Risk Management Overview

Instructor: One of the most important elements to ensuring the viability of an organization is understanding its risks, and planning for how to address them.

A formal definition from the national institute of standards and technology describes:

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

In other words, risk management is a proactive process of identifying and planning for, events that may impact the business or its operations. The result of a risk being realized is the risk impact; many of the activities in the management process are focused on limiting the negative impact on the confidentiality, integrity, or availability of information assets.

The assets are a central component of risk. They are the critical elements of a business mission - sensitive information, infrastructure, applications, and people. Each of these assets will have different security requirements for addressing vulnerabilities: any weakness that may be exploited. For instance: bugs in software or misconfigurations, lack of user training. And threats -like malicious code, social engineering, and natural disasters - are events that may compromise the CIA of an asset through; disclosure, modification, destruction. Putting it all together, it's the ability to identify and safeguard from, vulnerabilities that threaten assets.

To aid in prioritizing and better managing risks, there are techniques to calculate risk exposure; a measure of potential loss resulting from an event or activity. Qualitative risk analysis is a relative way to weigh the probability that a given risk will be realized, and the severity if it does. It can be matrixed several ways which can better convey comparisons and urgencies.

Quantitative analysis puts value on a potential loss if an asset is compromised. An exposure factor represents the percentage of loss a threat event would have on a specific asset. Once the exposure factor is established, the single loss expectancy, annualized rate of occurrence, and annualized loss expectancy can be further calculated.

Determining how risks will be addressed is a function of risk management. Options include: Avoid, although its rarely practical to eliminate a critical asset, or all risk exposure; Accept, meaning the risk exposure is tolerable. Most commonly, is to transfer or mitigate Transferring the risk is assigning it to a third party. Outsourcing services to cloud providers for instance; the provider is then responsible for protecting infrastructure and data. Mitigating is applying safeguards or security controls to minimize the risk exposure.

Assessing risk and deciding whether to retain or alleviate it, is the risk appetite. The amount and type of risk an organization is willing to cope with to achieve their business mission. Even after applying controls, a level of risk remains known as residual risk. This remaining threat is included in the risk management processes.

There is a plethora of resources dedicated to risk management, and the implementation of comprehensive enterprise programs. The Risk Management Framework (RMF) is a set of information security standards for federal agencies with a process that integrates security and risk management activities into the system development life cycle.

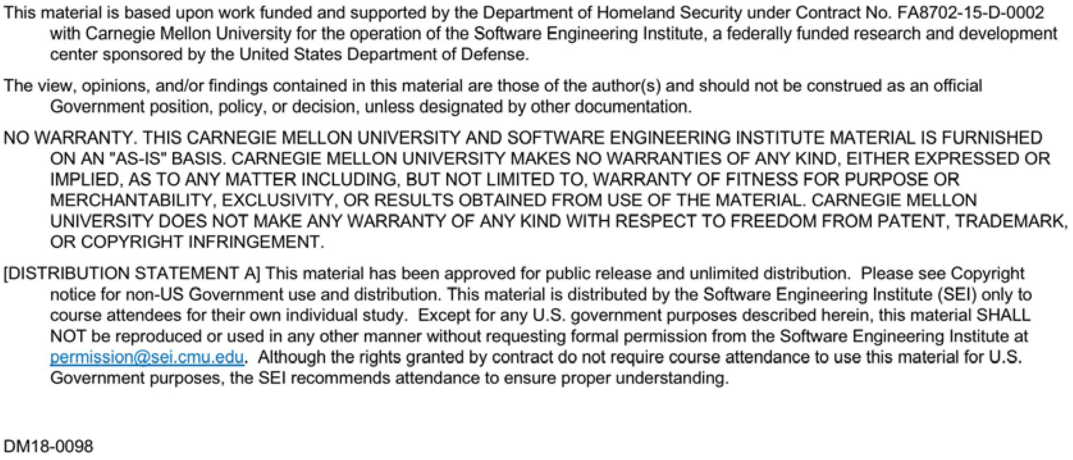
The activities in the RMF for managing risk begin with: Categorize, where the criticality of the information system, and adverse impacts to organizational elements if risk realized, is defined. The information from categorizing is used to select appropriate baseline security controls, that are tailored to specific agency risk. Implement security controls and apply security configuration settings. Those controls are then assessed to determine if they're operating correctly and meeting security requirements; The output of the controls' assessment is examined to Authorize operation if the risk level is determined to be acceptable, and a continuous Monitoring for any signs that may affect the system or controls, and reassess.

Each of the steps have accompanying standards and guidance documentation, for implementation.

Risk management takes a holistic enterprise-wide approach to safeguarding the critical assets that support the business mission. The result of these activities are an understanding of the organizations threat, vulnerability, and risk profile risk exposure. Potential consequences if a threat is realized, with priorities established based on those consequences. Risk mitigation strategies sufficient to achieve an acceptable level of residual risk. And integrating risk management strategies to support critical business functions

Risk management activities are a primary link to organizational processes. Ensuring the survivability of an entity requires understanding the crucial business assets and addressing the threats to each through procedures and policies for safeguards.

Notices



This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098