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

The following correction applies to page 235 of the *CRISC® Review Questions, Answers & Explanations Manual 4th Edition*. Choice C for question 35 has been corrected.

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