classification beneficial to ensure assignment to correct cloud type
- Aggregate risk of merging different deployment models

Discussion Question-3

An IS auditor is evaluating the IT governance framework of an organization. Which of the following would be the **GREATEST** concern?

A. Senior management has limited involvement.
B. Return on investment (ROI) is not measured.
C. Chargeback of IT cost is not consistent.
D. Risk appetite is not quantified.

Discussion Question-4

Which of the following IT governance good practices improves strategic alignment?

A. Supplier and partner risk is managed.
B. A knowledge base on customers, products, markets and processes is in place.
C. A structure is provided that facilitates the creation and sharing of business information.
D. Top management mediates between the imperatives of business and technology.

GISSP

THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman