PIRDR2 Ch01 Review Questions

1. What is information security?

Information security is an umbrella term for the many programs and activities that work to assure the confidentiality, integrity, and availability of information used by organizations. This includes steps to assure the confidentiality, integrity, and (specifically in the case of contingency planning) availability of organizational information systems. Information security (InfoSec) is the protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission.

2. How is the CNSS model of information security organized?

The CNSS model is organized along three axes. The first represents whether the data is being stored, being processed, or in transit. The second axis represents the characteristics of confidentiality, integrity and availability, which must be protected in each data mode. The third axis represents the controls that implement policy, technology, or education for each mode and characteristic.

3. What three principles are used to define the C.I.A. triangle? Define each in the context in which it is used in information security.

C.I.A. represents confidentiality, integrity and availability. Information has the characteristic of confidentiality when only those with the rights and privileges to access it are able to do so. Information has integrity when it has not been exposed (while stored or transmitted) to corruption, damage, destruction, or other disruption of its authentic state; in other words, it is whole, complete, and uncorrupted. Finally, information has availability when authorized users—

persons or computer systems—are able to access it in the specified format without interference or obstruction.

4. What is a threat in the context of information security?

A threat is a category of objects, persons, or other entities that pose a potential risk of loss to an asset.

5. What is an asset in the context of information security?

An asset is an organizational resource that has value and thus needs to be protected.

6. What is a vulnerability in the context of information security?

A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited and result in a security breach or violation of the system's security policy.

7. What is risk management?

Risk management is the process of identifying and controlling the risks to an organization's information assets. It consists of two major undertakings: risk identification and risk control.

8. What are the component parts of risk management?

Risk management consists of two major undertakings: risk identification and risk control.

9. Who is expected to be engaged in risk management activities in most organizations?

All management levels are engaged in risk management. Among the communities of interest, the general management of the organization must structure the IT and information security functions to lead a successful defense of the organization's information assets, which consist of information and data, hardware, software, procedures, and people.

10. What are the basic strategies used to control risk? Define each.

The five basic risk-control strategies are:

Defense—Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability.

Transferal—Shift the risk to other areas or to outside entities.

Mitigation—Reduce the impact should the vulnerability be exploited.

Acceptance—Determine the potential consequences and accept the risk without control or mitigation.

Termination—Remove the information asset from the environment that represents a risk to its security.

11. What is a contingency plan?

A contingency plan helps an organization anticipate, react to, and recover from events that threaten the security of information and information assets in the organization; it is also used to restore the organization to normal modes of business operations.

12. List and describe the four subordinate functions of a contingency plan.

Contingency planning involves four subordinate functions:

Business impact assessment

Incident response planning

Disaster recovery planning

Business continuity planning

13. In general terms, what is policy?

A policy is a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the context of the organization's culture.

14. What is the enterprise information security policy, and how is it used?

An enterprise information security policy (EISP), also known as a general security policy, IT security policy, or information security policy, is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts. It is an executive-level document, usually drafted by, or in cooperation with, the chief information officer of the organization.

15. Why is shaping policy considered difficult?

Shaping policy is difficult because it must never conflict with laws, it must stand up in court if challenged, and must be properly administered through dissemination and documented acceptance.

16. What are standards? How are they different from policy?

More detailed than policy, standards state what must be done to comply with policy.

17. What is an issue-specific security policy?

The issue-specific security policy (ISSP) addresses specific areas of technology and contains a statement on the organization's position on a specific issue. It requires frequent updates.

18. List the critical areas covered in an issue-specific security policy.

The critical elements of an ISSP are: statement of policy, authorized access and usage of equipment, prohibited usage of equipment, systems management, violations of policy, policy review and modification, and limitations of liability.

19. What is a systems-specific security policy?

Systems-specific security policies (SysSPs) are detailed policies that govern how specific technology systems are to be managed. They may resemble procedures or guidelines and blend aspects of policy with the need to control specific technology systems.

20. When is a systems-specific security policy used?

SysSPs are often used when specifying the configuration or maintenance of systems.