# Week 5 Hands On

Eric Vara

The University of Arizona Global Campus

CYB 300

Instructor Bipin Bhatt

19, December 2022

## Part One

### Module 11: Implementing Information Security Review Questions

1. What is a methodology in the context of implementing secure systems?
   * Answer:
2. What is a systems development life cycle (or SDLC)?
   * Answer:
3. What is a project plan? List what a project plan can accomplish.
   * Answer:
4. What categories of constraints to project plan implementation are noted in the module? Explain each of them.
   * Answer:
5. List and describe the three major steps in executing the project plan.
   * Answer:
6. What is a work breakdown structure (WBS)? Is it the only way to organize a project plan?
   * Answer:
7. What is projectitis? How is it cured or its impact minimized?
   * Answer:
8. List and define the common attributes of tasks within a WBS.
   * Answer:
9. How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step?
   * Answer:
10. What is a deliverable? Name two uses for deliverables.
    * Answer:
11. What is a resource? What are the two types?
    * Answer:
12. Why is it a good practice to delay naming specific people as resources early in the planning process?
    * Answer:
13. What is a milestone, and why is it significant to project planning?
    * Answer:
14. Why is it good practice to assign start and end dates sparingly in the early stages of project planning?
    * Answer:
15. Who is the best judge of effort estimates for project tasks and action steps? Why?
    * Answer:
16. Within project management, what is a dependency? What is a predecessor? What is a successor?
    * Answer:
17. What is a negative feedback loop? How is it used to keep a project in control?
    * Answer:
18. When a task is not being completed according to the plan, what two circumstances are likely to be involved?
    * Answer:
19. List and describe the four basic conversion strategies that are used when converting to a new system. Under which circumstances is each strategy the best approach?
    * Answer:
20. What is technology governance? What is change control? How are they related?
    * Answer:

### Module 12: Information Security Maintenance Review Questions

1. List and define the factors that are likely to shift in an organization’s information security environment.
   * Answer:
2. Who decides if the information security program can adapt to change adequately?
   * Answer:
3. Is information security risk management usually a static or dynamic process?
   * Answer:
4. What is a management maintenance model? What does it accomplish?
   * Answer:
5. What changes need to be made to the model in SP 800-100 to adapt it for use in security management maintenance?
   * Answer:
6. What ongoing responsibilities do security managers have in securing the SDLC?
   * Answer:
7. What is vulnerability assessment?
   * Answer:
8. What is penetration testing?
   * Answer:
9. What is the difference between vulnerability assessment and penetration testing?
   * Answer:
10. List and briefly describe the five domains of the general security maintenance model, as identified in the text.
    * Answer:
11. What is the objective of the external monitoring domain of the maintenance model?
    * Answer:
12. List and describe four vulnerability intelligence sources. Which seems the most effective? Why?
    * Answer:
13. What does CERT stand for? Is there more than one CERT?
    * Answer:
14. What is the primary objective of the internal monitoring domain?
    * Answer:
15. What is the objective of the planning and risk assessment domain of the maintenance model? Why is this important?
    * Answer:
16. What is the primary goal of the vulnerability assessment and remediation domain of the maintenance model? Is this important to an organization with an Internet presence? Why?
    * Answer:
17. List and describe the five vulnerability assessments described in the text. Can you think of other assessment processes or variations that might exist?
    * Answer:
18. What is physical security?
    * Answer:
19. What are the roles of an organization’s IT, security, and general management with regard to physical security?
    * Answer:
20. Define a secure facility. What is the primary objective of designing such a facility? What are some secondary objectives of designing a secure facility?
    * Answer:
21. What are the two possible modes of locks when they fail? What implications do these modes have for human safety? In which situation is each preferred?
    * Answer:
22. What is a mantrap? When should it be used?
    * Answer:
23. What is considered the most serious threat within the realm of physical security? Why is it valid to consider this threat the most serious?
    * Answer:
24. What is the relationship between HVAC and physical security? What four physical characteristics of the indoor environment are controlled by a properly designed HVAC system? What are the optimal temperature and humidity ranges for computing systems?
    * Answer:
25. List and describe the three fundamental ways that data can be intercepted. How does a physical security program protect against each of these data-interception methods?
    * Answer:

## Part Two

### Hands-On Project: Using OSSIM

Complete the Hands-On Project: Using OSSIM

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Attach the screen shot taken at completion of OSSIM setup or insert it here.

Were you able to complete the setup, configuration, and use of OSSIM?

|  |
| --- |
|  |

If you were not able to complete the setup and configuration, explain what went wrong.

|  |
| --- |
|  |

### Hands-On Project: Image Analysis with Autopsy

Complete the Hands-On Project: Image Analysis with Autopsy

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Attach the final report.

Were you able to complete the setup, configuration, and use of Autopsy?

|  |
| --- |
|  |

If you were not able to complete the setup and configuration, explain what went wrong.

|  |
| --- |
|  |