Unit 5 Risk Management Associations

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**January 10, 2023**

**Part 1**

The National Institute of Standards and Technology Special Publication 800-37 is a document synthesized to provide a framework for risk management. It is separated into three main chapters with appendices following them (The National Institute of Standards and Technology, 2018). The first chapter is an introduction going over key information such as background information, the purpose of the document, and target audience. The second chapter details additional information such as organizational elements that will be elaborated upon in chapter three elements and requirements. The third chapter is dedicated to the process of risk management itself. It serves as a broad outline of different steps in the risk management process to adhere to as a framework for organizational life cycles. This itself is also organized in seven categories, or steps (The National Institute of Standards and Technology, 2018). Firstly, the “prepare” category Details critical activities of an organization at different levels to prepare an organization for security and privacy vulnerabilities while utilizing this framework. The “categorized” category is dedicated to determining risk factors with association to their impact on an organization and the assets it controls, or has access to. This may not be limited in scope to the organization itself, as assets may be far reaching. Thirdly, the “select” category details the implementation of controls that would be required In order to maintain the validity and security of organizational operations. This step is a precursor to the next, the “implement” category. Implementation overseas the creation of such controls and the organization of creating the controls within the life cycle of the body utilizing this framework. This is further elaborated upon in the “assess” step. This scan identifies the control implementation from the previous step and cross examines the implementation with the expected results detailed by security officers. It is then examined to see if the controls have the desired effect maintaining security and privacy within the organization. This is followed by the “authorized” step. During this step senior management is called to determine whether or not risk factors remain acceptable, and by doing so increases the accountability of employees with respect. Finally, the monitor step maintains awareness with regards to risk factors by keeping an ongoing look at the securities within an organization, and how the controls affect current circumstances and presentations. Utilizing such a framework can prove beneficial to a company in numerous ways. Organizational coherence is particularly important in times of stress. Utilizing a framework as detailed as Special Publication 800-37 can provide an organization with a detailed list of prevention and response actions to adhere to in such times of stress. Not only that, but security is also to be gained from utilizing this framework. Due to the peer reviewed nature of this document, revisions may be stacked on top of this framework in order to further bolster the security gained overall, unless the peace of mind of all those attached to the organization that is utilizing such a framework. Cybersecurity is a vastly growing discipline, and adaptability is required in order to survive. Rigorous and thorough frameworks may be required to adapt, but also an individuality is accustomed in any organization. Because of this, this framework is just that; it is a list of resources to be altered at the behest of the organization that requires it. This framework may be altered in any way to accommodate unique risks posed to an organization.

**Part 2**

**Discuss the different categories of security controls and give examples.**

Security controls come in many different forms. They are used to deter numerous different disciplines of malicious attempts to gain access to data that should be confidential. Although there are many different types they can be categorized into three main theories (University of Massachusetts Amherst, 2024). Firstly, technical controls oversee digital implementations of barriers that may prevent malicious actors from gaining access to confidential data. This could come in the form of something as simple as a configuration list. This keeps in access log of which user may be granted access to which files on a given network. A second category of controls are administrative security controls. An example of such a control would be an acceptable use case policy. This policy would detail how to use equipment that the organization oversees. The third type of security controls would be physical security controls. This could be any implementation of a keypad leading into a server room that requires a specific code to be entered in order to gain access. These specifically exist physically to act as a real barrier to prevent an individual from physically entering a premises. These controls can be paramount to the success of an organization, and must be used in tandem with one another.

**Give an everyday example of risk analysis that you do every day.**

Whether we think about it or not, risk assessment is part of our every-day activities. For example, I have had some relatively stern conversations with my parents regarding the way I drive. I will not turn right on a red light at certain intersections that may introduce confusion to those around me, or may be busy enough to warrant a stop. This is a risk assessment that I have done consciously, and do not deviate from. Certain risk assessments are derived from previous experiences but that particular risk assessment and action plan has thankfully just been derived from my personal logic, and no collision experience. Another example of risk analysis that I do in my daily life would be Locking the doors on my house after I leave for work. My house has only once been broken into before and as a result I have a routine of verifying the locks on each door are engaged before leaving the house. There are a number of expensive items such as my computer the I am not able to acquire once more should they be stolen. Because of this, I have identified this as a high-risk event with a low probability. Despite the low probability, I still lock my locks routinely.

**Discuss how to design cybersecurity policies that support risk assessment.**

Risk assessment is an important factor in any cybersecurity planning done to date. Because of the various malicious actors present within online technologies in the various disciplines that they employ, risk assessment is paramount to cybersecurity policies. There are a number of methodologies one can employ when designing a cyber security policy in order to support risk assessment. One ideology to consider may be cause and effect. During this ideology it is important to consider how specific elements of a policy may interact with the organization in ways that are either intended or unintended to uncover certain vulnerabilities that may pose problems while employees are carrying out the policy as written (The National Academies of Science, Engineering, and Medicine, 2016). This will help the policy become grounded in real world experiences that take into account how actions within the policy may contribute to vulnerabilities within the organization’s system. Because of this outlook, new information may be uncovered while drafting the policy that could be used to further bolster risk assessment within the policy itself. Because of the grounded nature of this outlook it may be possible to redesign policies within certain disciplines to further focus on organizational vulnerabilities and the risks that they present. Given this, risk assessment may be at the forefront of a cyber security policy being drafted.

# **References**

The National Academies of Science, Engineering, and Medicine. (2016). *Protection of Transportation Infrastructure from Cyber Attacks: A Primer* . Retrieved from The National Academies Press: https://nap.nationalacademies.org/catalog/23520/protection-of-transportation-infrastructure-from-cyber-attacks-a-primer

The National Institute of Standards and Technology. (2018, December 20). *Risk Management Framework for Information Systems and Organizations*. Retrieved from Special Publication 800-37: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

University of Massachusetts Amherst. (2024). *Information Security Controls*. Retrieved from Information Technology Dashboard: https://www.umass.edu/it/security/controls