**CIS-481: Introduction to Information Security**

**Module 3 - Information Security Management**

**Exercise #3**

**Team: 3**

**Participants: Dustin Thompson, Bryce Watson, George Flarsheim, Bradley Lawton, Destinee Matsoumou**

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or virtually.
2. Discuss and complete this assignment in a collaborative manner. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.
3. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

**Problem 1** *(10 points)*

This module introduced the NIST Cybersecurity Framework (p. 111). NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. In order to reflect the ever-changing cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is planning a significant update to the Framework in the coming months to CSF 2.0.  
  
Review the current CSF 1.1 Quick Start Guide, linked below:  
  
<https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide>   
  
and choose one of the five key Functions (**Identify**, **Protect**, **Detect**, **Respond**, **Recover**). For your selected key function, briefly describe the main activities associated with this (one) function.

The first essential function of the NIST Cybersecurity Framework is Identify. One main activity of the Identify function is identifying critical systems, assets, data, and capabilities. Some examples are a website customers use to process payments, secure customer data, or ensure employees and customers can digitally interact reliably with each other. Another activity is understanding where information is going. Knowing where your data is coming from and its use is vital. Having documentation on hardware and software currently being used in your organization is also essential. Keeping track of computers and software employees use is critical to secure vulnerabilities. Putting in place cybersecurity policies is also crucial. These policies should identify how systems will be protected and what they are protecting, including other risks like financial or time-loss. The final activity of the Identify function is to identify all threats, vulnerabilities, and risks to assets. It is important to determine who is a potential enemy and what weak points the organization has that the enemy might want to exploit to gain access. Identifying threats and vulnerabilities will help develop a plan to reduce the risk to assets.

**Problem 2** *(15 points)*

The University of Louisville’s [Information Security Office](http://louisville.edu/security) maintains the University’s information security policies, standards, and procedures. Click on the following URL for an overview:

<http://louisville.edu/security/policies/overview-of-policies-and-standards>

The current list of UofL Information Security Office Policies & Standards can be reviewed here:

<http://louisville.edu/security/policies/policies-standards-list>

1. From the above list, look for which policy is serving as the Enterprise Information Security Policy (EISP) as discussed in your text. What is its policy number (ISO PSxxx) and name? When did it take effect? How often is it supposed to be reviewed? When was it last reviewed? Is this consistent with the policy’s stated timeline for review? *(5 points)*

The EISP is, ISO PS001 Information Security Responsibility, and it took effect on July 23, 2007. The policy states to be reviewed annually. It was last reviewed on June 23, 2022. This is consistent with the policy of an annual review; however, there were no reviews for 2019 and 2020.

1. From the above list, look for a policy that would be an example of a Systems-Specific Policy (SysSP). What is the policy number (ISO PSxxx) and name? Is this of the Managerial Guidance, Technical Specifications, or Combination SysSP type? *(5 points)*

An example of a SysSP is ISO-017 v2.1, Firewalls – IT Division Policy. The Firewalls policy seems to be a combination of managerial guidance and technical specifications. An example of managerial guidance is the policy addressing the behavior of employees with the requirement of more than a single password to manage firewalls. Technical specifications are many and mention the blocking of many ports, remote procedures, services and commands.

1. From the above list, look for a policy that would be an example of an Issue-Specific Policy (ISSP). What is the policy number (ISO PSxxx) and name? Is this of the independent, comprehensive, or modular ISSP type? *(5 points)*

Policy ISO PS021 Voice Mail is an independent ISSP since it only covers one issue. It covers the operation of the University's voice mail system including permissible uses of the systems, the risks a user takes by agreeing to use the system, and consequences of not following voice mail policies for the University.