Vendor: ISC

Exam Code: CISSP

Exam Name: Certified Information Systems Security Professional

Version: Demo

7

QUESTION 1
All of the following are basic components of a security policy EXCEPT the

A. definition of the issue and statement of relevant terms
B. statement of roles and responsibilities
C. statement of applicability and compliance requirements
D. statement of performance of characteristics and requirements

Correct Answer: D

QUESTION 2
A security policy would include all of the following EXCEPT

A. Background
B. Scope statement
C. Audit requirements
D. Enforcement

Correct Answer: B

QUESTION 3
Which one of the following is an important characteristic of an information security policy?

A. Identifies major functional areas of information.
B. Quantifies the effect of the loss of the information.
C. Requires the identification of information owners.
D. Lists applications that support the business function.

Correct Answer: A

QUESTION 4
Ensuring the integrity of business information is the PRIMARY concern of

A. Encryption Security
B. Procedural Security
C. Logical Security
D. On-line Security

Correct Answer: B

QUESTION 5
Which of the following would be the first step in establishing an information security program?

A. Adoption of a corporate information security policy statement.
B. Development and implementation of an information security standards manual.
C. Development of a security awareness-training program.
D. Purchase of security access control software.

Correct Answer: A

QUESTION 6
Which of the following department managers would be best suited to oversee the development of an information security policy?

A. Information Systems
B. Human Resources
C. Business operations
D. Security administration

Correct Answer: C

QUESTION 7
What is the function of a corporate information security policy?

A. Issue corporate standard to be used when addressing specific security problems.
B. Issue guidelines in selecting equipment, configuration, design, and secure operations.
C. Define the specific assets to be protected and identify the specific tasks which must be completed to secure them.
D. Define the main security objectives which must be achieved and the security framework to meet business objectives.

Correct Answer: D

QUESTION 8
Why must senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

Correct Answer: A

QUESTION 9
In which one of the following documents is the assignment of individual roles and responsibilities MOST appropriately defined?

A. Security policy
B. Enforcement guidelines
C. Acceptable use policy
D. Program manual

Correct Answer: C

QUESTION 10
Which of the following defines the intent of a system security policy?

A. A definition of the particular settings that have been determined to provide optimum security.
B. A brief, high-level statement defining what is and is not permitted during the operation of the system.
C. A definition of those items that must be excluded on the system.
D. A listing of tools and applications that will be used to protect the system.

Correct Answer: A

QUESTION 11
When developing an information security policy, what is the FIRST step that should be taken?

A. Obtain copies of mandatory regulations.
B. Gain management approval.
C. Seek acceptance from other departments.
D. Ensure policy is compliant with current working practices.

Correct Answer: B

QUESTION 12
Which one of the following should NOT be contained within a computer policy?

A. Definition of management expectations.
B. Responsibilities of individuals and groups for protected information.

C. Statement of senior executive support.
D. Definition of legal and regulatory controls.

Correct Answer: B

QUESTION 13
Which one of the following is NOT a fundamental component of a Regulatory Security Policy?

A. What is to be done?
B. When it is to be done?
C. Who is to do it?
D. Why is it to be done?

Correct Answer: C

QUESTION 14
Which one of the following statements describes management controls that are instituted to implement a security policy?

A. They prevent users from accessing any control function.
B. They eliminate the need for most auditing functions.
C. They may be administrative, procedural, or technical.
D. They are generally inexpensive to implement.

Correct Answer: C

QUESTION 15
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Seniors security analysts
D. system auditors

Correct Answer: B

QUESTION 16
Which of the following choices is NOT part of a security policy?

A. definition of overall steps of information security and the importance of security
B. statement of management intend, supporting the goals and principles of information security
C. definition of general and specific responsibilities for information security management
D. description of specific technologies used in the field of information security

Correct Answer: D

QUESTION 17
In an organization, an Information Technology security function should:

A. Be a function within the information systems functions of an organization.
B. Report directly to a specialized business unit such as legal, corporate security or insurance.
C. Be lead by a Chief Security Officer and report directly to the CEO.
D. Be independent but report to the Information Systems function.

Correct Answer: C

QUESTION 18
Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards
B. Guidelines
C. Procedures
D. Baselines

Correct Answer: C

QUESTION 19
A significant action has a state that enables actions on an ADP system to be traced to individuals who may then be held responsible. The action does NOT include:

A. Violations of security policy.
B. Attempted violations of security policy.
C. Non-violations of security policy.
D. Attempted violations of allowed actions.

Correct Answer: C

QUESTION 20
Network Security is a

A. Product
B. protocols
C. ever evolving process
D. quick-fix solution

Correct Answer: C

QUESTION 21
Security is a process that is:

A. Continuous
B. Indicative
C. Examined
D. Abnormal

Correct Answer: A

QUESTION 22
What are the three fundamental principles of security?

A. Accountability, confidentiality, and integrity.
B. Confidentiality, integrity, and availability.
C. Integrity, availability, and accountability.
D. Availability, accountability, and confidentiality.

Correct Answer: B

QUESTION 23
Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?

A. Communications security management and techniques.
B. Networks security management and techniques.
C. Clients security management and techniques.
D. Servers security management and techniques.

Correct Answer: A

QUESTION 24
Making sure that the data is accessible when and where it is needed is which of the following?

A. confidentiality
B. integrity
C. acceptability
D. availability

Correct Answer: D

QUESTION 25
Which of the following describes elements that create reliability and stability in networks and systems and which assures that connectivity is accessible when needed?

A. Availability
B. Acceptability
C. Confidentiality
D. Integrity

Correct Answer: A

QUESTION 26
Most computer attacks result in violation of which of the following security properties?

A. Availability
B. Confidentiality
C. Integrity and control
D. All of the choices

Correct Answer: D

QUESTION 27
Which of the following are objectives of an information systems security program?

A. Threats, vulnerabilities, and risks.
B. Security, information value, and threats.
C. Integrity, confidentiality, and availability.
D. Authenticity, vulnerabilities, and costs.

Correct Answer: C

QUESTION 28
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability

Correct Answer: B

QUESTION 29
The Structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, and authentication, and confidentiality for transmissions over private and public communications networks and media includes:

A. The Telecommunications and Network Security domain.
B. The Telecommunications and Netware Security domain.
C. The Technical communications and Network Security domain.
D. The Telnet and Security domain.

Correct Answer: A

QUESTION 30
Which one of the following is the MOST crucial link in the computer security chain?

A. Access controls
B. People
C. Management
D. Awareness programs

Correct Answer: C

QUESTION 31
The security planning process must define how security will be managed, who will be responsible, and

A. Who practices are reasonable and prudent for the enterprise?
B. Who will work in the security department?
C. What impact security will have on the intrinsic value of data?
D. How security measures will be tested for effectiveness?

Correct Answer: D

QUESTION 32
Information security is the protection of data. Information will be protected mainly based on:

A. Its sensitivity to the company.
B. Its confidentiality.
C. Its value.
D. All of the choices.

Correct Answer: D

QUESTION 33
Organizations develop change control procedures to ensure that

A. All changes are authorized, tested, and recorded.
B. Changes are controlled by the Policy Control Board (PCB).
C. All changes are requested, scheduled, and completed on time.
D. Management is advised of changes made to systems.

Correct Answer: A

QUESTION 34
Within the organizational environment, the security function should report to an organizational level that

A. Has information technology oversight.
B. Has autonomy from other levels.
C. Is an external operation.
D. Provides the internal audit function.

Correct Answer: B

QUESTION 35
What is the MAIN purpose of a change control/management system?

A. Notify all interested parties of the completion of the change.
B. Ensure that the change meets user specifications.
C. Document the change for audit and management review.
D. Ensure the orderly processing of a change request.

Correct Answer: C

QUESTION 36
Which of the following is most relevant to determining the maximum effective cost of access control?

A. the value of information that is protected
B. management's perceptions regarding data importance
C. budget planning related to base versus incremental spending
D. the cost to replace lost data

Correct Answer: A

QUESTION 37
Which one of the following is the MAIN goal of a security awareness program when addressing senior management?

A. Provide a vehicle for communicating security procedures.
B. Provide a clear understanding of potential risk and exposure.
C. Provide a forum for disclosing exposure and risk analysis.
D. Provide a forum to communicate user responsibilities.

Correct Answer: B

QUESTION 38
In developing a security awareness program, it is MOST important to

A. Understand the corporate culture and how it will affect security.
B. Understand employees preferences for information security.
C. Know what security awareness products are available.
D. Identify weakness in line management support.

Correct Answer: A

QUESTION 39
Which of the following would be best suited to provide information during a review of the controls over the process of defining IT service levels?

A. Systems programmer
B. Legal stuff

C. Business unit manager
D. Programmer

Correct Answer: C

QUESTION 40
Which of the following best explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools
B. Constantly changing user needs
C. Inadequate user participation in defining the system's requirements
D. Inadequate project management.

Correct Answer: C

QUESTION 41
Which of the following is not a compensating measure for access violations?

A. Backups
B. Business continuity planning
C. Insurance
D. Security awareness

Correct Answer: D

QUESTION 42
Risk analysis is MOST useful when applied during which phase of the system development process?

A. Project identification
B. Requirements definition
C. System construction
D. Implementation planning

Correct Answer: A

QUESTION 43
Which one of the following is not one of the outcomes of a vulnerability analysis?

A. Quantitative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C

QUESTION 44
Which of the following is not a part of risk analysis?

A. Identify risks
B. Quantify the impact of potential threats
C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasures
D. Choose the best countermeasure

Correct Answer: D

QUESTION 45
A new worm has been released on the Internet. After investigation, you have not been able to determine if you are at risk of exposure. Management is concerned as they have heard that a number of their counterparts are being affected by the worm. How could you determine if you are at risk?

A. Evaluate evolving environment.
B. Contact your anti-virus vendor.
C. Discuss threat with a peer in another organization.
D. Wait for notification from an anti-virus vendor.

Correct Answer: B

QUESTION 46
When conducting a risk assessment, which one of the following is NOT an acceptable social engineering practice?

A. Shoulder surfing
B. Misrepresentation
C. Subversion
D. Dumpster diving

Correct Answer: A

QUESTION 47
Which one of the following risk analysis terms characterizes the absence or weakness of a risk reducing safegaurd?

A. Threat
B. Probability
C. Vulnerability
D. Loss expectancy

Correct Answer: C

QUESTION 48
Risk is commonly expressed as a function of the

A. Systems vulnerabilities and the cost to mitigate.
B. Types of countermeasures needed and the system's vulnerabilities.
C. Likelihood that the harm will occur and its potential impact.
D. Computer system-related assets and their costs.

Correct Answer: C

QUESTION 49
How should a risk be handled when the cost of the countermeasures outweighs the cost of the risk?

A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk

Correct Answer: C

QUESTION 50
Which of the following is an advantage of a qualitative over quantitative risk analysis?

A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes cost-benefit analysis of recommended controls easier.
D. None of the above.

Correct Answer: A

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820		