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

The following correction applies to page 65 of the *CRISC™ Review Questions, Answers & Explanations Manual 2015*. Choices A and B have been reversed to align with the justifications.

R2-48 The goal of IT risk analysis is to:

A. enable the alignment of IT risk management with enterprise risk management (ERM).
B. enable the prioritization of risk responses.
C. satisfy legal and regulatory compliance requirements.
D. identify known threats and vulnerabilities to information assets.

B is the correct answer.

Justification:
A. Aligning IT risk management with enterprise risk management (ERM) is important to ensure the cost-effectiveness of the overall risk management process. However, risk analysis does not enable such an alignment.
B. Risk analysis is a process by which likelihood and magnitude of IT risk scenarios are estimated. Risk analysis is conducted to ensure that areas with greatest risk likelihood and impact are prioritized above those areas with lower likelihood and impact. Prioritization of IT risk helps maximize return on investment (ROI) on risk responses.
C. Risk analysis evaluates risk on the basis of likelihood and impact and includes financial, environmental, regulatory and other risk. It does look at regulatory risk as one of many types of risk that the enterprise faces, and is not specifically designed to satisfy legal and regulatory compliance requirements.
D. Risk analysis occurs after risk identification and evaluation. Risk identification does identify known threats and vulnerabilities. Risk evaluation assesses the risk and creates valid risk scenarios. Risk analysis quantifies risk along the vectors of likelihood and impact to facilitate the prioritization of risk responses.

R2-49 Which of the following factors should be assessed after the likelihood of a loss event has been determined?

A. Risk tolerance
B. Magnitude of impact
C. Residual risk
D. Compensating controls

B is the correct answer.

Justification:
A. Risk tolerance is the acceptable deviation from acceptable risk. This is taken into account once risk has been quantified, which is dependent on determining the magnitude of impact.
B. Once likelihood has been determined, the next step is to determine the magnitude of impact.
C. Residual risk is the remaining risk after management has implemented a risk response. This cannot be calculated until the controls have been selected.
D. Compensating controls are internal controls that reduce the risk of an existing or potential control weakness resulting in errors and omissions. They would not be assessed directly in conjunction with assessing the likelihood of a loss event.