**Chapter 14 – IT Security Management and Risk Assessment**

**TRUE/FALSE QUESTIONS:**

T F 1. IT security management consists of first determining a clear view of an

organization’s IT security objectives and general risk profile.

T F 2. IT security management has evolved considerably over the last few

decades due to the rise in risks to networked systems.

T F 3. Detecting and reacting to incidents is not a function of IT security

management.

T F 4. IT security needs to be a key part of an organization’s overall

management plan.

T F 5. Once the IT management process is in place and working the process

never needs to be repeated.

T F 6. Organizational security objectives identify what IT security outcomes

should be achieved.

T F 7. The assignment of responsibilities relating to the management of IT

security and the organizational infrastructure is not addressed in a

corporate security policy.

T F 8. Organizational security policies identify what needs to be done.

T F 9. It is not critical that an organization’s IT security policy have full

approval or buy-in by senior management.

T F 10. Because the responsibility for IT security is shared across the

organization, there is a risk of inconsistent implementation of security and a loss of central monitoring and control.

T F 11. Legal and regulatory constraints may require specific approaches to

risk assessment.

T F 12. A major advantage of the informal approach is that the individuals

performing the analysis require no additional skills.

T F 13. A major disadvantage of the baseline risk assessment approach is the

significant cost in time, resources, and expertise needed to perform

the analysis.

T F 14. One asset may have multiple threats and a single threat may target

multiple assets.

T F 15. A threat may be either natural or human made and may be accidental

or deliberate.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_\_ ensures that critical assets are sufficiently protected in a cost-effective manner.

A. IT control B. IT security management

C. IT discipline D. IT risk implementations

2. The \_\_\_\_\_\_\_\_ has revised and consolidated a number of national and international standards into a consensus of *best practice*.

A. ISO B. CSI

C. VSB D. DBI

3. IT security management functions include:

A. determining organizational IT security objectives, strategies, and policies

B. detecting and reacting to incidents

C. specifying appropriate safeguards

D. all of the above

4. Implementing the risk treatment plan is part of the \_\_\_\_\_\_ step.

A. check B. act

C. do D. plan

5. Maintaining and improving the information security risk management process

in response to incidents is part of the \_\_\_\_\_\_\_\_\_ step.

A. act B. plan

C. check D. do

6. Establishing security policy, objectives, processes and procedures is part of the \_\_\_\_\_\_ step.

A. plan B. check

C. act D. none of the above

7. The intent of the \_\_\_\_\_\_\_\_ is to provide a clear overview of how an organization’s IT infrastructure supports its overall business objectives.

A. risk register B. corporate security policy

C. vulnerability source D. threat assessment

8. The advantages of the \_\_\_\_\_\_\_\_\_ approach are that it doesn’t require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems.

A. combined B. informal

C. baseline D. detailed

9. The \_\_\_\_\_\_\_\_\_ approach involves conducting a risk analysis for the organization’s IT systems that exploits the knowledge and expertise of the individuals performing the analysis.

A. baseline B. combined

C. detailed D. informal

10. A \_\_\_\_\_\_\_\_ is anything that might hinder or present an asset from providing appropriate levels of the key security services.

A. vulnerability B. threat

C. risk D. control

11. \_\_\_\_\_\_\_\_\_ include management, operational, and technical processes and procedures that act to reduce the exposure of the organization to some risks by reducing the ability of a threat source to exploit some vulnerabilities.

**A. Security controls** B. Risk appetite

C. Risk controls D. None of the above

12. The results of the risk analysis should be documented in a \_\_\_\_\_\_\_\_\_.

A. journal B. consequence

C. risk register D. none of the above

13. \_\_\_\_\_\_\_\_ specification indicates the impact on the organization should the particular threat in question actually eventuate.

A. Risk B. **Consequence**

C. Threat D. Likelihood

14. The purpose of \_\_\_\_\_\_\_\_ is to determine the basic parameters within which the risk assessment will be conducted and then to identify the assets to be examined.

A. **establishing the context**  B. control

C. risk avoidance D. combining

15. \_\_\_\_\_\_\_\_\_ is choosing to accept a risk level greater than normal for business reasons.

A. Risk avoidance B. Reducing likelihood

C. Risk transfer D. Risk acceptance

**SHORT ANSWER QUESTIONS:**

1. IT SECURITY MANAGEMENT\_\_\_\_\_\_\_\_\_ is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability.
2. ISO details a model process for managing information security that comprises the following steps: plan, do, CHECK\_\_\_\_\_\_\_\_, and act.
3. The term SECURITY POLICY\_\_\_\_\_\_\_\_ refers to a document that details not only the overall security objectives and strategies, but also procedural policies that define acceptable behavior, expected practices, and responsibilities.
4. The aim of the RISK ASSESSMENT\_\_\_\_\_\_\_\_\_ process is to provide management with the information necessary for them to make reasonable decisions on where available resources will be deployed.
5. The four approaches to identifying and mitigating risks to an organization’s IT infrastructure are: baseline approach, detailed risk analysis, combined approach, and INFORMAL\_\_\_\_\_\_\_\_\_\_ approach.
6. The BASELINE \_\_\_\_\_\_\_\_\_\_ approach to risk assessment aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and industry best practice.
7. The use of the INFORMAL\_\_\_\_\_\_\_\_\_ approach would generally be recommended for small to medium-sized organizations where the IT systems are not necessarily essential to meeting the organization’s business objectives and additional expenditure on risk analysis cannot be justified.
8. The advantages of the DETAILED\_\_\_\_\_\_\_\_\_ risk assessment approach are that it provides the most detailed examination of the security risks of an organization’s IT system and produces strong justification for expenditure on the controls proposed.
9. A(n) VULNERABILITY\_\_\_\_\_\_\_\_\_ is a weakness in an asset or group of assets that can be exploited by one or more threats.
10. A(n) ASSET \_\_\_\_\_\_\_\_\_ is anything that has value to the organization.
11. The level of risk the organization views as acceptable is the organization’s RISK APPETITE\_\_\_\_\_\_\_\_\_\_.
12. RISK TRANSFER\_\_\_\_\_\_\_\_\_ is sharing responsibility for the risk with a third party.
13. Not proceeding with the activity or system that creates the risk is RISK AVOIDANCE\_\_\_\_\_\_\_\_\_.
14. The COMBINED\_\_\_\_\_\_\_\_\_ approach combines elements of the baseline, informal, and detailed risk analysis approaches.
15. The DETAILED SECURITY RISK ANALYSIS APPROACH\_\_\_\_\_\_\_\_\_ provides the most accurate evaluation of an organization’s IT system’s security risks.