Chapter 01 - Introduction to the Management of Information Security

TRUE/FALSE

1. Corruption of information can occur only while information is being stored.

   ANS: F PTS: 1 REF: 6

2. The authorization process takes place before the authentication process.

   ANS: F PTS: 1 REF: 8

3. The first step in solving problems is to gather facts and make assumptions.

   ANS: F PTS: 1 REF: 12

4. Project scope management ensures that the project plan includes only those activities that are necessary to complete it.

   ANS: T PTS: 1 REF: 20

5. A project can have more than one critical path.

   ANS: T PTS: 1 REF: 28

MULTIPLE CHOICE

1. Communications security involves the protection of which of the following?.
   a. radio handsets
   b. people, physical assets
   c. the IT department
   d. media, technology, and content

   ANS: D PTS: 1 REF: 4

2. According to the C.I.A. triangle, which of the following is a desirable characteristic for computer security?
   a. accountability
   b. availability
   c. authorization
   d. authentication

   ANS: B PTS: 1 REF: 6

3. Which of the following is a C.I.A. characteristic that ensures that only those with sufficient privileges and a demonstrated need may access certain information?
   a. Integrity
   b. Availability
   c. Authentication
   d. Confidentiality

   ANS: D PTS: 1 REF: 6

4. The use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections is an example of which process?
   a. accountability
   b. authorization
   c. identification
   d. authentication

   ANS: D PTS: 1 REF: 7-8

5. What do audit logs that track user activity on an information system provide?

a. identification
b. authorization
c. accountability
d. authentication

ANS: C PTS: 1 REF: 8

6. Which of the following is the process that develops, creates, and implements strategies for the accomplishment of objectives?

a. leading
b. controlling
c. organizing
d. planning

ANS: D PTS: 1 REF: 9

7. Which of the following is the principle of management dedicated to the structuring of resources to support the accomplishment of objectives?

a. organization
b. planning
c. controlling
d. leading

ANS: A PTS: 1 REF: 10

8. Which of the following is the first step in the problem-solving process?

a. Analyze and compare the possible solutions
b. Develop possible solutions
c. Recognize and define the problem
d. Select, implement and evaluate a solution

ANS: C PTS: 1 REF: 12

9. Which of the following is NOT a step in the problem-solving process?

a. Select, implement and evaluate a solution
b. Analyze and compare possible solutions
c. Build support among management for the candidate solution
d. Gather facts and make assumptions

ANS: C PTS: 1 REF: 11-13

10. Which of the following is NOT a unique function of Information Security Management?

a. planning
b. protection
c. project management
d. principles

ANS: D PTS: 1 REF: 13

11. Which of the following functions of Information Security Management seeks to dictate certain behavior within the organization through a set of organizational guidelines?

a. planning
b. policy
c. programs
d. people

ANS: B PTS: 1 REF: 14

12. Which function of InfoSec Management encompasses security personnel as well as aspects of the SETA program?

a. protection
b. people
c. projects
d. policy

ANS: B PTS: 1 REF: 15

13. Information security project managers often follow methodologies based on what methodology promoted by the Project Management Institute?
a. The Security Systems Development Life Cycle (SecSDLC)
b. The Security Project And Management Methodology (SPAMM)
c. Project Management System Methodology (PMS/Meth)
d. Project Management Body of Knowledge (PMBoK)

ANS: D PTS: 1 REF: 17-18

14. Which of the following is NOT a knowledge area in the Project Management knowledge body?
a. Integration
b. Quality
c. Scope
d. Technology

ANS: D PTS: 1 REF: 19

15. What is one of the most frequently cited failures in project management?
a. Overly restrictive management
b. Excessive personnel on project
c. Failure to meet project deadlines
d. Loose or ambiguous project specifications

ANS: C PTS: 1 REF: 21

16. The management of human resources must address many complicating factors; which of the following is NOT among them?
a. All workers operate at approximately the same level of efficiency
b. Not all workers begin the project with the same degree of skill
c. Skill mixtures among the actual project workers seldom match the needs of the project plan.
d. Some tasks may require skills that are not available from resources on hand

ANS: A PTS: 1 REF: 23

17. In the WBS approach, the project plan is first broken down into tasks placed on the WBS task list. The minimum attributes that should be identified for each task include all but which of the following?
a. Work to be accomplished (activities and deliverables)
b. Estimated amount of effort required for completion, in hours or workdays
c. The common or specialized skills needed to perform the task
d. The number of people and other resources needed for each task

ANS: D PTS: 1 REF: 25

18. Which of the following was originally developed in the late 1950s to meet the need of the rapidly expanding engineering projects associated with government acquisitions such as weapons systems?
a. GANTT
b. PERT
c. CPM
d. WBS

ANS: B PTS: 1 REF: 27

19. Using the Program Evaluation and Review Technique, which of the following identifies the sequence of events or activities that requires the longest duration to complete, and that therefore cannot be delayed without delaying the entire project?
a. program path
c. critical path

b. critical function d. crucial factor set

ANS: C PTS: 1 REF: 27

20. It is possible to take a very complex operation and diagram it in PERT if you can answer three key questions about each activity. Which of the following is NOT one of them?
   a. How long will it take?
   b. What activity occurs immediately before this activity?
   c. What activity occurs immediate activity after this activity?
   d. What other activities require the same resources as this activity?

ANS: D PTS: 1 REF: 27

COMPLETION

1. The three levels of planning are strategic planning, tactical planning, and ____________________ planning.

ANS: operational

PTS: 1 REF: 9

2. The set of organizational guidelines that dictates certain behavior within the organization is called ____________________.

ANS: policy

PTS: 1 REF: 14

3. ____________________ occurs when the quantity or quality of project deliverables is expanded from the original project plan.

ANS: Scope creep

PTS: 1 REF: 20

4. If the project deliverables meet the requirements specified in the project plan, the project has met its ____________________ objective.

ANS: Quality

PTS: 1 REF: 22

5. In the PERT technique, the difference in time between the critical path and any other path is called ____________________.

ANS: slack time

PTS: 1 REF: 28

MATCHING

a. identification
b. authentication
c. scope creep
d. slack time
e. information security
f. integrity
g. project management
h. Operations security
i. authorization
j. organizing

1. the difference between the time needed to complete the critical path and the time needed to arrive at completion using any other path
2. a mechanism that provides information about a supplicant that wants to be granted access to a known entity
3. a process for identifying and controlling the resources applied to the project
4. a state that occurs when the quantity or quality of project deliverables is expanded from the original project plan
5. a process that determines if a user has been specifically and explicitly authorized by the proper authority to perform a function
6. the protection of information and its critical characteristics
7. the management function dedicated to the structuring of resources to support the accomplishment of objectives
8. a specialized area of security that encompasses protecting the organization’s ability to carry out its operational activities without interruption or compromise
9. the process of validating a supplicant’s purported identity, thus ensuring that the entity requesting access is the entity it claims to be
10. a quality or state of being whole, complete, and uncorrupted

1. ANS: D	PTS: 1	REF: 28
2. ANS: A	PTS: 1	REF: 7
3. ANS: G	PTS: 1	REF: 15
4. ANS: C	PTS: 1	REF: 20
5. ANS: I	PTS: 1	REF: 8
6. ANS: E	PTS: 1	REF: 4
7. ANS: J	PTS: 1	REF: 10
8. ANS: H	PTS: 1	REF: 4
9. ANS: B	PTS: 1	REF: 7
10. ANS: F	PTS: 1	REF: 6

SHORT ANSWER

1. Explain the differences between a leader and a manager.

ANS:
The distinctions between a leader and a manager arise in the execution of organizational tasks. A leader provides purpose, direction, and motivation to those that follow. By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees.

PTS: 1 REF: 8

2. List and explain the critical characteristics of information as defined by the C.I.A. triangle.

ANS:

Confidentiality of information ensures that only those with sufficient privileges and a demonstrated need may access certain information. When unauthorized individuals or systems can view information, confidentiality is breached.

Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state.

Availability is the characteristic of information that enables user access to information without interference or obstruction and in a useable format.

PTS: 1 REF: 6-7

3. List and explain the four principles of management under the contemporary or popular management theory. Briefly define each.

ANS:
Popular management theory, which categorizes the principles of management into planning, organizing, leading, and controlling (POLC).

The process that develops, creates, and implements strategies for the accomplishment of objectives is called planning.

The management function dedicated to the structuring of resources to support the accomplishment of objectives is called organization.

Leadership includes supervising employee behavior, performance, attendance, and attitude. Leadership generally addresses the direction and motivation of the human resource.

Monitoring progress toward completion, and making necessary adjustments to achieve desired objectives, requires the exercise of control.

PTS: 1 REF: 9-11

4. List the steps that can be used as a basic blueprint for solving organizational problems.

ANS:
1. Recognize and Define the Problem
2. Gather Facts and Make Assumptions
3. Develop Possible Solutions
4. Analyze and Compare Possible Solutions.
5. Select, Implement and Evaluate a Solution.

PTS: 1 REF: 12-13

5. List the advantages and disadvantages of using the Program Evaluation and Review Technique method?

ANS:
Among the advantages to the PERT method are:
>Planning large projects is made easier by facilitating the identification of pre- and post activities.
>Planning to determine the probability of meeting requirements (that is, timely delivery through calculation of critical paths) is allowed.

>The impact of changes on the system are anticipated. Should a delay in one area occur, how does it affect the overall project schedule?
>Information is presented in a straightforward format that both technical and non-technical managers can understand and refer to in planning discussions.
>No formal training is required. After a brief explanation most people understand it thoroughly.

Disadvantages of the PERT method include:
>Diagrams can become awkward and cumbersome, especially in very large projects.
>Diagrams can become expensive to develop and maintain due to the complexities of some project development processes.
>It can be difficult to place an accurate “time to complete” on some tasks, especially in the initial construction of a project; inaccurate estimates invalidate any close critical path calculations.

PTS: 1 REF: 28-29

6. What are the three distinct groups of decision makers or communities of interest on an information security team?

ANS:
Managers and professionals in the field of information security
Managers and professionals in the field of IT
Managers and professionals from the rest of the organization

PTS: 1 REF: 3

7. List the four specialized areas of security.

ANS:
Physical security
Operations security
Communications security
Network security

PTS: 1 REF: 4

8. List three measures that are commonly used to protect the confidentiality of information.

ANS:
Information classification
Secure document (and data) storage
Application of general security policies
Education of information custodians and end users
Cryptography (encryption)

PTS: 1 REF: 6

9. What is authentication? Provide some examples.

ANS:
Authentication is the process by which a control establishes whether a user (or system) has the identity it claims to have. Examples include the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections as well as the use of cryptographic hardware devices—for example, hardware tokens such as RSA’s SecurID. Individual users may disclose a personal identification number (PIN) or a password to authenticate their identities to a computer system.

PTS: 1 REF: 7

10. Discuss the planning element of information security.

ANS:
Planning in InfoSec management is an extension of the basic planning model. Included in the InfoSec planning model are activities necessary to support the design, creation, and implementation of InfoSec strategies within the IT planning environment. The business strategy is translated into the IT strategy. Both the business strategy and the IT strategy are then used to develop the InfoSec strategy. For example, the CIO uses the IT objectives gleaned from the business unit plans to create the organization’s IT strategy.

PTS: 1 REF: 13