IT INSIGHTS
ROCHESTER NEW YORK

585-283-7102
info@itinsightsroc.com
itinsightsroc.com

NIST Cybersecurity Framework compliance guide

IT Insights can help you achieve and maintain NIST CSF compliance.

Following Federal suggestions and meeting the NIST Cybersecurity Framework (CSF) is a great goal for any organization as it grows its IT infrastructure, policies, and security practices. Mandatory for all government contractors and subscontractors, this is a best practice for organizations that fall outside that scope. While the NIST framework has been in place since 2014, new guidelines have been released to better accommodate small and midsize business's (SMBs) ability to comply with these standards.

WHAT IS THE NIST CSF?

The NIST CSF is a collection of voluntary best practices and guidelines that organizations can follow to help reduce their cybersecurity risk. The practice and application of this standard is outlined in categories defined to the right, with requirements that fall into each category. These serve as a roadmap to ensure that an organization is covering any vulnerabilities or problematic behavior from all angles.

WHY SHOULD MY ORGANIZATION CARE?

Over 40% of SMB's experienced a cybersecurity incident in 2023. The average cost of a breach in the SMB market is approximately $2 million. Unfortunately, there is no silver bullet to this problem. The best course of action is to adopt some type of risk management framework, such as NIST CSF, to reduce the cybersecurity risk to the organization.

HOW DOES IT INSIGHTS HELP?

As an MSP, it is our responsibility to ensure we provide the correct people, tools, and processes to address the entire attack surface. Cybersecurity is a layered approach, and our services are carefully evaluated, deployed, and managed to ensure we help our customers minimize their cybersecurity risks. Take a look at the matrix on the following page to see how IT Insights is addressing the various functions of NIST CSF 2.0.

WHAT IS NEW WITH NIST CSF 2.0?

On Feb. 26, 2024, NIST released CSF 2.0 which builds on previous versions. Previous versions of CSF were composed of five functions, including Identify, Protect, Detect, Respond, and Recover. CSF 2.0 added a sixth function, Govern, which aims to highlight the importance of governance and supply chains.

In each compliance pillar, there are a number of controls with varying levels of complexity. The table below identifies the NIST requirements and how they align with IT Insights services.

	IT INSIGHTS OFFERING							
FUNCTION	Remote Monitoring and Management (RMM)	Account Management	Managed Services	Policy and Procedure Development	Procurement	Table Top Exercises	Business Continuity and Disaster Recovery (BCDR)	Instrusion Detection and Prevention Systems (IPS/IDS) within Firewall
GOVERN								
Establishes and communicates cybersecurity risk management strategy, expectations, and policy while monitoring them		✓	✓	✓	✓			
IDENTIFY								
Identification of resources, assets, systems, and data that exist within the organization to help ensure effective use of the framework and with defense and remediation efforts	✓	✓	✓	✓	✓			
PROTECT								
Protection of resources, assets, systems, and data against cybersecurity incidents to curb the adverse effects of possible cyber attacks	✓	✓	✓	✓		✓	✓	
DETECT								
Implementation and development of needful activities to quickly identify the affordance of any cybersecurity breach	✓	✓	✓	✓		✓		✓
RESPOND								
Development and implementation of activities to take required actions against cybersecurity breaches that have been detected		✓	✓	✓		✓	✓	✓
RECOVER								
Recovery from a cyber attack without interacting with cyber criminals		✓	✓	✓		✓	✓	

IT INSIGHTS SECURITY PARTNERS

Cisco Duo · Graphus, A Kaseya Company · Huntress · ID Agent, A Kaseya Company · RapidFire Tools, A Kaseya Company · Trend Micro

585-283-7102 · info@itinsightsroc.com · itinsightsroc.com