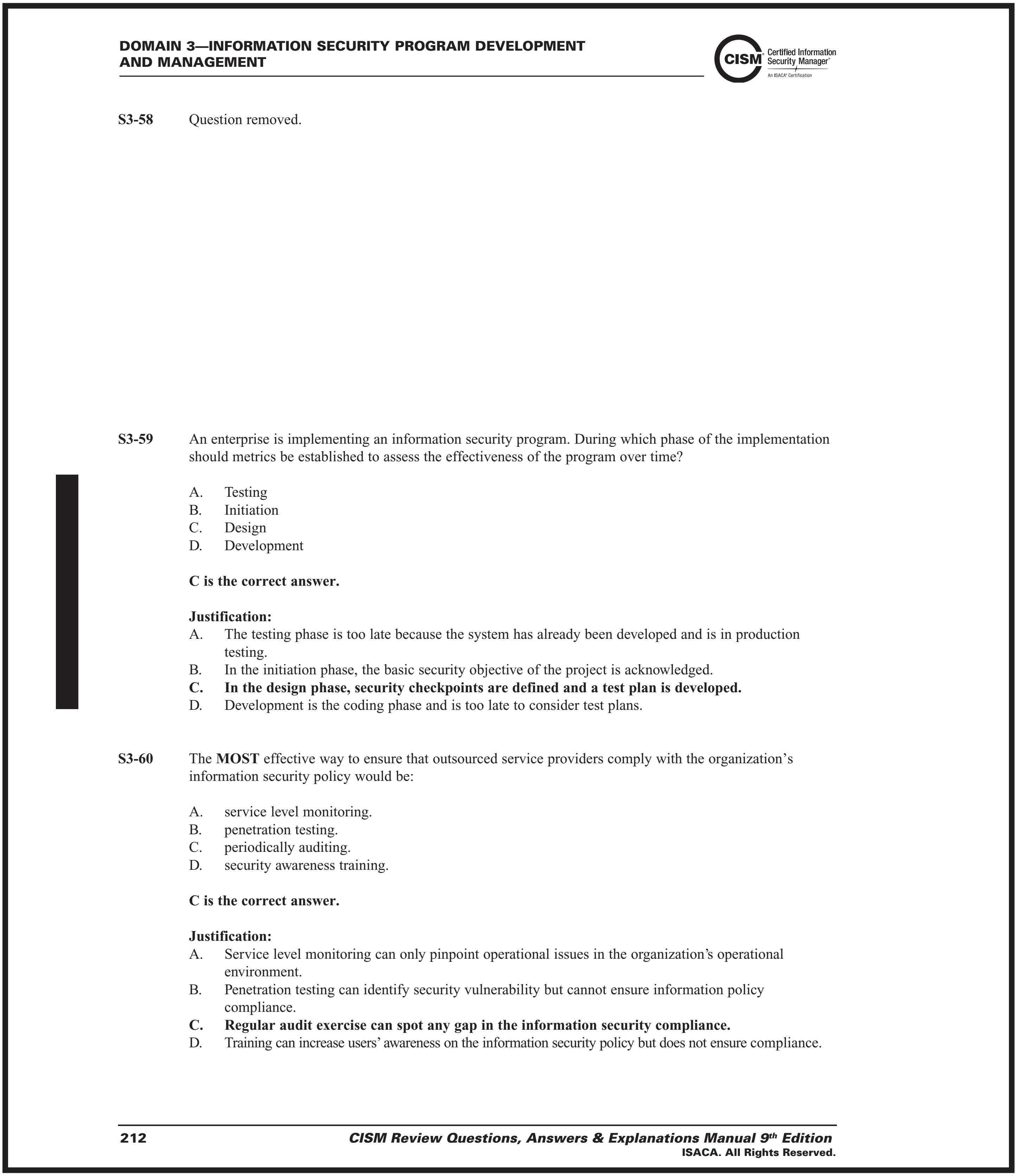
The following correction applies to page 212 of the *CISM® Review Questions, Answers & Explanations Manual 9th Edition*. Question S3-58 has been removed.



S3-58 Question removed.

S3-59 An enterprise is implementing an information security program. During which phase of the implementation should metrics be established to assess the effectiveness of the program over time?

A. Testing
B. Initiation
C. Design
D. Development

C is the correct answer.

Justification:
A. The testing phase is too late because the system has already been developed and is in production testing.
B. In the initiation phase, the basic security objective of the project is acknowledged.
C. In the design phase, security checkpoints are defined and a test plan is developed.
D. Development is the coding phase and is too late to consider test plans.

S3-60 The **MOST** effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

A. service level monitoring.
B. penetration testing.
C. periodically auditing.
D. security awareness training.

C is the correct answer.

Justification:
A. Service level monitoring can only pinpoint operational issues in the organization's operational environment.
B. Penetration testing can identify security vulnerability but cannot ensure information policy compliance.
C. Regular audit exercise can spot any gap in the information security compliance.
D. Training can increase users' awareness on the information security policy but does not ensure compliance.