NIST Cybersecurity Framework Solution

NIST CSF

At-a-Glance

The Cybersecurity Enhancement Act of 2014 directed the National Institute of Standards & Technology to develop a voluntary, risk-based, framework focused on cybersecurity standards and best-practices in support of critical infrastructure management. The resulting framework provides a common language for organizations to communicate how they view cybersecurity risk while providing flexibility to accommodate their unique activities, desired outcomes, and risk management approaches.

Solution Key Features

- **Purpose-Built for NIST CSF**
- **Integrated Risk Management Design**
- **NIST CSF Core mapped to Rsam harmonized control content**
- **Cyber Security Summary and Executive Reports**
- **Modular approach provides flexibility while minimizing implementation costs**

An Ever-Changing Landscape

Cybersecurity leaders have their hands full. They face a diverse and ever-evolving threat landscape. They have little certainty about which technologies are the best investments. Challenges exist with clearly understanding, validating, and articulating the organization's risk posture. At any time CISOs must be ready to report status to the Board of Directors and other stakeholders.

Unlike the many other risk management approaches that have been introduced over the years, the NIST CSF is gaining significant traction. A recent Rsam survey revealed that **87% of InfoSec leaders** indicated they plan to incorporate the framework into their risk and compliance strategy.

While the NIST CSF is detailed and well-documented, it is not prescriptive making it difficult for many organizations to operationalize it. Every organization has different risk tolerance levels and varying levels of cybersecurity maturity. Organizations need a technology solution specifically designed to support the CSF while providing flexibility to adapt to their unique environment.

Rsam NIST Cybersecurity Framework Solution

The Rsam NIST CSF Solution helps operationalize the NIST CSF in a manner that works for you. The solution is specifically designed to support cybersecurity assessments using the NIST CSF framework principles of the core, profile, and implementation tiers. Rsam offers five complementary approaches to implementing the framework based on an organization's security investments and maturity. Each approach builds upon the previous and provides increasing levels of confidence and defensibility.

Approach 1: Link risks to NIST CSF categories to achieve an aggregate view of risk across all categories. This enables organizations to set different thresholds across the categories and talk about risk in terms the business understands.

Approach 2: Organizational-level risk assessments of current and target tiers provide visibility of your security posture across the enterprise. Leaders obtain the organizational perspective of security gaps providing a roadmap to prioritizing cybersecurity initiatives.

Approach 3: Leveraging Rsam's cross-mapped controls, asset-level risk assessments dynamically provide sub-category specific feedback of profile-related assets in support of tier evaluations. This provides extraordinary flexibility for organizations to continue to use tried-and-true control frameworks in their implementation of the NIST CSF.

Approach 4: Integrated continuous control testing supports residual risk determination across the NIST CSF core domains. Empirical test results validate maturity levels, organizational performance, resource allocation, and security technology investments.

Approach 5: Incorporate any meaningful data into your tier evaluation/validation through key risk and performance indicator integration. Threshold-based automated indicators provide point-in-time analysis and trending information further supplementing your ability to monitor security and operational metrics and make informed decisions.

 | www.rsam.com | /company/rsam | @RsamGRC | +1-800-920-Rsam (7726)