Chapter 14 & 15 Homework Assignment

Instructions: Answer each of the following questions in your own words. Provide examples where appropriate. Be thorough and concise.

Chapter 14: Oversight & Operations

1. Governance Fundamentals:
Explain the five core principles of governance (Accountability, Leadership, Integrity, Stewardship, Transparency). Why is each important in an organization?
2. Governance Bodies:
Differentiate between internal and external governance bodies. Provide an example of each and describe their role in decision-making.
3. System & Data Roles:
Define the roles of the Owner, Custodian, Controller, and Processor. Who is responsible for what when it comes to a sensitive file like SALARY.XLSX?
4. Policy Hierarchy:
Describe the relationship between policies, procedures, standards, and guidelines. Why is this hierarchy essential to information security?
5. Compliance Monitoring:
What are the differences between internal and external compliance monitoring? What are some benefits and limitations of each?
6. Security Automation Benefits:
Choose three benefits of automation listed in the chapter and describe how each improves information security operations.
7. Security Orchestration and SOAR:
What is SOAR? How does it improve an organization’s ability to detect and respond to threats?
8. Threat Hunting vs. Incident Response:
Contrast the roles of an incident responder and a threat hunter. When would you use one over the other?
9. Artificial Intelligence in Cybersecurity:
List two advantages and two risks of using AI in information security operations.
10. Adversarial AI:
What is adversarial AI? Provide one example of how an attacker might exploit it.

Chapter 15: Information Security Management

11. Asset Classification:

Review the asset categories listed in the chapter (e.g., data, software, physical items). Which ones are considered high value and why?

12. CAM (Cybersecurity Asset Management):

What is CAM and why is it critical for maintaining enterprise security?

13. Asset Lifecycle:

Outline the stages of an asset's lifecycle. How does each stage impact cost and security?

14. Change Management Documentation:

Why is documentation critical in change management? What problems could occur if changes aren't documented?

15. Types of Risk Assessments:

Describe the differences between qualitative and quantitative risk assessments. When would each be most appropriate?

16. Unconscious Bias in Risk Analysis:

Choose two types of bias from the chapter and describe how they might affect cybersecurity decision-making.

17. Risk Formulas:

Define and explain SLE, ARO, and ALE. Provide a simple numeric example showing how they work together.

18. Risk Response Strategies:

Explain the four risk response strategies (Accept, Transfer, Avoid, Mitigate). Give an example of each in an IT context.

19. Third-Party Risk Management:

Why is vendor oversight important? What steps can an organization take to reduce third-party risk?

20. Security Awareness Techniques:

Choose two user training techniques (e.g., phishing simulations, CBT). Describe how they help raise awareness and reduce human error.