Global Information Security Society for Professionals of Pakistan

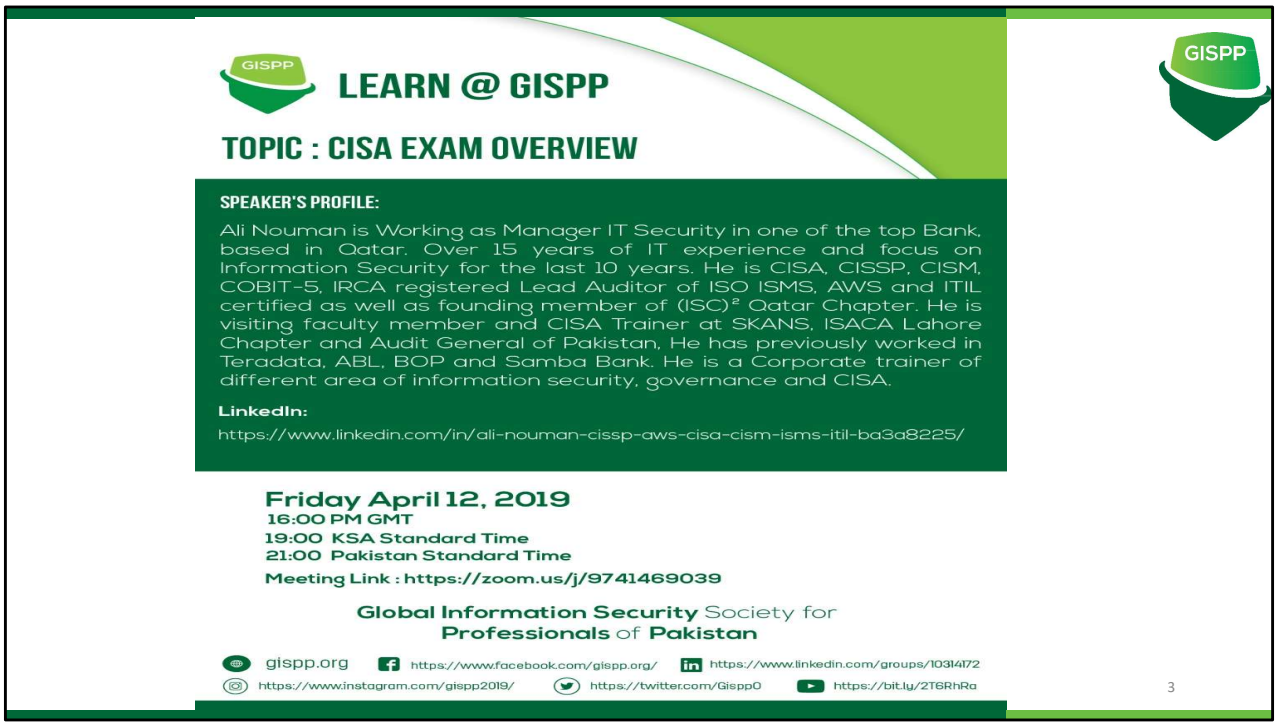
Certified Information System Auditor-CISA

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


GISPP
LEARN @ GISPP
TOPIC : CISA EXAM OVERVIEW
SPEAKER'S 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/
Friday April 12, 2019
16:00 PM GMT
19:00 KSA Standard Time
21:00 Pakistan Standard Time
Meeting Link : https://zoom.us/j/9741469039
Global Information Security Society for Professionals of Pakistan
gispp.org
https://www.facebook.com/gispp.org/
https://www.linkedin.com/groups/10314172
https://www.instagram.com/gispp2019/
https://twitter.com/GisppO
https://bit.ly/2T6RhRa
GISPP
3

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

CISA Certification

- CISA certification benefits include:

Gives you a competitive edge	Helps you achieve a high professional standard	Confirms and demonstrates your knowledge and experience
Quantifies and markets your experience	Provides global recognition as a mark of excellence	Increases your value to your organization

CISA Accreditation

- The American National Standards Institute (ANSI) has accredited CISA under ISO/IEC 17024:2012, General Requirements for Bodies Operating Certification Schemes for Persons.
- Accreditation by ANSI achieves the following:
  - Promotes the unique qualifications and expertise ISACA's certifications provide
  - Protects the integrity of the certifications and provides legal defensibility
  - Enhances consumer and public confidence in the certifications and the people who hold them
  - Facilitates mobility across borders or industries
- More than 118,000 professionals have earned the CISA certification since it was introduced in 1978.

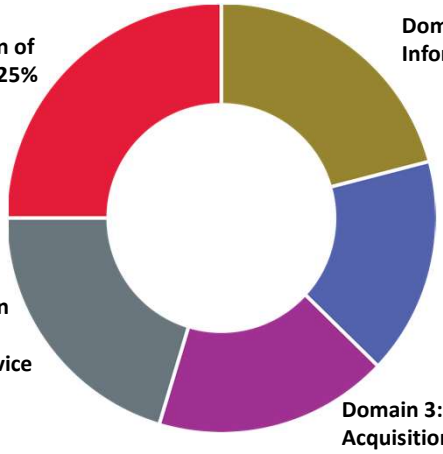
The CISA Exam

- The CISA exam is offered three times a year, in June, September and December.
- Exam registration dates:
  - Registration opens approximately eight months prior to exam date.
  - Early registration ends approximately five months prior to exam date.
  - Registration closes approximately eight weeks prior to exam date.
- Register at www.isaca.org.

About the CISA Exam

- The CISA Certification Working Group oversees the development of the CISA exam, ensuring that the job practice is properly tested.
- The exam consists of 150 multiple-choice questions covering the CISA job practice domains.

CISA Domains & Weightage



Domain 1: The Process of Auditing Information Systems, 21%

Domain 2: Governance and Management of IT, 16%

Domain 3: Information Systems Acquisition, Development and Implementation, 18%

Domain 4: Information Systems Operations, Maintenance and Service Management, 20%

Domain 5: Protection of Information Assets, 25%

Pre-Course Question 1

Which of the following is the MOST important skill an IS auditor should develop to understand the constraints of conducting an audit?

- **A. Contingency planning**
- **B. IS management resource allocation**
- **C. Project management**
- **D. Knowledge of internal controls**

C is the correct answer.

Justification:

A. Contingency planning is often associated with the organization's operations. IS auditors should have knowledge of contingency planning techniques, but this is not essential regarding constraints on the conduct of the audit.

B. IS managers are responsible for resource management of their departments. IS auditors do not manage IS resources.

C. Audits often involve resource management, deliverables, scheduling and deadlines similar to project management best practices.

D. Knowledge of internal controls is fundamental to IS auditors. Professional competence is an auditing standard. A lack of understanding of the control environment would be a constraint on the effectiveness of the audit, but is not the most important skill needed by the IS auditor.

Pre-Course Question 2

The CSIRT of an organization disseminates detailed descriptions of recent threats. An IS auditor's **GREATEST** concern should be that the users may:

A. use this information to launch attacks.
B. forward the security alert.
C. implement individual solutions.
D. fail to understand the threat.

A is the correct answer.

Justification:

A. An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risk arising from security failures and to prevent additional security incidents resulting from the same threat.

B. Forwarding the security alert is not harmful to the organization.
C. Implementing individual solutions is unlikely and inefficient, but not a serious risk.
D. Users failing to understand the threat would not be a serious concern.

Pre-Course Question 3

An IS auditor is evaluating a virtual machine–based (VM-based) architecture used for all programming and testing environments. The production architecture is a three-tier physical architecture. What is the MOST important IT control to test to ensure availability and confidentiality of the web application in production?

A. Server configuration has been hardened appropriately.

B. Allocated physical resources are available.

C. System administrators are trained to use the virtual machine (VM) architecture.

D. The VM server is included in the disaster recovery plan (DRP).

A is the correct answer.

Justification:

A. The most important control to test in this configuration is the server configuration hardening. It is important to patch known vulnerabilities and to disable all non-required functions before production, especially when production architecture is different from development and testing architecture.

B. The greatest risk is associated with the difference between the testing and production environments. Ensuring that physical resources are available is a relatively low risk and easily addressed.

C. Virtual machines (VMs) are often used for optimizing programming and testing infrastructure. In this scenario, the development environment (VM architecture) is different from the production infrastructure (physical three-tier). Because the VMs are not related to the web application in production, there is no real requirement for the system administrators to be familiar with a virtual environment.

D. Because the VMs are only used in a development environment and not in production, it may not be necessary to include VMs in the disaster recovery plan (DRP).

Pre-Course Question 4

A database administrator has detected a performance problem with some tables, which could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.

B. deadlocks.

C. unauthorized access to data.

D. a loss of data integrity.

D is the correct answer.

Justification:

A. Denormalization will have no effect on concurrent access to data in a database; concurrent access is resolved through locking.

B. Deadlocks are a result of locking of records. This is not related to normalization.

C. Access to data is controlled by defining user rights to information and is not affected by denormalization.

D. Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity.

Pre-Course Question 5

Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an electronic funds transfer (EFT) system?

A. Three users with the ability to capture and verify their own messages

B. Five users with the ability to capture and send their own messages

C. Five users with the ability to verify other users and to send their own messages

D. Three users with the ability to capture and verify the messages of other users and to send their own messages

A is the correct answer.

Justification:

A. The ability of one individual to capture and verify their own messages represents an inadequate segregation because messages can be taken as correct and as if they had already been verified. The verification of messages should not be allowed by the person who sent the message.

B. Users may have the ability to send messages but should not be able to verify their own messages.

C. This is an example of separation of duties. A person can send their own message but only verify the messages of other users.

D. The ability to capture and verify the messages of others but only send their own messages is acceptable.

Domain-1

The Process of Auditing Information Systems

Objective:

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

Domain-1

Focus:

The focus of Domain 1 is to encompass the entire practice of IS auditing, including a set of procedures and a thorough methodology that allows an IS auditor to perform an audit on any given IT area in a professional manner.

Domain-1

On the CISA Exam:

- **Domain 1 represents 21% of the questions on the CISA exam (approximately 32 questions).**
- **Domain 1 incorporates five tasks related to the process of auditing information systems.**

Domain-2

The Governance and Management of IT

Objective:

The objective of this domain is to ensure that the CISA candidate is prepared for the role of completing a review in the following areas to ensure that IT governance requirements are met:

- **Organizational structure**
- **Management policies**
- **Accountability mechanisms**
- **Monitoring practices**

Domain-2

Focus:

The focus of Domain 2 is the knowledge of IT governance, which is fundamental to the work of the IS auditor and for the development of sound control practices and mechanisms for management oversight and review.

Domain-2

On the CISA Exam:

- **Domain 2 represents 16% of the questions on the CISA exam (approximately 24 questions).**
- **Domain 2 incorporates 10 tasks related to the management of IT governance.**

Domain-3

Information Systems Acquisition, Development and Implementation

Objective:

- **The objective of this domain is to ensure that the CISA candidate understands and can provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the organization's strategies and objectives.**
- **The CISA candidate must understand how an organization evaluates, develops, implements, maintains and disposes of its IT systems and related components.**

Domain-3

Focus:

The focus of Domain 3 is to provide an overview of key processes and methodologies used by organizations when creating and changing application systems and infrastructure components.

Domain-3

On the CISA Exam:

- **Domain 3 represents 18% of the questions on the CISA exam (approximately 27 questions).**
- **Domain 3 incorporates seven tasks related to information systems acquisition, development and implementation.**

Domain-4

Information Systems Operations, Maintenance and Service Management

Objective:

- The objective of this domain is to ensure that the CISA candidate possesses a sound understanding of key service delivery elements, such as:
  - Service management frameworks
  - Service level agreements
  - Incident handling
  - Network administration and control
  - Data quality and data life cycle management
  - Planning for service delivery interruptions

Domain-4

Focus:

The focus of Domain 4 is on providing assurance that IT service level expectations are derived from the business objectives of the enterprise.

Domain-4

On the CISA Exam:

- **Domain 4 represents 20% of the questions on the CISA exam (approximately 30 questions).**
- **Domain 4 incorporates 10 tasks related to information systems operations, maintenance and service management.**

Domain-5

Protection of Information Assets

Objective:

- The objective of this domain is to ensure that the CISA candidate understands the following:
  - Elements of information security management
  - Logical entry points into a system
  - Identification and authentication practices
  - Network infrastructure security
  - Importance of OS and software maintenance
  - Environmental exposures
  - Risks from mobile devices, social media and cloud computing

Domain-5

Focus:

- **The focus of Domain 5 is the need for protecting information assets through the evaluation of design, implementation and monitoring of controls.**

Domain-5

On the CISA Exam:

- **Domain 5 represents 25% of the questions on the CISA exam (approximately 38 questions).**
- **Domain 5 incorporates six tasks related to the protection of information assets.**

Pre-Course Question 6

The success of control self-assessment (CSA) depends highly on:

A. having line managers assume a portion of the responsibility for control monitoring.
B. assigning staff managers the responsibility for building, but not monitoring, controls.
C. the implementation of a stringent control policy and rule-driven controls.
D. the implementation of supervision and the monitoring of controls of assigned duties.

A is the correct answer.

Justification:

A. The primary objective of a control self-assessment (CSA) program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a CSA program depends on the degree to which line managers assume responsibility for controls. This enables line managers to detect and respond to control errors promptly.

B. CSA requires managers to participate in the monitoring of controls.
C. The implementation of stringent controls will not ensure that the controls are working correctly.
D. Better supervision is a compensating and detective control and may assist in ensuring control effectiveness, but would work best when used in a formal process such as CSA.

Pre-Course Question 7

When evaluating the controls of an electronic data interchange (EDI) application, an IS auditor should **PRIMARILY** be concerned with the risk of:

A. excessive transaction turnaround time.
B. application interface failure.
C. improper transaction authorization.
D. nonvalidated batch totals.

C is the correct answer.

Justification:

A. An excessive turnaround time is an inconvenience, but not a serious risk.
B. The failure of the application interface is a risk, but not the most serious issue. Usually such a problem is temporary and easily fixed.
C. Foremost among the risk associated with electronic data interchange (EDI) is improper transaction authorization. Because the interaction with the parties is electronic, there is no inherent authentication. Improper authentication would pose a serious risk of financial loss.
D. The integrity of EDI transactions is important, but not as significant as the risk of unauthorized transactions.

Pre-Course Question 8

An IS auditor reviewing a series of completed projects finds that the implemented functionality often exceeded requirements and most of the projects ran significantly over budget. Which of these areas of the organization's project management process is the **MOST** likely cause of this issue?

A. Project scope management
B. Project time management
C. Project risk management
D. Project procurement management

A is the correct answer.

Justification:

A. Because the implemented functionality is greater than what was required, the most likely cause of the budget issue is failure to effectively manage project scope. Project scope management is defined as the processes required to ensure that the project includes all of the required work, and only the required work, to complete the project.

B. Project time management is defined as the processes required to ensure timely completion of the project. The issue noted in the question does not mention whether projects were completed on time, so this is not the most likely cause.

C. Project risk management is defined as the processes concerned with identifying, analyzing and responding to project risk. Although the budget overruns mentioned above represent one form of project risk, they appear to be caused by implementing too much functionality, which relates more directly to project scope.

D. Project procurement management is defined as the processes required to acquire goods and services from outside the performing organization. Although purchasing goods and services that are too expensive can cause budget overruns,

in this case the key to the question is that implemented functionality is greater than what was required, which is more likely related to project scope.

Pre-Course Question 9

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's **MAIN** concern should be that the:

A. complexity and risk associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. technical deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

A is the correct answer.

Justification:

A. Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome.
B. The resources needed will be dependent on the complexity of the project.
C. It is too early to identify the technical deliverables.
D. Not all projects will require contracts with external parties.

Pre-Course Question 10

The **PRIMARY** objective of service-level management (SLM) is to:

A. define, agree on, record and manage the required levels of service.
B. ensure that services are managed to deliver the highest achievable level of availability.
C. keep the costs associated with any service at a minimum.
D. monitor and report any legal noncompliance to business management.

A is the correct answer.

Justification:

A. The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services.

B. SLM does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb.

C. SLM cannot ensure that costs for all services will be kept at a low or minimum level because costs associated with a service will directly reflect the customer's requirements.

D. Monitoring and reporting legal noncompliance is not a primary objective of SLM.

GISSP

THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman