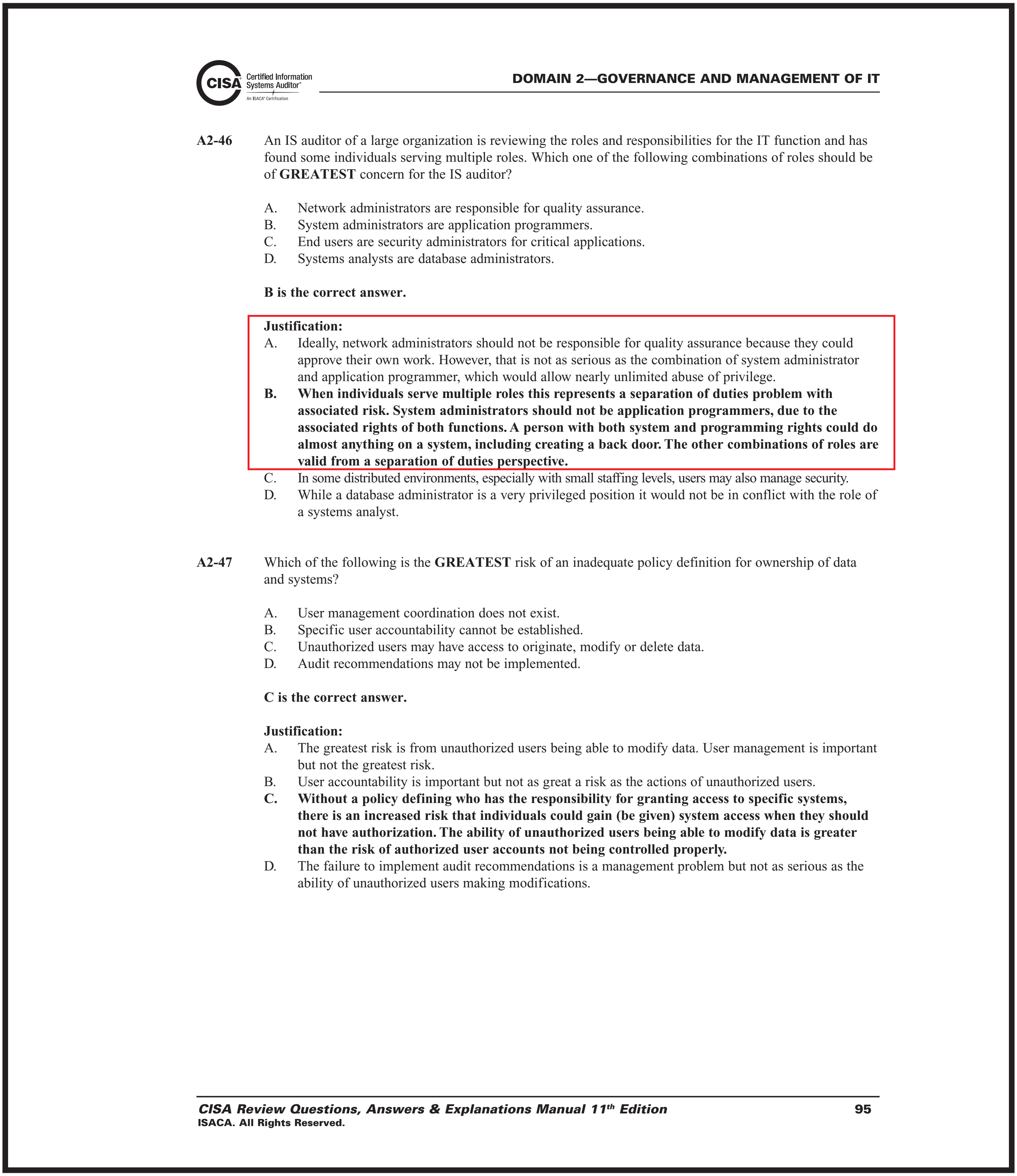
The following correction applies to page 95 of the *CISA Review Questions, Answers & Explanations Manual 11th Edition*. Justifications A and B for question A2-46 have been corrected.



A2-46 An IS auditor of a large organization is reviewing the roles and responsibilities for the IT function and has found some individuals serving multiple roles. Which one of the following combinations of roles should be of **GREATEST** concern for the IS auditor?

A. Network administrators are responsible for quality assurance.
B. System administrators are application programmers.
C. End users are security administrators for critical applications.
D. Systems analysts are database administrators.

B is the correct answer.

Justification:
A. Ideally, network administrators should not be responsible for quality assurance because they could approve their own work. However, that is not as serious as the combination of system administrator and application programmer, which would allow nearly unlimited abuse of privilege.
B. When individuals serve multiple roles this represents a separation of duties problem with associated risk. System administrators should not be application programmers, due to the associated rights of both functions. A person with both system and programming rights could do almost anything on a system, including creating a back door. The other combinations of roles are valid from a separation of duties perspective.
C. In some distributed environments, especially with small staffing levels, users may also manage security.
D. While a database administrator is a very privileged position it would not be in conflict with the role of a systems analyst.

A2-47 Which of the following is the **GREATEST** risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.
B. Specific user accountability cannot be established.
C. Unauthorized users may have access to originate, modify or delete data.
D. Audit recommendations may not be implemented.

C is the correct answer.

Justification:
A. The greatest risk is from unauthorized users being able to modify data. User management is important but not the greatest risk.
B. User accountability is important but not as great a risk as the actions of unauthorized users.
C. Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that individuals could gain (be given) system access when they should not have authorization. The ability of unauthorized users being able to modify data is greater than the risk of authorized user accounts not being controlled properly.
D. The failure to implement audit recommendations is a management problem but not as serious as the ability of unauthorized users making modifications.

ISACA. All Rights Reserved.