CHAPTER 4: SECURITY MANAGEMENT

Multiple Choice:

1. An effective security policy contains all of the following information except:

A. Reference to other policies

B. Measurement expectations

C. Compliance management and measurements description

D. Glossary of terms

Answer: D **Reference:** Security Policies Set the Stage **Difficulty:** moderate

2. Which of the following is typically NOT found in corporate security policy?

A. Effective/expiration dates

B. Standards library structure

C. Authorizing individual

D. Exception process

Answer: B **Reference:** Security Policies Set the Stage **Difficulty:** moderate

3. A(n) _____ policy might prescribe the need for information security and may delegate the creation and management of the program.

A. Programme-level

B. System-specific

C. Issue-specific

D. Programme-framework

Answer: A **Reference:** Four Types of Policies **Difficulty:** moderate

4. A(n) _____ policy focuses on policy issues that management decided for a specific system.

A. Programme-level

B. System-specific

C. Issue-specific

D. Programme-framework

Answer: B **Reference:** Four Types of Policies **Difficulty:** easy

5. _____ policy speaks to specific issues of concern to the organization.

A. Programme-level

B. System-specific

C. Issue-specific

D. Programme-framework

Answer: C **Reference:** Four Types of Policies **Difficulty:** moderate

6. Programme-level policy helps management do all of the following except:

A. Establish a security programme

B. Assign programme management responsibilities

C. Depict the library standards structure

D. Establish a basis for policy compliance

Answer: C **Reference:** Programme-Level Policies **Difficulty:** moderate

7. Which of the following is not a programme-level policy component?

A. Compliance

B. Responsibilities

C. Scope

D. Rationale

Answer: D **Reference:** Programme-Level Policies **Difficulty:** moderate

8. The programme-level policy component _____ authorizes and defines the use of specific penalties and disciplinary action for those failing to comply with computer security policies.

A. Purpose

B. Scope

C. Compliance

D. Responsibilities

Answer: C **Reference:** Programme-Level Policies **Difficulty:** moderate

9. The programme-level policy component _____ specifies which resources, information, and personnel are covered.

A. Purpose

B. Scope

C. Compliance

D. Responsibilities.

Answer: B **Reference:** Programme-Level Policies **Difficulty:** moderate

10. All of the following information technology management's decisions are reflected in the programme-framework policy EXCEPT:

A. Priorities for protection

B. Resource allocation

C. Assignment of responsibilities

D. None of the above.

Answer: D **Reference:** Programme-Framework Policies **Difficulty:** moderate

11. Some organizations distribute handbooks that address the programme-framework policy, these combine:

A. Policy

B. Standards

C. Both of the above

D. None of the above

Answer: C **Reference:** Programme-Framework Policies **Difficulty:** moderate

12. The "key" policy areas of computer security include all of the following except:

A. Library security structure

B. Life-cycle management

C. Contingency planning

D. Network security

Answer: A **Reference:** Programme-Framework Policies **Difficulty:** moderate

13. Which of the following is NOT something included in a system-specific policy?

A. State the security objectives of a specific system

B. Describe the security functions of a specific system

C. Define how the system should be operated to achieve security

D. Specify how technology protections and features will be used to support the security objectives

Answer: B **Reference:** Issue-Specific Policies **Difficulty:** moderate

14. The basic components of an issue-specific policy might include all of the following except:

A. Compliance

B. Applicability

C. Standard library structure

D. Issue statement

Answer: C **Reference:** Issue-Specific Policies **Difficulty:** moderate

15. A basic component of an issue-specific policy that defines a security issue and any relevant terms, distinctions, and conditions is a(n):

A. Issue statement

B. Statement of the organization's position

C. Point of contact and supplementary information

D. Role and responsibility

Answer: A **Reference:** Issue-Specific Policies **Difficulty:** moderate

16. A basic component of an issue-specific policy that states where, how, when, to whom, and to what a particular policy applies is:

A. Issue statement

B. Role and responsibility

C. Applicability

D. Compliance

Answer: C **Reference:** Issue-Specific Policies **Difficulty:** moderate

17. Compliance defines penalties that must be consistent with organizational personnel policies and are coordinated with all of the following except appropriate:

A. Officials

B. Offices

C. Employee bargaining units

D. ISP administrators

Answer: D **Reference:** Issue-Specific Policies **Difficulty:** moderate

18. Which of the following is NOT considered an example of an issue-specific policy?

A. E-Mail acceptable use

B. Internet acceptable use

C. Read/write access to the HR database

D. Laptop acceptable use

Answer: C **Reference:** Issue-Specific Policies **Difficulty:** moderate

19. Examples of system-specific policy decisions which focus on only one system, include all of the following except:

A. Who is allowed to read or modify data?

B. Under what conditions can data be read or modified?

C. Can users dial into the system from home?

D. Are users permitted to use flash drives?

Answer: D **Reference:** System-Specific Policies **Difficulty:** moderate

20. The model for a system security policy does NOT include:

A. Security objectives

B. Operational security

C. Management structure

D. Policy implementation

Answer: C **Reference:** Development and Management of Security Policies **Difficulty:** moderate

21. All of the following statements about operational security documentation are true except:

A. Formal policy is published as a distinct policy document

B. Less formal policy may be written in memos

C. Informal policy may not be written at all

D. Uncommon policies are included in informal policy.

Answer: D **Reference:** Operational Security **Difficulty:** moderate

22. Automated methods of enforcing or supporting security policy would NOT include:

A. Block file save to all but hard disk

B. Intrusion detection software

C. Prevent booting from a floppy disk

D. Blocking telephone systems users from calling some numbers

Answer: A **Reference:** Development and Management of Security Policies **Difficulty:** moderate

23. The supporting documents derived from policy statements include all of the following except:

A. Regulations

B. Procedural maps

C. Standards and baselines

D. Guidelines

Answer: B **Reference:** Policy Support Documents **Difficulty:** moderate

24. Step-by-step directions to execute a specific security activity is referred to as a:

A. Regulation

B. Standard

C. Guideline

D. Procedure

Answer: D **Reference:** Policy Support Document **Difficulty:** moderate

25. Which of the following regulatory agencies regulates U.S. banks?

A. FTC

B. FFIEC

C. FDA

D. SEC.

Answer: B **Reference:** Regulations **Difficulty:** moderate

26. _____ is needed by businesses and agencies to determine how much security is needed for appropriate protection.

A. Separation of duties

B. Education, awareness, and training

C. Asset and data classification

D. Risk analysis and management.

Answer: C **Reference:** Asset Classification **Difficulty:** moderate

27. In the standards taxonomy _____ suggests that no single person is responsible for approving his own work.

A. Separation of duties

B. Education, awareness, and training

C. Asset and data classification

D. Risk analysis and management.

Answer: A **Reference:** Separation of Duties **Difficulty:** moderate

28. Which of the following would NOT be checked as part of an employee screening process?

A. Credit report

B. Worker's compensation reports

C. Education verification and credential confirmation

D. All of the above are checked.

Answer: D **Reference:** Employee Screening **Difficulty:** moderate

29. _____ provides technical facilities, data processing, and support services to users of information systems.

A. Chief information security officer

B. Information resources manager

C. Owners of information resources

D. Custodians of information resources

Answer: D **Reference:** Who is Responsible for Security **Difficulty:** moderate

30. Which of the following is NOT a calculation used for quantitative risk analysis?

A. ALE

B. Probability

C. Standard deviation

D. Vulnerability

Answer: C **Reference:** Quantitative Risk Analysis **Difficulty:** moderate

Fill in the Blank:

31. A constantly funded, ongoing management activity, a(n) _____ is intended for the preservation and advancement of the organization.

Answer: programme **Reference:** Introduction **Difficulty:** moderate

32. Even before security technology is acquired and deployed, _____ must be considered.

Answer: policies **Reference:** Security Policies Set the Stage **Difficulty:** moderate

33. A programme-level policy is also thought of as the _____ statement for the IT security program.

Answer: mission **Reference:** Four Types of Policies **Difficulty:** moderate

34. The _____ component of programme-level policy indicates which resources, information, and personnel the programme covers.

Answer: scope **Reference:** Programme-Level Policies **Difficulty:** moderate

35. The organization-wide direction for broad areas of programme implementation is found in the _____ policies.

Answer: programme-framework **Reference:** Programme-Framework Policies **Difficulty:** moderate

36. Security rules are derived from security _____.

Answer: goals **Reference:** Development and Management of Security Policies **Difficulty:** moderate

37. Security _____ are designed to describe meaningful actions about specific resources.

Answer: objectives **Reference:** Security Objectives **Difficulty:** moderate

38. Security objectives may not be fully met because of cost, operational, _____ and other constraints.

Answer: technical **Reference:** Operational Security **Difficulty:** moderate

39. Enforcing security is typically a combination of technical and _____ management methods.

Answer: traditional **Reference:** Policy Implementation **Difficulty:** moderate

40. Policy support _____ explain the system development, management, and operational requirements.

Answer: documents **Reference:** Policy Support Documents **Difficulty:** moderate

41. Information security _____ are often dictated by the nature of an organization’s business.

Answer: standards **Reference:** Regulations **Difficulty:** moderate

42. A(n) _____ refers to specific security requirements but a _____ is a specific set of requirements for a technology implementation.

Answer: standard, baseline **Reference:** Standards and Baselines **Difficulty:** moderate

43. To determine how much security is needed for protection, businesses use asset and data _____.

Answer: classification **Reference:** Asset Classification **Difficulty:** moderate

44. One way to limit any individual's ability to cause harm is to _____ duties within a business.

Answer: separate **Reference:** Separation of Duties **Difficulty:** moderate

45. Critical information used to make the best hiring decision is typically found in _____ records.

Answer: public **Reference:** Employee Screening **Difficulty:** moderate

46. Those individuals seeking employment involving access to sensitive government assets will have a _____ security clearance.

Answer: defense (or military) **Reference:** Military Security Clearance **Difficulty:** moderate

47. The two basic types of risk analysis and quantitative and _____.

Answer: qualitative **Reference:** Risk Analysis and Management **Difficulty:** moderate

48. User education, awareness, and training on policies and procedures are important because _____ are the weakest link in a security-related process.

Answer: people **Reference:** Education, Training, and Awareness **Difficulty:** moderate

Matching:

49. Match the following terms to their meanings:

I. Issue statement	A. Lists applicable standards or guidelines
II. Applicability	B. Describes infractions and states penalties
III. Compliance	C. Defines relevant terms, distinctions, and conditions
IV. Roles and responsibilities	D. Where, how, when, to whom policy applies
V. Points of contact	E. Identifies approving authority

Answer: C D B E A **Reference:** Issue Specific Policies **Difficulty:** moderate

50. Match the following terms to their meanings:

I. Asset classification	A. Limit individual's ability to cause harm
II. Separation of duties	B. Which security controls are appropriate and cost effective
III. Preemployment hiring practices	C. Top-driven and comprehensive
IV. Risk analysis and management	D. internal information security process
V. Education, awareness, and management	E. How much security is appropriate protection

Answer: E A D B C **Reference:** Suggested Standards Taxonomy **Difficulty:** moderate

51. Match the following terms to their meanings:

I. ALE	A. Absence of a risk-reducing safeguard
II. Probability	B. An event having an undesired impact
III. Threat	C. Single loss expectancy multiplied by annualized rate of occurrence
IV. Control	D. Chance that an event will occur
V. Vulnerability	E. Risk-reducing measure acts to detect, prevent, or minimize loss

Answer: C D B E A **Reference:** Risk Analysis and Management **Difficulty:** moderate

52. Match the following terms to their meanings:

I. CISO	A. Conduct periodic risk-based reviews
II. Information resources manager	B. Carry out programme that uses resources
III. Owners of information resources	C. People who have access to information resources
IV. Internal auditors	D. Maintains policies and procedures
V. Users	E. Establishes and maintains security and risk management programmes

Answer: E D B A C **Reference:** Who Is Responsible for Security **Difficulty:** moderate