NIST Special Publication

Emmiliia Fedina

University Of Washington Tacoma

Prepared for Dr. Grant

TINFO 463

Spring, 2022

Why there is a need to protect information, systems, organizations, and individuals. In the modern world all the devices and platforms have computers with complex software in common. Security controls are the safeguards that are used to protect important information for the company. NIST publication should serve a diverse audience that includes software engineers, chief information officers, etc. It is complex to manage security and privacy risks, so to make sure it will happen there should be well defined security and privacy requirements for the organization. It is organizations’ responsibility to select the appropriate security and privacy control selection process. The NIST publication rules can also be applied to international organizations. The controls and rules in NIST are reviewed periodically to make sure it produces the updated Information. Requirements and controls are two different words but have a connection. Requirements are something with what organization must comply to. Specification requirements are the requirements that implements part (or all) of control and that may be assessed. Controls, on the other hand, are something that a company chooses and implements. Controls can be used as descriptions of safeguards. Security and privacy controls have a base control section, discussion section, a related control section, a control enhancement section, and a reference section. Some controls are more flexible that lets organization to define more specific values with the control. Iteration and refinement actions allows to add more flexibility. Iteration allows organization to use control several times and apply it in different situations. Discussion section have more information about a control. Related control section addresses a related security or privacy. Control enhancement section provides statements of security and privacy capabilities. There are three types of control: common, system-specific and hybrid control. Common control is the one that can be inherited by multiple Information systems or programs. System-specific controls are the primary responsibility of information system owners. Hybrid control is combination of common control and system specific control. Role of privacy programs is to ensure compliance with current privacy requirement. Trustworthiness means being worthy to be trusted to fulfill specific requirement. Two main concepts of trustworthiness are functionality and assurance. Functionality means to make sure the programs work as it should work. Assurance is the measure of confidence that your program works correctly.

References

Force, Joint Task. “Security and Privacy Controls for Information Systems and Organizations.” *CSRC*, 10 Dec. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.