How flexible is NIST SP 800-53? What controls are most important to prevent cybersecurity threats?

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. One of its various publications NIST SP 800-53, address the urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure, ensuring those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States.

The NIST SP 800-53 also establishes controls for federal information systems and organizations. According to the publication, the use of these controls is mandatory, in accordance with the provisions of the Federal Information Security Modernization Act (FISMA), which requires the development and maintenance of minimum controls to protect federal information and information systems. The controls can be implemented within any organization or information system that processes, stores, or transmits information. Additionally, the publication is intended to help organizations manage risk and to satisfy the security and privacy requirements in FISMA.

When it comes to flexibility, the publication provides a flexible methodology to manage information security and privacy risk. That is, it provides a flexible catalog of security controls for systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies. Additionally, the controls in the catalog are independent of the specific process employed to select those controls. Such selection processes can be part of an organization-wide risk management process, a life cycle-based system engineering process, or risk management or cybersecurity framework.

According to NIST SP 800-53, the controls that are most important to prevent cybersecurity threats are part of the catalog of security and privacy controls. They can be effectively used to protect organizations, individuals, and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios. They vary from technical access controls to security awareness and training and policies and procedures. These controls can also be used to demonstrate compliance with a variety of governmental, organizational, or institutional security and privacy requirements. These controls are also part of the NIST cybersecurity framework that includes the five functions: Identify, Protect, Detect, Respond, and Recover.

References

https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

https://www.nist.gov/cyberframework/online-learning/five-functions