Workshop 4 for Week 5

1. Quick Quiz:

1.1 True or False: Policy must be able to stand up in court if challenged.

1.2 In the bull's-eye model, the outer layer in the diagram represents_____.
a. networks
b. applications
c. policies
d. systems

1.3 What is one of the three types of an information security policy?
a. Enterprise information security policy
b. Network information security policy
c. Threat assessment information security policy
d. Privacy information security policy

1.4 What type of security policy provides detailed, targeted guidance to instruct all members of the organization in the use of a process, technology or system?

ISSP, Issue-Specific Security Policy

1.5 True or False: An ISSP should not require frequent updates.

1.6 True or False: For policies to be effective, they must be properly developed using industry-accepted practices.

1.7 What documents should be gathered or produced during the analysis phase of developing an information security policy?

EISP

1.8 What are some methods of policy distribution?

Inform, email.

1.9 What is the name of the policy management software tool covered in this chapter?

VigilEnt Policy Center (VPC),

1.10 What is the recommended review schedule for information security policies?

Periodic review

1.11 Short term policies should have a(n)_____ to avoid becoming permanent policies.

review date

2. Describe the bull's-eye model. What does it say about policy in the InfoSec program?

The bull's-eye model is a framework used in Information Security (InfoSec) that emphasizes the role of policy in an InfoSec program. It provides a visual representation of different levels of security policy, making it easier to understand and explain.

3. Is policy considered static or dynamic? Which factors might determine this status?

Statistic, tone and emphasis

4. List and describe the three types of InfoSec policy as described by NIST SP 800-14. In your opinion, which is best suited for use by a smaller organization and why? If the target organization were very much larger, which approach would be more suitable and why?

EISP, ISSP, and SysSP. Smaller organizations might prefer ISSPs, focusing on crucial security areas without extensive overhead. In contrast, larger organizations may favor EISPs for their comprehensive, strategic approach applicable to diverse operations, thereby promoting a strong security culture.

5. List and describe four elements that should be present in the EISP. Identify these four elements in the EISP.

1. Corporate Philosophy on Security, which clearly states the organization's stance and objectives on information security. 2. Structure of the InfoSec Organization, outlining the roles within the security framework and their interaction. 3. InfoSec Responsibilities, defining who is responsible for respective security tasks for accountability. 4. Policy Review and Modification Procedures,

6. List and describe three functions that the ISSP serves in the organization.

1.Detailed Guidance: ISSP provides comprehensive, targeted details instructing all members of an organization on how to use systems or processes, ensuring everyone is on the same page regarding security. 2. Clarification of Technology-based Expectations: It expresses the organization's expectations regarding the use of its technology-based resources, clearing any confusion about what's permitted. 3. Protection Strategy: By establishing a specific framework for each issue, the ISSP routes the strategy and protection measures to safeguard distinct assets.