Certified in Risk and Information Systems Control™
An ISACA® Certification

The following correction applies to page 19 of the *CRISC® Review Questions, Answers & Explanations Manual 5th Edition*. The correction is boxed.

R1-42 It is **MOST** important that risk appetite be aligned with business objectives to ensure that:

A. resources are directed toward areas of low risk tolerance.
B. major risk is identified and eliminated.
C. IT and business goals are aligned.
D. the risk strategy is adequately communicated.

A is the correct answer.

Justification:
A. Risk appetite refers to the amount of risk that an enterprise is willing to take on in pursuit of value. Aligning it with business objectives allows an enterprise to evaluate and deploy valuable resources toward those objectives where risk tolerance (for loss) is low.
B. There is no link between aligning risk appetite with business objectives and identification and elimination of major risk. Moreover, risk cannot be eliminated; it can be reduced to an acceptable level using various risk response options.
C. Alignment of risk appetite with business objectives does conform IT and business goals to a point, but alignment is not limited to these two areas. Other areas include organizational, strategic and financial objectives, among other objectives.
D. Communication of the risk strategy does not depend on aligning risk appetite with business objectives.

R1-43 Risk scenarios enable the risk assessment process because they:

A. cover a wide range of potential risk.
B. minimize the need for quantitative risk analysis techniques.
C. segregate IT risk from business risk for easier risk analysis.
D. help estimate the frequency and impact of risk.

D is the correct answer.

Justification:
A. When done correctly, risk scenarios can address a wide range of risk, but this is not always the case. However, risk scenarios always help to address the frequency and impact of risk—two key elements to the risk assessment process.
B. Risk scenarios do not necessarily minimize the need for quantitative risk analysis.
C. Risk scenarios can be applied to both IT risk and business risk and there is no question of segregating the risk.
D. While risk scenarios may address a wide range of risk, risk scenarios help to estimate the frequency and impact of risk—two key elements of the risk assessment process. These elements aid subsequent steps in risk management by making risk relevant to business process owners.

R1-44 Who is accountable for business risk related to IT?

A. The chief information officer
B. The chief financial officer
C. Users of IT services
D. The chief architect

C is the correct answer.

Justification:
A. The chief information officer supports the business, but does not own the business risk.
B. The chief financial officer tracks the cost of resources and financial risk, but does not own the business risk.
C. Ultimately, the business (i.e., the users of IT services) owns business-related risk, including the risk related to the use of IT. The business should set the mandate for risk management, provide the resources and funding to support a risk management plan designed to protect business interests, and monitor whether risk is being managed.
D. The chief architect mitigates IT risk through the architecture of the IT environment, but does not own the business risk.

ISACA®
Trust in, and value from, information systems