Certified in the Governance of Enterprise IT®
An ISACA® Certification

The following correction applies to page 66 of the *CGEIT® Review Questions, Answers & Explanations Manual 2015.* Justification D has been corrected.

G4-20 The responsibility for risk acceptance lies with:

A. the enterprise risk committee.
B. executive management.
C. the business process owner.
D. the audit committee.

B is the correct answer.

Justification:
A. The enterprise risk committee oversees risk governance, but the responsibility for accepting risk remains with executive management.
B. Risk acceptance is the responsibility of executive management or their designated representative.
C. The business process owner generally escalates risk acceptance requests to executive management for approval.
D. The audit committee identifies risk, but defers risk acceptance to executive management.

G4-21 Who of the following is **ULTIMATELY** responsible for monitoring the risk management process?

A. Chief information officer (CIO)
B. Chief information security officer (CISO)
C. Chief financial officer (CFO)
D. Chief executive officer (CEO)

D is the correct answer.

Justification:
A. The chief information officer (CIO) may be delegated this responsibility, but does not have the ultimate responsibility.
B. The chief information security officer (CISO) may be delegated this responsibility, but does not have the ultimate responsibility.
C. The chief financial officer (CFO) may be delegated this responsibility, but does not have the ultimate responsibility.
D. The overall responsibility of monitoring risk management rests with the chief executive officer (CEO).

G4-22 When outsourcing credit card processing, who is accountable for the compliance with regulatory requirements?

A. The outsourcing vendor is accountable.
B. Accountability is shared.
C. The client enterprise is accountable.
D. Accountability depends on the contract.

C is the correct answer.

Justification:
A. The outsourcing vendor performs the activities and delivers the services as contracted, but is not ultimately accountable.
B. The client enterprise and the outsourcing vendor cannot share the accountability because the outsourcing vendor provides the services, but is only accountable for the services rendered and not for the compliance with regulatory requirements.
C. The client enterprise remains accountable for the services delivered. The contract or procurement document does not relieve the client from this accountability.
D. The contract cannot relieve the client of its inherent responsibilities.