**CIDM 6341 01 Current Issues in Cybersecurity**

**Mid-term Exam Sp2022**

**CLOSED BOOK (25%) – 50 points**

Name\_\_\_\_\_\_\_\_Mike Pendleton\_\_\_\_\_\_\_\_BID\_\_\_\_\_\_\_ 1058201 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1. TEN True/False (write in the left side) – 20 points**

True a. It is the role of cybersecurity management to ensure that each strategy is properly planned, organized, staffed, directed, and controlled.

False b. A breach law specifies a requirement for organizations to notify affected parties when they have experienced a specified type of loss of information

False c. The value statement is an idealistic expression of what the organization wants to become

True d. Information security, like information technology, must support more than its immediate parent in the organizational chart

True e. In a small organization, InfoSec often becomes the responsibility of a jack-of-all-trades

True f. Risk = Likelihood + Impact

False g. Risk management answers the question “Where and what is the risk?”

True h. The organization should conduct a weighted table analysis with threats

False i. When a Mandatory Access Control (MAC) is implemented, users and data owners have full control over access to information resources

False j. Most organizations already have a set of RM practices in place

**B. Fill in the TEN Blanks [Find answers from the box] – 20 points**

1. The \_\_\_\_\_\_\_\_\_Security\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Model provides a more detailed perspective on security
2. \_\_\_\_Deterrence\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_is the best method for preventing an illegal or unethical activity
3. \_Digital Forensics\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_is the identification and preservation of evidentiary materials related to a specific legal action
4. After an organization develops a\_\_Risk management framework\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, it must create an overall strategic plan by extending that general strategy into \_\_\_\_\_\_\_policies\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_for major divisions
5. RM policy focuses on the “\_who and why\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_” of RM, the plan is focused on the “\_\_who and how\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_”
6. COSO’s framework is built on five interrelated components: Control environment, \_\_risk assessment\_,Control activities, \_information and communication\_\_\_\_\_\_, monitoring
7. Access control is built on several key principles including least privilege, need to know, and\_\_\_separation of duties\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |
| --- |
| Find you answer from the box |
| **Separation of duties , who and why, general strategy , Information and communication , Deterrence , McCumber Cube, E-discovery, specific strategic plans, who and how, Risk assessment** |

**Q3. Matching [Match from “left side” to “right-side”, you draw a line of connection or “a+h” etc.] 10 points**

|  |  |
| --- | --- |
| Left Side | Right Side |
| 1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2. Precursor documents developed to support organizational planning include 3. Risk management is the process of discovering and assessing the risks to an organization’s operations and 4. The risk treatment strategy that attempts to shift risk to another entity is known as 5. A single loss expectancy (SLE) = | 1. Defense 2. American Recovery and Reinvestment Act (ARRA) 3. Mission, Vision, and Values statement 4. determining how those risks can be controlled or mitigated 5. transference 6. Values statement 7. Mitigation 8. asset value (AV) + exposure factor (EF) 9. USA PATRIOT Act of 2001 10. asset value (AV) \* exposure factor (EF) |

**CIDM 6341 01 Current Issues in Cybersecurity**

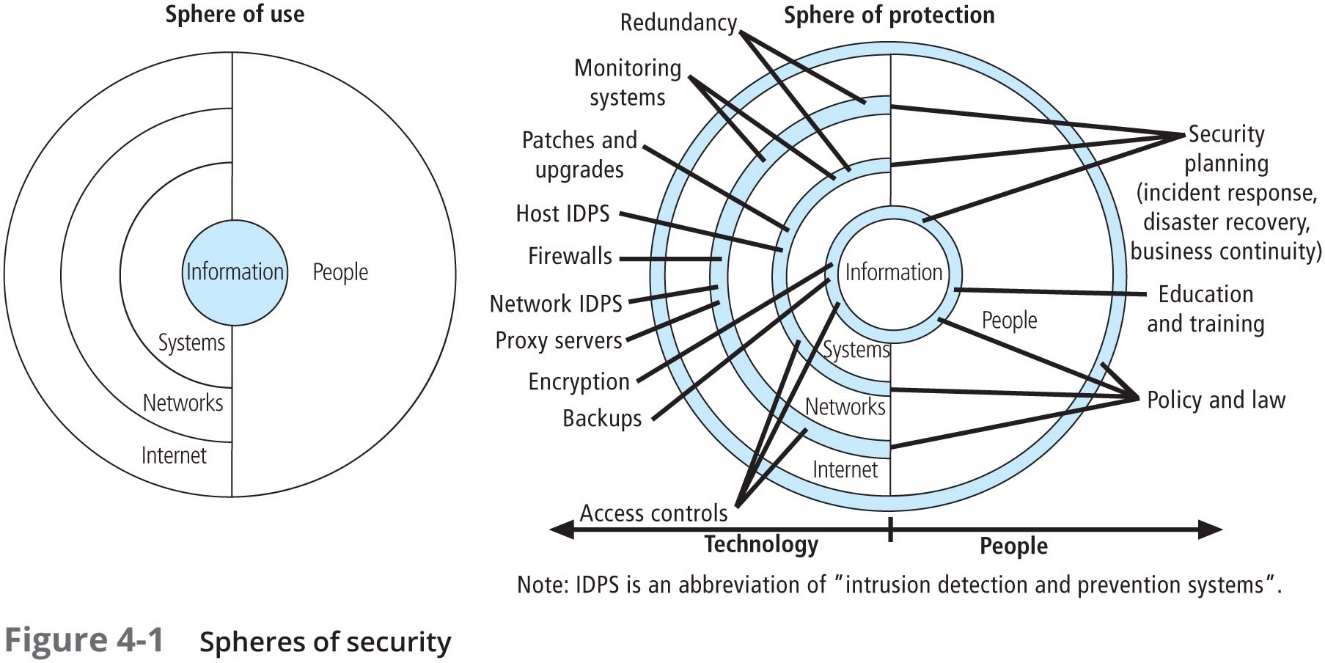
**Mid-term Exam Sp2022**

**OPEN BOOK (75%) – 150 points**

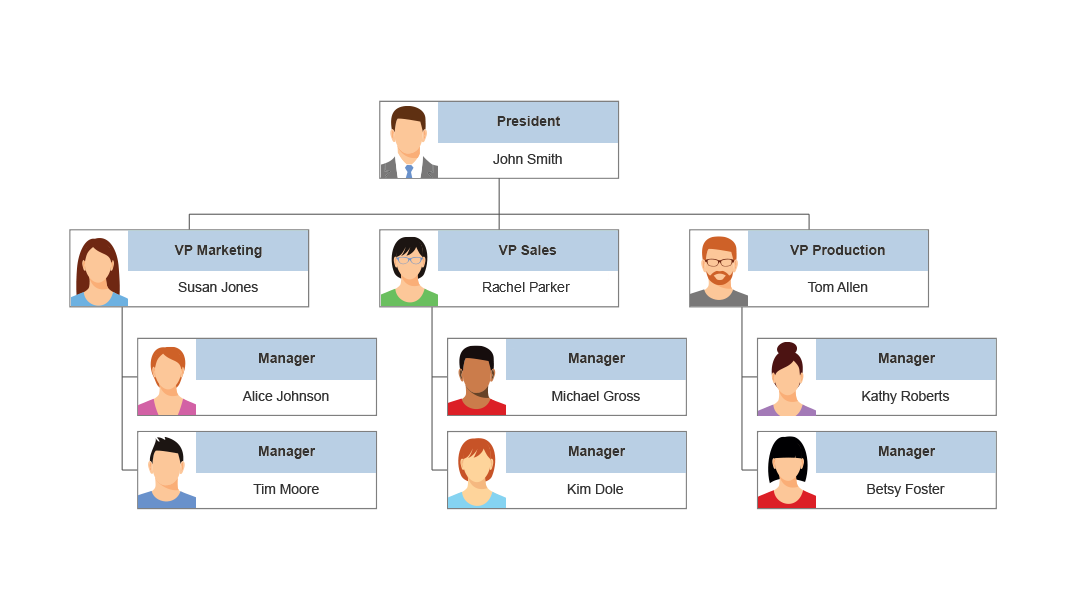
**Answer any THREE from the FIVE problems. Each problem worth 50 points.**

Name\_\_\_\_Mike Pendleton\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BID\_\_\_\_\_\_\_\_\_ 1058201 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1: Consider the Spare of Security and the IDPS (book Figure 4-1). Redraw this figure and create an IDPS for “Health Care Information System”.**



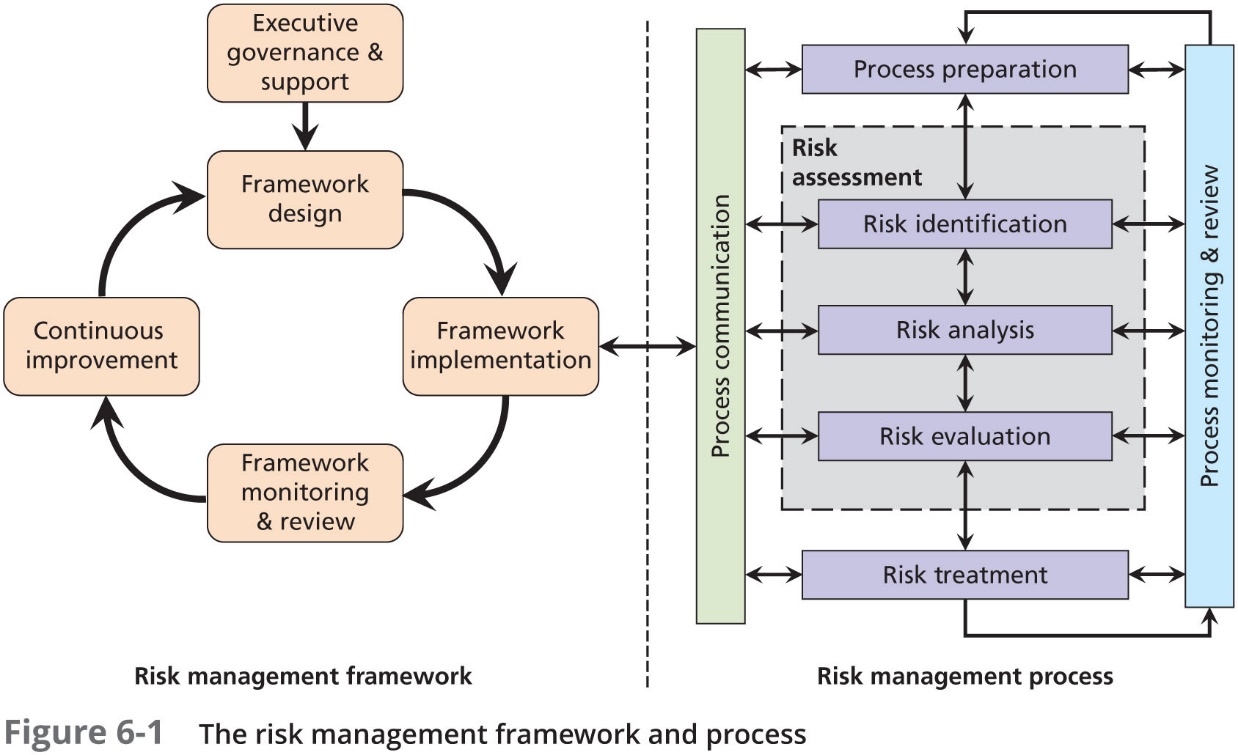
**Q2: The “BBB” Oil marketing company has the following organization chart. How do you classify the company and how will you add the information security branch in this chart. Explain the rational of doing so.**



Source: <https://mauwzola.com/topic/ideas/ideas/>

I would consider this a Hierarchical Structure. I would add the branch along the side of vp production. The security branch would report to the president for this example. The reason why, would be the business use case, the security team would need to be involved with all departments and the decisions should come from both the president and the related branches. If the security branch was under sales for instance, then there would not be an easy structured way to communicate with approvals to the other business units.

**Q3: Given the risk management framework and the process as in the book figure 6-1, expand the risk management process with at least five decision points for an organization have international online trading partners. You can assume any treading industry/company.**



1. Where to store the information that can be accessible by all partners? Ie datacenter, or cloud solution

2. How can the information be accessed by all partners or will some partners have limited access?

3. How to implement the systems full design and structure including disaster recovery?

4. How often should the framework be monitored and reviewed to ensure constant improvement?

5. Who will support the framework implemented and continue support for future changes?

Q4: Cybersecurity risk management can be completed through a threat/vulnerability/asset (TVA) triplet.

Consider the book figure 7-4 and the equation for cost benefit analysis CBA.

**Single loss expectancy (SLE) = asset value (AV) × exposure factor (EF)**

**Annualized loss expectancy (ALE) = SLE × ARO**

**CBA = ALE (precontrol) − ALE (postcontrol) – ACS**

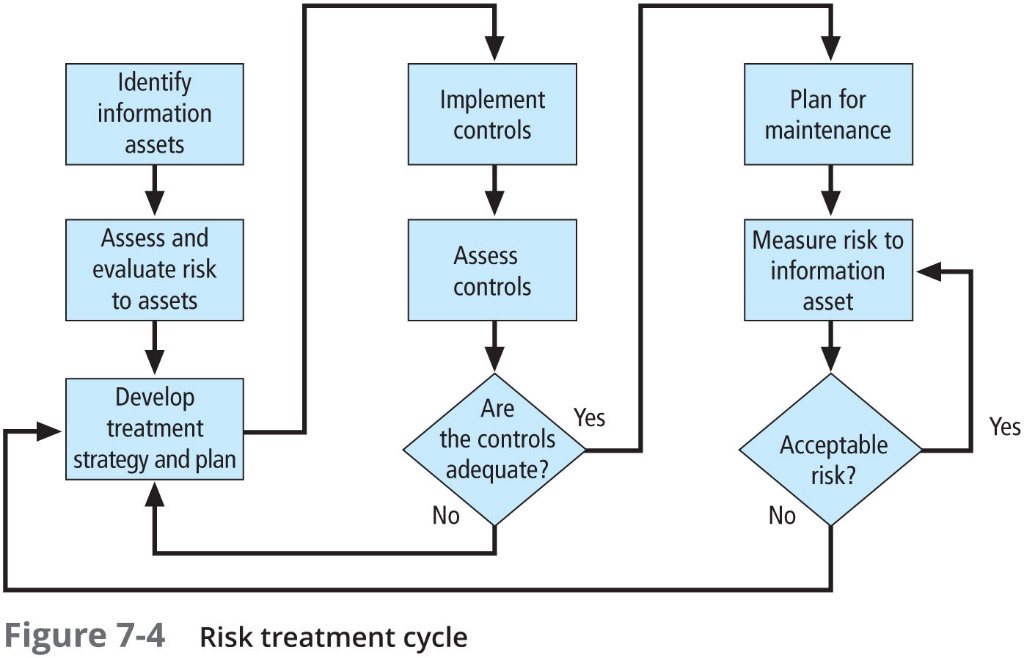
Where:

ALE (precontrol) = ALE of the risk before the implementation of the control

ALE (postcontrol) = ALE examined after the control has been in place for a period of time

ACS = annualized cost of the safeguard

Now, consider a website has an estimated value of $1M, and a cyber-hacking scenario indicates that 15% of the website would be damage in such an attack, calculate the single loss. If the success act of that attack occurs about once every two years, then what is the value of ARO? Also, calculate the overall potential loss per that risk.



Single loss would be 1 million \* 15% = 150,000

The Value of aro would be 0.50 because the occurrence happens once every 2 years

Annual loss expectancy over two years 150,000 \* 0.5 years = 75,000

The overall potential loss for the risk would be 150,000 every two years, or 75,000 every year, until a safeguard cost is stated, I don’t see how we can get the CBA. So this would be the cost until a safeguard was purchased and implemented.

**Q5: Given the NIST security control assessment process in book figure 8-2. Accept or reject all points for WTAMU information system.**

A chart identifies the security control assessment process overview of N I S T. Approved system security plan, ORGANIZATION PREPARATION includes: Implement the security controls in the information system. Notify key organizational officials of impending assessment. Establish and open communications channels among stakeholders. Identify and allocate necessary assessment resources; assemble assessment team. Establish key milestones to effectively manage the assessment. Assemble artifacts for assessment. Approved system security plan, ASSESSOR PREPARATION:  Establish appropriate organizational points of contact. Understand organization’s mission, functions, and business processes. Understand information system structure (system architecture). Understand security controls under assessment and relevant N I S T standards and guidelines. Develop security assessment plan. Obtain artifacts for assessment. ASSESSMENT- Implement security assessment plan. Execute assessment procedures to achieve assessment objectives. Maintain impartiality and report objectively. Produce assessment findings.  Recommend specific remediation actions (corrective actions or improvements in control implementation or in operation). Produce initial (draft) and final security assessment reports. Assessment procedure development: Assessment objectives. Selected assessment methods and objects. Assigned depth and coverage attributes. Procedures tailored with organization and system specific information. Assessment cases for specific assessor actions. Schedule and milestones. ORGANIZATION APPROVAL: Ensure assessment plan is appropriately tailored. Involve senior leadership. Balance schedule, performance, cost. These are the Initial draft report and Final report with organizational annotations. S P 800-53 A and Artifacts lead to Security assessment plan which leads to ORGANIZATION APPROVAL leading to Assessment which in turn leads to Security assessment report and Organization oversight leading to Plan of action and milestones and System security plan. Post assessment process, ORGANIZATION OVERSIGHT: Review assessor findings and assess risk of weaknesses and deficiencies. Consult with organizational officials regarding security control effectiveness. Initiate remediation actions. Develop or update plan of action and milestones. Update system security plan (including risk assessment).