Nist Control Risk Management

The National Institute of Standards and Technology is an agency under the United States Department of Commerce. Risk management is a NIST control family that has a major impact on how to conduct security in an organization. As the world continues to advance in technology, it's imperative for any organization to plan what they are willing to risk in order to protect their digital assets.

The main purpose of NIST is to promote innovation and industrial competitiveness by advancing standards, measurement science, and technology in ways that advance economic security and improve our quality of life. The non-regulatory agency will provide guidance for any organization to be in compliance with The Federal Security Management Act of 2002. This event requires NIST to develop standards to arrange and secure information based on the level of risk. This mandates all civilian federal government agencies to follow these practices and provides guidelines for other organizations. There are also different standards and practices that apply to agencies that contain classified information such as national security agencies.

There are a couple of risk management components to take into consideration when addressing the risk framework. Framing a risk is about the context in which an organization views the risk. Assessing risk is about finding what risk an organization has and its severity, while responding to risk is about the best course of action. Finally, monitoring risk is about following up with the response and how it impacts the organization. These risk components provide an overall model of how to conduct a risk assessment.

Risk models are a practical concept that is commonly used when it comes to addressing risk in an organization. These models are used to define risk factors, define the relationship between the factors, address the overall level of risk, communicate the level of risk, guide a response to a risk, incorporate organizational risk tolerance, and more. These models provide a risk management strategy or approach to address certain scenarios that can pose a risk that could possibly lead to a vulnerability or threat to an organization.

A threat is any circumstance or event with the potential for unauthorized access, disclosure, dismantling, or any modification of information. Threats are usually sourced from any party that can exploit a vulnerability whether it was intentional or not. Vulnerability is a weakness that could be exploited by any threat source. This could lead to a threat event, which is a damaging event that is caused by a threat source. When conducting risk analysis many threat scenarios will be modeled when addressing these issues. One major factor to consider for risk assessment is the likelihood of occurrence, which is a weighted risk factor based on the probability that a threat is capable of exploiting a vulnerability.

In risk management, there is a hierarchy that includes three tiers. The first level is the organizational level, the second is the mission/business process level, and the third is the information systems level. A risk analysis can be performed at any level, but the levels will interact with each other. It is important to relate the risk to multiple levels and make decisions in a predictable manner about how each level could be affected. There is a general overview when performing the NIST risk assessment process. The first step is to prepare the assessment by looking at the organization's risk frame, the environment it operates in, how it performs its information processing task, and the organization's risk tolerance. To prepare a risk assessment, it's best to identify a couple of key factors. These factors are identifying the purpose and the scope of the risk assessment. It's also important to identify the assumptions

and constraints for how the risk assessment is being conducted. Finally, It's best to define or redefine the risk model and assessment approach for the risk assessment.

The next step is to conduct the assessment. This is where the observer identifies the threat sources, threat events, vulnerabilities, and determines the threat likelihood along with the adverse impacts. Once the assessment is completed, this is where the information from the assessment should be shared. The next step is to communicate the results securely with the organization and determine what the appropriate response should be. This information can be shared with an organization's stakeholders along with any other parties that are involved. It is also best to share the results with supporting evidence that the organization was in compliance with their policies to determine if any further action is necessary.

Finally, it is important to maintain the assessment by first looking at changes in the risk environment and understanding the reasons for any changes. Another task would be to determine how effective the responses are when addressing a certain risk. Then, it's best to verify if the assumptions held up over time and update the assessment itself based on varying circumstances. This is where the observer can monitor if the organization is in compliance to ensure various regulatory requirements with NIST.

In conclusion, NIST provides standards for any organization that intends to protect its digital assets. Risk has to be taken into consideration if an organization is willing to adapt to the modern world. Risk management is the key to protecting an organization and without it, an institution can be exploited.

Sources:
Nist Controls: https://www.nist.gov/director/pao/nist-general-information

Risk: https://www.youtube.com/watch?v=dZZyYA6si10&t=1099s

Risk Management: https://en.wikipedia.org/wiki/IT_risk_management

Risk Assessment: https://www.youtube.com/watch?v=VR0PvwKpDUA&t=26s

Risk Management: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf