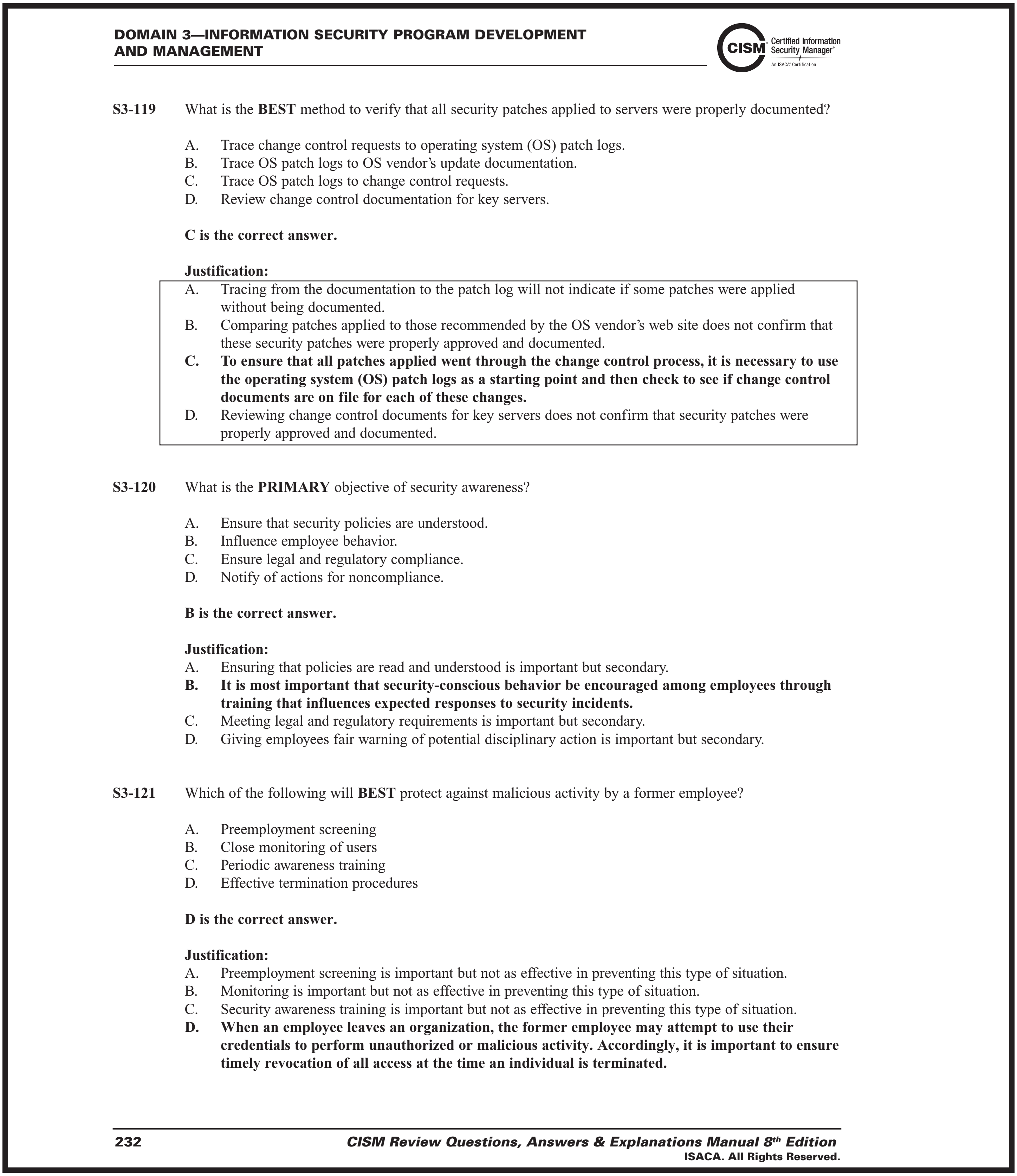
The following correction applies to page 232 of the *CISM® Review Questions, Answers & Explanations Manual 8th Edition*. The justifications have been corrected.



S3-119 What is the **BEST** method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to operating system (OS) patch logs.
B. Trace OS patch logs to OS vendor's update documentation.
C. Trace OS patch logs to change control requests.
D. Review change control documentation for key servers.

C is the correct answer.

Justification:

A. Tracing from the documentation to the patch log will not indicate if some patches were applied without being documented.
B. Comparing patches applied to those recommended by the OS vendor's web site does not confirm that these security patches were properly approved and documented.
C. To ensure that all patches applied went through the change control process, it is necessary to use the operating system (OS) patch logs as a starting point and then check to see if change control documents are on file for each of these changes.
D. Reviewing change control documents for key servers does not confirm that security patches were properly approved and documented.

S3-120 What is the **PRIMARY** objective of security awareness?

A. Ensure that security policies are understood.
B. Influence employee behavior.
C. Ensure legal and regulatory compliance.
D. Notify of actions for noncompliance.

B is the correct answer.

Justification:

A. Ensuring that policies are read and understood is important but secondary.
B. It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents.
C. Meeting legal and regulatory requirements is important but secondary.
D. Giving employees fair warning of potential disciplinary action is important but secondary.

S3-121 Which of the following will **BEST** protect against malicious activity by a former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

D is the correct answer.

Justification:

A. Preemployment screening is important but not as effective in preventing this type of situation.
B. Monitoring is important but not as effective in preventing this type of situation.
C. Security awareness training is important but not as effective in preventing this type of situation.
D. When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated.

Trust in, and value from, information systems