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

The following correction applies to page 54 of the *CRISC™ Review Questions, Answers & Explanations Manual 2015*. Justification C has been bolded to indicate that C is the correct answer.

R2-26 When assessing the performance of a critical application server, the **MOST** reliable assessment results may be obtained from:

A. activation of native database auditing.
B. documentation of performance objectives.
C. continuous monitoring.
D. documentation of security modules.

C is the correct answer.

Justification:
A. Native database audit logs are a good detective control, but do not provide information about the application server performance.
B. Documentation of performance objectives is important, but does not provide information about the application server performance.
C. It is essential to obtain monitoring data in a consistent manner to achieve reliable results. Changing the monitoring methodology frequently does not enable time-series data comparison.
D. Documentation of associated security modules may be helpful, but does not provide information about the application server performance.

R2-27 The **PRIMARY** goal of a postincident review is to:

A. gather evidence for subsequent legal action.
B. identify ways to improve the response process.
C. identify individuals who failed to take appropriate action.
D. make a determination as to the identity of the attacker.

B is the correct answer.

Justification:
A. Evidence should already have been gathered earlier in the process.
B. The goal of a postincident review is to identify ways to improve the incident response process.
C. A postincident review should not focus on finding and punishing individuals who did not take appropriate action, but rather on establishing a process to reduce the likelihood of similar incidents in the future and to improve the incident response process.
D. Identification of the attacker is not an objective of the postincident review process.