# 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 2.4

**Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.**

# IT Portfolio Management

- IT portfolio management is distinct from IT financial management.
- It has a strategic goal in determining IT direction toward:
  - What the enterprise will begin to invest in
  - What the enterprise will continue to invest in
  - What the enterprise will divest
- Key governance practices in IT portfolio management include the evaluation, direction and monitoring of value optimization.

# *IT Portfolio Management* (cont'd)

- The most significant advantage of IT portfolio management is agility in adjusting investments based on built-in feedback mechanisms.
- Implementation methods include:
  - Risk profile analysis
  - Diversification of projects, infrastructure and technologies
  - Continuous alignment with business goals
  - Continuous improvement

# Discussion Question-1

After the merger of two organizations, multiple self-developed legacy applications from both organizations are to be replaced by a new common platform. Which of the following would be the **GREATEST** risk?

A. Project management and progress reporting is combined in a project management office which is driven by external consultants.

B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.

C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.

D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

# Discussion Question-2

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

A. enterprise data model.

B. IT balanced scorecard (BSC).

C. IT organizational structure.

D. historical financial statements.

# Process Maturity Frameworks

- Maintaining consistency, efficiency and effectiveness of IT processes requires the implementation of a process maturity framework.
- Several different models may be encountered in organizations, including:
  - COBIT Process Assessment Model (PAM) — defines the minimum requirements for conducting an assessment to ensure reliable results
  - IDEAL model — designed to guide the planning and implementation of effective software improvement
  - CMMI — provides the essential elements of effective processes; used as a guide to process improvement across a project, division or organization

# The PDCA Method

**Plan**
- Establish objectives and processes needed to deliver desired results.

**Do**
- Implement the plan, collecting data for charting and analysis.

**Check**
- Study results from the “Do” step, looking for deviations from desired results.

**Act**
- Analyze deviations and request corrective actions.

# Quality Management

- The development and maintenance of defined and documented IT quality management processes is evidence of effective GEIT.
- Quality management defines a set of tasks that produce desired results when properly performed.
- Various standards provide guidelines for the governance of quality management, including those in ISO/IEC 27000.
- The IS auditor should be aware of quality management. However, the CISA exam does not test specifics on any ISO standards.

# Discussion Question-3

An IS auditor is performing a review of the software quality management process in an organization. The **FIRST** step should be to:

A. verify how the organization follows the standards.
B. identify and report the controls currently in place.
C. review the metrics for quality evaluation.
D. request all standards that have been adopted by the organization.

# Discussion Question-4

When developing a formal enterprise security program, the **MOST** critical success factor (CSF) would be the:

A. establishment of a review board.

B. creation of a security unit.

C. effective support of an executive sponsor.

D. selection of a security process owner.

# Performance Optimization

- Performance optimization is the process of improving both perceived service performance while bringing IS productivity to the highest level possible.
- Ideally, this productivity will be gained without excessive additional investment in the IT infrastructure.
- Effective performance measures are used to create and facilitate action to improve both performance and GEIT.
- These depend upon:
  - The clear definition of performance goals
  - The establishment of effective metrics to monitor goal achievement

# Tools and Techniques

- Several tools and techniques can be employed to facilitate performance measurement, ensure good communication and support organizational change.
- These include:
  - Six Sigma
  - IT BSC
  - KPIs
  - Benchmarking
  - Business process reengineering (BPR)
  - Root cause analysis
  - Life cycle cost-benefit analysis

# GISSP

# THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman