NIST CSF COMPLIANCE SCORECARD: YOUR GUIDE TO CYBERSECURITY READINESS

Cybersecurity is vital for businesses of all sizes, protecting sensitive data, intellectual property, and customer trust. The NIST CSF provides a structured approach to cybersecurity, helping organizations identify, protect, detect, respond to, and recover from cybersecurity threats. The scorecard offers a quick and high-level assessment of cybersecurity readiness, enabling organizations to identify strengths and weaknesses in their cybersecurity practices.

This guide will explore how the scorecard can help you evaluate and enhance your cybersecurity posture.

WHAT IS NIST CSF?

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a trusted roadmap for keeping your digital world safe. Created by experts, it's a simple yet powerful tool that helps businesses, big and small, tackle cybersecurity challenges.

CORE FUNCTIONS ASSESSMENT

The core functions of the NIST CSF form the foundation of cybersecurity readiness assessments:

Identify: Assess your organization's ability to identify cybersecurity risks, including identifying assets, data, and potential vulnerabilities.

Protect: Evaluate measures against identified risks, such as access controls, encryption, and data backup procedures.

Detect: Review capabilities for detecting cybersecurity events, including monitoring systems, anomaly detection, and incident response protocols.

Respond: Assess your organization's response to detected incidents, including incident containment, communication protocols, and incident reporting procedures.

Recover: Evaluate your organization's ability to recover from cybersecurity incidents, including data recovery, system restoration, and post-incident analysis.

IMPLEMENTATION TIERS EVALUATION

The NIST CSF includes four implementation tiers, reflecting varying levels of cybersecurity maturity:

01. **Partial:** Assess basic cybersecurity measures in place, including ad-hoc security practices and limited risk awareness.

02. **Risk-Informed:** Review risk management practices and informed decision-making processes, integrating cybersecurity into organizational risk management.

03. **Repeatable:** Evaluate consistent and repeatable cybersecurity processes with established policies, procedures, and controls.

04. **Adaptive:** Assess proactive and adaptive cybersecurity practices, including continuous monitoring, threat intelligence, and response automation.

NIST CYBERSECURITY FRAMEWORK COMPLIANCE SCORECARD

Implement our customizable scorecard template to conduct your cybersecurity assessment. This template is designed with sections for each core function tier, accompanied by scoring and interpretation. Identify strengths and weaknesses in your cybersecurity practices, enabling you to prioritize areas for improvement and enhance your organization's cybersecurity posture.

FUNCTION 1: IDENTITY

- **Category 1.1: Asset Management**
  - Subcategory 1.1.1: Asset Inventory **SCORE:____**
  - Subcategory 1.1.2: Asset Management Strategy **SCORE:____**
- **Category 1.2: Business Environment**
  - Subcategory 1.2.1: Organizational Mission **SCORE:____**
  - Subcategory 1.2.2: Legal/Regulatory Requirements **SCORE:____**
  - Subcategory 1.2.3: Risk Management Strategy **SCORE:____**

FUNCTION 2: PROTECT

- **Category 2.1: Access Control**
  - Subcategory 2.1.1: Access Control Policy **SCORE:____**
  - Subcategory 2.1.2: Account Management **SCORE:____**
- **Category 2.2: Awareness and Training**
  - Subcategory 2.2.1: Security Awareness Training **SCORE:____**
  - Subcategory 2.2.2: Security Training for New Employees **SCORE:____**

FUNCTION 3: DETECT

- **Category 3.1: Anomalies and Events**
  - Subcategory 3.1.1: Anomalous Activity Detection **SCORE:____**
  - Subcategory 3.1.2: Event Detection **SCORE:____**

FUNCTION 4: RESPOND

- **Category 4.1: Response Planning**
  - Subcategory 4.1.1: Response Plan Development **SCORE:____**
  - Subcategory 4.1.2: Incident Management Policy **SCORE:____**

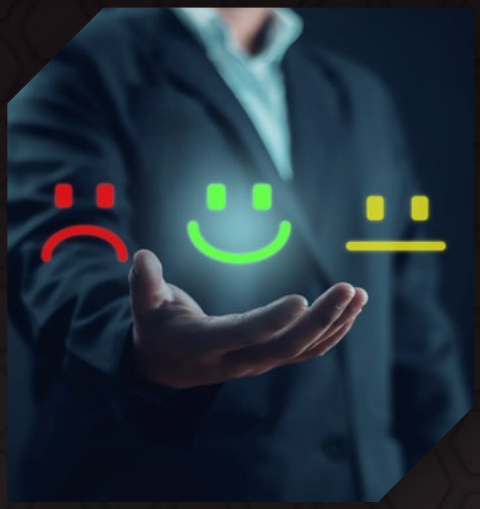
FUNCTION 5: RECOVER

- **Category 5.1: Recovery Planning**
  - Subcategory 5.1.1: Recovery Plan Development **SCORE:____**
  - Subcategory 5.1.2: Recovery Coordination **SCORE:____**

SCORING KEY:

- 0: Not Implemented - **Risk: High**
- 1: Partially Implemented - **Risk: Medium**
- 2: Fully Implemented - **Risk: Low**

Note: Assess each subcategory based on its implementation level within your organization. Score accordingly.



NEXT STEPS

After your organization has been scored - whether it's low, medium, or high - understanding the implications for your business is crucial.

- A **low** score indicates that your cybersecurity measures are relatively strong, with minimal vulnerabilities and risks identified. However, it's still crucial to remain vigilant and proactive in maintaining your security posture to prevent any potential threats.

- A **medium** score suggests that while your cybersecurity measures are adequate, there may be some areas where improvements can be made. This could include strengthening access controls, updating software patches, or enhancing employee training programs to mitigate potential risks effectively.

- On the other hand, a **high** score indicates that your organization faces significant cybersecurity risks and may have several vulnerabilities that need immediate attention. This could include outdated software, weak password policies, or inadequate network security measures. In such cases, it's essential to prioritize remediation efforts and implement robust security controls to reduce the risk of a data breach or cyberattack.

No matter where your cybersecurity risk falls on the spectrum, our team at FUSE3 is here to provide personalized recommendations tailored to your organization's needs. Contact us today for expert support and guidance on your cybersecurity journey.

SPEAK WITH AN IT EXPERT!