

Bellevue University

Step 2

Select

Timothy Jelinek

CYBR250-T301

9/9/2023

This pdf goes in-depth about the second step of the risk management framework security life cycle, which is the select step. I chose to research the select step because it isn't the first step and it's not the last step but it's in the middle of the security life cycle. The purpose of me wanting to look at the middle of the cycle is to understand how the two steps around it are related to it and why this step is important. There are guidelines in the NIST SP 800-53 for minimum security requirements for the appropriate level of security control of information systems. The risk executive paragraph talks about organizations needing a good and understandable approach to managing risk which is a good balance between the organization's mission, business functions, and its day-to-day operations. It is important to have a risk executive (function) to provide senior leadership input and guidance over all of the risk management and information security activities of the organization. It is then important for an organization-wide view of the security control selection process to make sure that the risk mitigation is successful. Senior leadership is responsible in the select step for the resulting risk that will be observed by the organization. Senior leadership and organizational support are very important in helping process the select step.

There are other important things to look at when in the select step. FIPS 200 is where it is talked about what the minimum security requirements are and specifies the minimum assurance requirements. This is important in order to satisfy the minimum security requirements and make it possible to be consistent and repeatable. NIST SP 800-53 gives a big catalog of security controls that are used as guidelines for selecting and choosing security controls and minimum assurance requirements needed for enabling organizations to protect their information systems. The information system

owner is the one who selects the security controls that will be used. The process of choosing the security controls includes choosing a set of baseline security codes, adjusting the baseline controls by applying scoping, parameterization, and compensating control guidance, supplementing these adjusted baseline controls with additional controls or enhancements, and specifying minimum assurance requirements where needed. It is important to select the appropriate set of security controls to match the specific security requirements of an organization's commitment to security. Baseline controls are the minimum security controls that are suggested for an information system that is based on the security level of said system. Risk assessments are important because they provide inputs in deciding whether or not the security controls in the baseline protect the organization's assets. These are all important things that are kept in mind during the select step.

Through reading this pdf I have learned all of the important steps and reasons for the steps of the select step. It is important to have senior leadership work alongside the owner of an organization to set the standards of the select step to protect the organization's processes and assets. The organization must be aware of all of the steps and chosen requirements to make sure they don't jeopardize any of the assets the organization is protecting. By setting baselines the organization has a clear blueprint on how they are going to protect their assets and what assets they are going to protect. These baselines will be used alongside the recommended security controls for the information system to keep everything safe. I feel I have chosen the right step to look into as it is a very important one in securing the assets of an organization.

Sources:

"Select Step – Management Perspective",

https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/select/qsg_select_management-perspective.pdf.

Accessed 9 September 2023.