CISSP®:
Certified Information Systems Security Professional
Study Guide
3rd Edition

James Michael Stewart
Ed Tittel
Mike Chapple

San Francisco • London

SYBEX®

Contents

27. B. Layers 1 and 2 contain device drivers but are not normally implemented in practice. Layer 0 always contains the security kernel. Layer 3 contains user applications. Layer 4 does not exist. For more information, please see Chapter 7.

28. C. Transposition ciphers use an encryption algorithm to rearrange the letters of the plaintext message to form a ciphertext message. For more information, please see Chapter 9.

29. C. The annualized loss expectancy (ALE) is computed as the product of the asset value (AV) times the annualized rate of occurrence (ARO). The other formulas displayed here do not accurately reflect this calculation. For more information, please see Chapter 15.

30. C. The principle of integrity states that objects retain their veracity and are only intentionally modified by authorized subjects. For more information, please see Chapter 5.

31. D. E-mail is the most common delivery mechanism for viruses, worms, Trojan horses, documents with destructive macros, and other malicious code. For more information, please see Chapter 4.

32. A. Technical security controls include access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression. For more information, please see Chapter 19.

33. A. Administrative determinations of federal agencies are published as the Code of Federal Regulations. For more information, please see Chapter 17.

34. A. Identification of priorities is the first step of the Business Impact Assessment process. For more information, please see Chapter 15.

35. C. Any recipient can use Mike's public key to verify the authenticity of the digital signature. For more information, please see Chapter 10.

36. C. A Type 3 authentication factor is something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, hand geometry, and so on. For more information, please see Chapter 1.

37. C. The primary goal of risk management is to reduce risk to an acceptable level. For more information, please see Chapter 6.