The following corrections apply to page 84 of the *CRISC® Review Questions, Answers & Explanations Manual 4th Edition*. The corrections are circled.

R2-59 Which automated monitoring technique in an application uses triggers to indicate a suspicious condition?

A. Snapshots
B. An integrated test facility
C. Audit hooks
D. Continuous and intermittent simulation

C is the correct answer.

Justification:
A. The snapshots technique takes a picture of a system status to identify specific values or configuration settings.
B. An integrated test facility feeds dummy transactions into the production flow and compares them to predetermined results.
C. The audit hooks technique has embedded hooks in the application that act as triggers if certain conditions are met.
D. In continuous and intermittent simulation, data are monitored only if they meet certain criteria.

R2-60 Which of the following is the **BEST** reason to perform a risk assessment?

A. To satisfy regulatory requirements
B. To budget appropriately for needed controls
C. To analyze the effect on the business
D. To help determine the current state of risk

D is the correct answer.

Justification:
A. Performing a risk assessment may satisfy regulatory requirements but is not the reason to perform a risk assessment.
B. Budgeting appropriately may come as a result but is not the reason to perform a risk assessment.
C. Analyzing the effect on the business is part of the process, but the needs or acceptable effect or response must also be determined.
D. The risk assessment is used to identify and evaluate the impact of failure on critical business processes (and IT components supporting them) and to determine time frames, priorities, resources and interdependencies. It is part of the process to help determine the current state of risk and helps determine risk countermeasures in alignment with business objectives.

The following corrections apply to page 235 of the *CRISC® Review Questions, Answers & Explanations Manual 4th Edition*. The corrections are circled.

29. Which of the following categories of information security controls addresses a deficiency or weakness in the control structure of an enterprise?

A. Corrective
B. Preventive
C. Compensating
D. Directive

30. At the end of which phase of risk management would information about newly discovered risk be communicated to decision makers and relevant stakeholders?

A. Risk identification
B. Risk response and mitigation
C. Risk assessment
D. Risk and control monitoring and reporting

31. Which of the following is **MOST** useful when computing annual loss exposure?

A. The cost of existing controls
B. The number of vulnerabilities
C. The net present value (NPV) of the asset
D. The business value of the asset

32. Which of the following measures is **MOST** effective against insider threats to confidential information?

A. Audit trail monitoring
B. A privacy policy
C. Role-based access control (RBAC)
D. Defense in depth

33. In which phase of the system development life cycle (SDLC) should a risk practitioner **FIRST** become involved?

A. Analysis
B. Design
C. Planning
D. Implementation

34. Minimizing single points of failure of a widespread natural disaster can be controlled by:

A. implementing redundant systems and applications onsite.
B. using fireproof vaults to retain onsite backup data.
C. preparing business continuity and disaster recovery planning documents for identified disasters.
D. allocating resources geographically.

35. Which automated monitoring technique in an application uses triggers to indicate a suspicious condition?

A. Snapshots
B. An integrated test facility
C. Audit hooks
D. Continuous and intermittent simulation