

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a voluntary framework, consisting of a set of standards, guidelines, and practices developed in the interest of reducing or managing cybersecurity risk. Originally released in 2014 and updated subsequently, the framework is a structured approach to protecting digital utilities. There are five core functions; Identify, Protect, Detect, Respond, and Recover help organizations to develop comprehensive cybersecurity strategies.

The NIST CSF was created as a result of Executive Order 13636, which President Obama signed in 2013. This included an executive order designed to increase the security of critical infrastructure sectors like energy, finance, healthcare, and transportation in the face of rising threats from cyberattacks. This framework was intended to be a high-level, technology-neutral set of best practices to help organizations regardless of size, sector, or industry better align their cybersecurity efforts while also addressing where those efforts could and should do better. The NIST CSF was developed based on the consensus that a common language and framework were needed for how organizations can assess, communicate, and manage cybersecurity risk. Before the NIST cybersecurity framework, organizations had to figure out their cybersecurity policies, resulting in inconsistent and generally de-centralized security postures.

Any institution, regardless of size or sector, can apply the NIST CSF. It is a flexible methodology that enables organizations to design customized security infrastructures based on their individual requirements and risk profiles. The five main functions of the framework give a full roadmap to cybersecurity management. The Identify function assists organizations in understanding their operational environment, managing cybersecurity risks, as well as assessing and managing assets. The Protect function is all about safeguarding critical operations, including access control,

employee training, and data security. Detect focuses on making sure that security events are detected and investigated in real time. The Respond function assists organizations in determining measures for a cybersecurity incident, such as communication and mitigation strategies. Lastly, Recovery is about resilience, planning, and improvements in order to restore normal operations. When applied together, these functions allow organizations to proactively address cyber threats and respond to them as they arise.

The NIST CSF is part of the larger national strategy to improve cybersecurity resilience and safeguard critical infrastructure. It works in conjunction with other federal initiatives, including those set forth in the Federal Information Security Modernization Act (FISMA) and those from the Cybersecurity and Infrastructure Security Agency (CISA). The framework also enables organizations to fulfill various industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

The NIST CSF has been embraced by a number of countries and organizations on the international stage. Its flexible, risk-based approach aligns with global initiatives to standardize cybersecurity practices. The framework has already inspired some cooperation such as the national cybersecurity strategies of Australia and Japan.

The NIST CSF has been selected for this analysis due to its wide-ranging applicability and adaptability, as well as its substantial impact on the national and global cybersecurity landscape. This prescriptive, practical guidance in addressing cybersecurity risk encourages innovation and flexibility. Moreover, its focus on public-private partnership makes it a key instrument for fortifying the global cyber security landscape. With its flexible framework of guidelines, the

NIST CSF has transformed into a go-to reference for organizations aiming to shield themselves from a constantly changing environment of cyber threats.