**Chapter 15 – IT Security Controls, Plans, and Procedures**

**TRUE/FALSE QUESTIONS:**

T F 1. To ensure that a suitable level of security is maintained, management

must follow up the implementation with an evaluation of the effectiveness of the security controls.

T F 2. Management controls refer to issues that management needs to address.

T F 3. Operational controls range from simple to complex measures that work

together to secure critical and sensitive data, information, and IT systems functions.

T F 4. Detection and recovery controls provide a means to restore lost

computing resources.

T F 5. Water damage protection is included in security controls.

T F 6. All controls are applicable to all technologies.

T F 7. Physical access or environmental controls are only relevant to areas

housing the relevant equipment.

T F 8. Once in place controls cannot be adjusted, regardless of the results of

risk assessment of systems in the organization.

T F 9. Controls may vary in size and complexity in relation to the

organization employing them.

T F 10. It is likely that the organization will not have the resources to

implement all the recommended controls.

T F 11. The selection of recommended controls is not guided by legal

requirements.

T F 12. The recommended controls need to be compatible with the

organization’s systems and policies.

T F 13. The implementation phase comprises not only the direct

implementation of the controls, but also the associated training and general security awareness programs for the organization.

T F 14. Appropriate security awareness training for all personnel in an

organization, along with specific training relating to particular systems and controls, is an essential component in implementing controls.

T F 15. The IT security management process ends with the implementation of

controls and the training of personnel.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_ is a formal process to ensure that critical assets are sufficiently protected in a cost-effective manner.
2. Configuration management control
3. IT security management
4. Detection and recovery control
5. Security compliance

2. An IT security \_\_\_\_\_\_\_\_ helps to reduce risks.

A. control B. safeguard

C. countermeasure D. all of the above

3. \_\_\_\_\_\_\_ controls focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization’s mission.

A. Management B. Technical

C. Preventative D. Supportive

4. \_\_\_\_\_\_\_ controls are pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.

A. Preventative B. Supportive

C. Operational D. Detection and recovery

5. \_\_\_\_\_\_\_\_ controls focus on the response to a security breach, by warning of violations or attempted violations of security policies.

A. Technical B. Preventative

C. Detection and recovery D. Management

6. A contingency plan for systems critical to a large organization would be \_\_\_\_\_\_\_\_\_ than that for a small business.

A. smaller, less detailed B. larger, less detailed

C. larger, more detailed D. smaller, more detailed

7. Management should conduct a \_\_\_\_\_\_\_\_ to identify those controls that are most appropriate and provide the greatest benefit to the organization given the available resources.

A. cost analysis B. cost-benefit analysis

C. benefit analysis D. none of the above

8. An IT security plan should include details of \_\_\_\_\_\_\_\_\_.

A. risks B. recommended controls

C. responsible personnel D. all of the above

9. The implementation process is typically monitored by the organizational \_\_\_\_\_\_.

A. security officer B. general counsel

C. technology officer D. human resources

10. The follow-up stage of the management process includes \_\_\_\_\_\_\_\_\_.

A. maintenance of security controls

B. security compliance checking

C. incident handling

D. all of the above

11. The objective of the \_\_\_\_\_\_\_\_ control category is to avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements.

A. access B. asset management

C. compliance D. business continuity management

12. The objective of the \_\_\_\_\_\_\_\_ control category is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A. asset management

B. business continuity management

C. information security incident management

D. physical and environmental security

13. Identification and authentication is part of the \_\_\_\_\_\_\_ class of security controls.

A. technical B. operational

C. management D. none of the above

14. Maintenance of security controls, security compliance checking, change and configuration management, and incident handling are all included in the follow-up stage of the \_\_\_\_\_\_\_\_\_ process.

A. management B. security awareness and training

C. maintenance D. all of the above

15. Periodically reviewing controls to verify that they still function as intended, upgrading controls when new requirements are discovered, ensuring that changes to systems do not adversely affect the controls, and ensuring new threats or vulnerabilities have not become known are all \_\_\_\_\_\_\_\_ tasks.

A. security compliance B. maintenance

C. incident handling D. program management

**SHORT ANSWER QUESTIONS:**

1. A \_\_\_\_\_\_\_\_\_ on an organization’s IT systems identifies areas needing treatment.
2. \_\_\_\_\_\_\_\_ is a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures.
3. The three steps for IT security management controls and implementation are: prioritize risks, respond to risks, and \_\_\_\_\_\_\_\_\_\_ .
4. \_\_\_\_\_\_\_\_ controls involve the correct use of hardware and software security capabilities in systems.
5. The \_\_\_\_\_\_\_ plan documents what needs to be done for each selected control, along with the personnel responsible, and the resources and time frame to be used.
6. When the implementation is successfully completed, \_\_\_\_\_\_\_ needs to authorize the system for operational use.
7. \_\_\_\_\_\_ checking is an audit process to review the organization’s security processes.
8. \_\_\_\_\_\_\_ management is the process used to review proposed changes to systems for implications on the organization’s systems and use.
9. \_\_\_\_\_\_\_ management is concerned with specifically keeping track of the configuration of each system in use and the changes made to each.
10. The \_\_\_\_\_\_\_\_\_ controls focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.
11. Contingency planning falls into the \_\_\_\_\_\_\_\_\_ class of security controls.
12. \_\_\_\_\_\_\_\_\_ controls focus on preventing security beaches from occurring by inhibiting attempts to violate security policies or exploit a vulnerability.
13. The \_\_\_\_\_\_\_\_ audit process should be conducted on new IT systems and services once they are implanted; and on existing systems periodically, often as part of a wider, general audit of the organization or whenever changes are made to the organization’s security policy.
14. Controls can be classified as belonging to one of the following classes: management controls, operational controls, technical controls, detection and recovery controls, preventative controls, and \_\_\_\_\_\_\_ controls.
15. Incident response is part of the \_\_\_\_\_\_\_\_ class of security controls.