

30. Which of the following is NOT a specific characteristic of ISSP?

A. It addresses specific technology-based resources

B. It requires frequent updates

C. It addresses hardware implementation issues

D. It contains an issue statement

31. Which of the following is NOT an InfoSec policy recommended in NIST's Special Publication 800-14 document?

A. Enterprise information security policy (EISP)

B. Issue-specific security policies (ISSP)

C. System-specific security policies (SysSP)

D. Task-specific security policies (TSSP)

32. What is used to regulate the who, what, when, where, and how aspects of access to a system or resource?

A. Configuration rules

B. Access control lists

C. Rule-based policies

D. Security policies

33. True or False: A policy administrator is the combination of a system administrator and a CIO.

34. In which SecSDLC phase should the policy development committee determine the fundamental philosophy of the organization when it comes to policy?

A. Implementation phase

B. Design phase

C. Investigation phase

D. Analysis phase

35. What is the name of the agreement screen that prompts for user acceptance of fair and responsible use terms for a particular software package?

A. End-user license agreement

- B. End-user fair-use policy
- C. End-user terms of use agreement
- D. End-user distribution policy

36. All but which of the following occurs during the investigation phase of policy development?

- A. Attaining support from senior management
- B. Providing clear articulation of goals

C. Performing a risk assessment

- D. Creating a detailed outline of a policy's scope

37. Which of the following information security roles best describe a type of specialized security administrator, and is typically responsible for analyzing and designing security solutions in a specific domain.

- A. Security manager
- B. Chief security officer

C. Security analyst

- D. Chief information security officer

38. True or **False**: A CISO never reports to the CIO, and must always go through management hierarchies.

39. Which security role is typically an entry-level position responsible for monitoring some aspect of the organization's security posture?

A. Security technicians

- B. Security administrators
- C. Analysts
- D. Watchstanders

40. Which certification is considered to be one of the most prestigious certifications for security managers and CISOs?

A. CISA

B. CISSP

C. CND

D. CompTIA Security+

41. An organization is considered to be medium-sized when it has approximately how many devices?

A. Less than 100

B. More than 1000

C. More than 100, less than 1000

D. More than 2000

42. True or False: It is the CISO's responsibility to ensure that InfoSec functions are performed within an organization.

43. All but which of the following is certification training recommended for a student focusing on managerial information security?

A. Certified Information Systems Security Professional

B. Security+

C. Certified Information Security Manager

D. Global Information Security Officer

44. Which of the following is NOT a major benefit of SETA programs?

A. They enable the organization to hold employees accountable

B. They can inform members of the organization about where to report policy violations

C. They can improve employee behavior

D. They can improve configuration rule security

45. Which of the following represents a sequence of activities or events that take the majority of time to complete on a PERT or CPM diagram?

A. Critical order

B. Absolute path

C. Slack time

D. Critical path

46. Which of the following is considered one of the least frequently implemented but most effective security methods?

A. Security Education

B. Security Certifications

C. Security Training

D. Security Awareness

47. True or False: Only the InfoSec and IT communities have a role to play in the management of risks to information assets.

48. The evaluation and reaction to risk to the entire organization is known as which of the

following?

A. RM framework

B. RM process

C. Enterprise Risk Management (ERM)

D. risk management policy

49. Which of the following is the first stage of the RM framework?

A. Framework design

B. Framework monitoring and review

C. Continuous improvement

D. Executive governance and support

50. What name is given to the relative executives who work together with the support of the CISO in developing and enabling the RM framework and its resulting process?

A. governance group

B. RM framework team

C. risk management policy developers

D. risk tolerance team

51. Which of the following framework implementation methods is considered the boldest method?

- A. desk check
- B. pilot test
- C. phased approach

D. direct cutover

52. An evaluation of the threats to information assets?

A. threat assessment

- B. risk analysis
- C. data classification scheme
- D. risk identification

53. In some corporate models, information assets can be categorized into which of the following groups?

- A. People, planning, technology
- B. Planning, performing, tasking
- C. Preparedness, planning, and technology

D. People, process, and technology

54. Which term below defines the identification and assessment of risks for each vulnerability identified by an organization?

A. Risk determination

- B. Risk analysis
- C. Risk identification
- D. Risk management

55. The overall rating, or numerical value, of the probability that a specific vulnerability will be exploited is known as which of the following?

- A. risk
- B. risk determination

C. likelihood

- D. qualitative assessment

56. Which of the following terms best describes the state of having limited or imperfect

knowledge of a situation, making it less likely the organization can successfully anticipate future events or outcomes?

A. uncertainty

B. risk determination

C. likelihood

D. risk appetite

57. Which risk treatment strategy focuses on planning and preparation to reduce the damage caused by a realized incident or disaster?

A. Mitigation

B. Termination

C. Transference

D. Acceptance

58. True or False: An example of using the transference risk treatment strategy would be to outsource the security of an asset to another organization.

59. Which of the following is NOT one of the three types of plans included in a mitigation risk treatment strategy?

A. Incident response (IR) plan

B. Disaster recovery (DR) plan

C. Business continuity (BC) plan

D. Risk control plan (RC)

60. When is the acceptance risk treatment strategy NOT an acceptable approach?

A. The cost of protecting an asset is more than the asset is worth

B. The asset consists of employee and / or customer information

C. The asset is considered expendable

D. The asset has relatively little risk