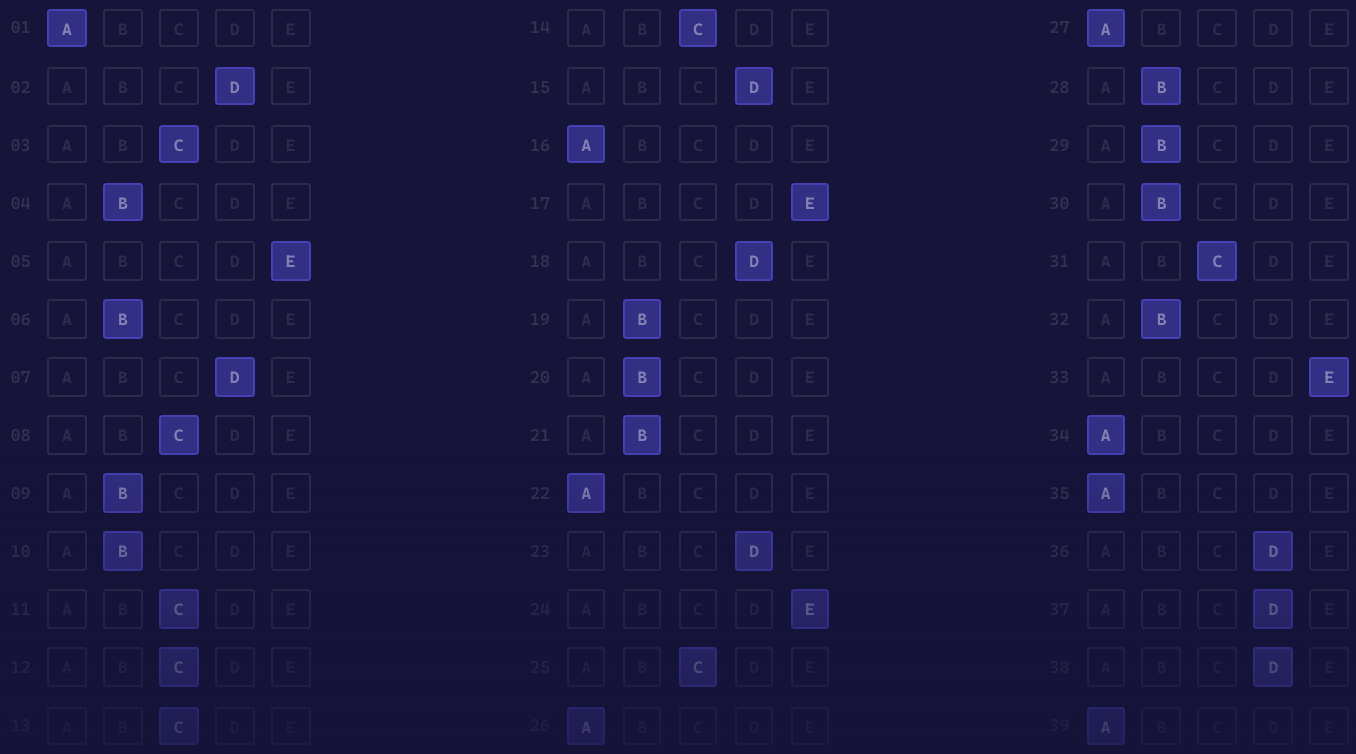
MOMETRIX
SMARTER PREP. BETTER RESULTS.



PRACTICE QUESTIONS

CPA

ISCGU

Information Systems and Controls (Guam)

EDITION	QUESTIONS	FORMAT
Demo	9	Limited Edition PDF

WEB www.mometrix.net

SUPPORT support@mometrix.net

Before you begin

What this is

9 practice questions for CPA `ISCGU`, each with its answer key and an explanation. Answer a question before you read its key — the explanation is worth more once you have committed.

If something looks wrong

Send us three things and we will check it:

- the exam code, `ISCGU`
- the question number
- the email address on your order

Write to **support@mometrix.net**. We reply within one business day.

QUESTION 1 SINGLE CHOICE

Which of the following best describes the primary purpose of a general control in an information systems environment?

A It ensures that specific application transactions are processed accurately.

B It supports the overall operation and security of the information systems infrastructure.

C It focuses solely on detecting fraudulent financial transactions.

D It applies only to end-user computing activities.

ANSWER B

WHY General controls (also called IT general controls) support the overall operation and security of the information systems environment, including areas such as access security, change management, and IT operations. They differ from application controls, which relate to the processing of specific transactions.

QUESTION 2 SINGLE CHOICE

An organization is evaluating the risks associated with a new cloud-based application. Which of the following is the MOST appropriate first step in the risk assessment process?

A Identify and document the threats and vulnerabilities associated with the application.

B Implement compensating controls to mitigate identified risks.

C Purchase cyber insurance to transfer residual risk.

D Perform penetration testing on the production environment.

ANSWER A

WHY The risk assessment process begins with identifying and documenting the threats and vulnerabilities that could affect the system. Controls, insurance, and testing follow only after risks have been identified and analyzed.

QUESTION 3 SINGLE CHOICE

Which IT operational control is designed to ensure that data can be restored after an unexpected disruption or disaster?

A Change management

B Backup and recovery

C Input validation

D User access reviews

ANSWER B

WHY Backup and recovery controls ensure that critical data can be restored following an unexpected event such as hardware failure, accidental deletion, or a disaster. Change management controls unauthorized modifications, input validation prevents invalid data entry, and access reviews ensure appropriate user privileges.

QUESTION 4 SINGLE CHOICE

A company wants to ensure that employees are only granted the minimum system privileges necessary to perform their job duties. Which security principle does this represent?

A Defense in depth

B Least privilege

C Segregation of duties

D Need to know

ANSWER B

WHY Least privilege is the principle that users should be granted only the minimum access necessary to perform their job duties. Defense in depth involves layering multiple controls, segregation of duties divides responsibilities to reduce fraud risk, and need to know restricts access to specific information.

QUESTION 5 SINGLE CHOICE

During the system development life cycle (SDLC), at which phase are application controls typically FIRST designed and incorporated into the system?

A Post-implementation review

B Operations and maintenance

C Design and development

D Testing and conversion

ANSWER C

WHY Application controls should be designed and incorporated during the design and development phase of the SDLC. Incorporating controls after development is significantly more costly and less effective than building them into the system from the beginning.

QUESTION 6 SINGLE CHOICE

Which of the following is the PRIMARY reason an organization requires formal approval before migrating a system to a new platform?

A To reduce the number of help desk tickets after deployment

B To ensure the change is authorized, tested, and aligned with business objectives

C To eliminate the need for post-implementation testing

D To allow end users to bypass standard procedures

ANSWER B

WHY Formal change management approval ensures that changes are authorized, tested, and aligned with business objectives before implementation. This reduces the risk of unauthorized or faulty changes disrupting production systems.

QUESTION 7 SINGLE CHOICE

Which type of disaster recovery site allows an organization to resume operations most quickly following a disaster but is typically the most expensive option?

A Cold site

B Warm site

C Hot site

D Reciprocal site

ANSWER C

WHY A hot site is fully equipped and operational, allowing an organization to resume operations within hours. Because it requires continuous maintenance of hardware, software, and connectivity, it is the most expensive option. Cold sites require the longest recovery time, while warm sites fall between the two.

QUESTION 8 SINGLE CHOICE

Which of the following is an example of a detective control within an information system?

A A password policy requiring complex passwords

B An approval workflow before a financial transaction is posted

C A log review that identifies unauthorized system access attempts

D Encryption of sensitive data at rest

ANSWER C

WHY Detective controls identify and report when a policy violation or undesirable event has occurred. Log reviews detect unauthorized activity after the fact. Password policies and approvals are preventive controls, and encryption is primarily a preventive control protecting confidentiality.

QUESTION 9 MULTIPLE CHOICE

Which of the following are common characteristics of effective information security policies? (Choose two.)

A **They are reviewed and updated on a periodic basis.**

B **They are communicated to all relevant personnel.**

C They are developed exclusively by the IT department without input from management.

D They require no enforcement to remain effective.

E They address only physical security topics.

ANSWER **A** · **B**

WHY Effective information security policies must be reviewed and updated periodically to remain relevant, and they must be communicated to all relevant personnel so that users understand their responsibilities. Policies require executive involvement and management support, must be enforceable, and typically address logical, physical, and administrative security topics.