# IGNYTE NIST CSF DATA SHEET

**Ignyte Assurance Platform: Simplifying NIST CSF Compliance – Build a strong defense and continuously monitor how your organization's security posture aligns with NIST CSF with minimum management costs over time.**

## OVERVIEW

The NIST Cybersecurity Framework (CSF) developed for critical infrastructure has been around for four years now. In 2017, President Trump signed the Cybersecurity of Federal Networks and Critical Infrastructure Executive Order that requires all federal agencies to begin running risk management, reporting, and recovery programs under the NIST Cyber Security Framework (CSF). The order is in line with the US policy to support growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving the nation's objectives in cyberspace.

Today, NIST CSF is widely adopted across both private and public organizations of all sizes. NIST CSF is crucial for your organization since it helps you establish what needs to be protected and how to implement safeguards to detect, respond, and recover from incidents.

NIST CSF can also be used to help contractors manage NIST SP 800 – 171 standard compliance, which is a requirement of the federal government for all organizations that work with controlled unclassified information (CUI). NIST suggests using CSF and NIST SP 800-171 together for improved results.

In 2018, the U.S. Commerce Department's National Institute of Standards and Technology released version 1.1 of the popular framework for improving Critical Infrastructure Cybersecurity. The new release significantly reflects the success of the public-private model for addressing cybersecurity issues. It advances the existing collaborative effort involving the government, academia, and private industry. Key areas of focus included in version 1.1 include:

1. Authentication and identity
2. Self-assessing cyber security risk
3. Managing cybersecurity within the supply chain
4. Vulnerability disclosure

## OUR SOLUTION

Ignite understands that when it comes to NIST CSF implementation, there is not a one-size-fits-all approach. We examine your unique business risk, regulatory requirements, resource constraints and then take those factors into consideration while automating NIST CSF compliance.

Ignyte Assurance Platform automatically maps information security programs to the NIST CSF framework, enabling organizations to rapidly assess their cybersecurity maturity and identify crucial trends. The solution is updated regularly to help organizations to identify, detect, and respond to changes while communicating observations with stakeholders, such as senior management and audit teams.

## OUR APPROACH

Ignyte engineers are experienced in NIST-based assessment, especially the NIST CSF. We apply this knowledge to help your business to comply with the framework.

Our solution uses the following approach to help you achieve NIST CSF compliance:

i. **Identify:** we help your organization identify the data and assets that store, transmit, and process that information. Ignyte helps in developing an inventory of data, devices, applications, and the underlying infrastructure that process and store the data. Identifying the data and other assets helps discover the threats and vulnerabilities in your business environment.
ii. **Protect:** after establishing what should be protected, we help put measures in place to secure information. Ignyte Assurance Platform guides you in implementing a layered approach to security to ensure that the device, application layer, and connectivity layer are well protected.
iii. **Detect:** Our solution helps you to easily find threats and bad actors. Ignyte Assurance Platform guides your organization in developing and implementing the appropriate activities to identify the occurrence of a cybersecurity incident
iv. **Respond:** Ignyte helps your business develop an efficient and effective response plan that features appropriate actions to be taken regarding a detected security event.
v. **Recover:** In case your organization is disrupted by a breach, Ignyte guides in the process of restoring business and IT operations, including investigating the incident and ways security mechanisms can be enhanced to prevent future threats.


## OUR BENEFITS

Reduced compliance burdens: Ignyte Compliance Management and Oversight model provides a powerful workflow feature as well as integration with other platform modules and third-party applications to automate compliance related processes. You can automatically map your information security to the NIST CSF to rapidly assess your security maturity

Effective Gap Identification: Ignyte Assurance Platform enables quick analysis to help highlight gaps between your security programs and critical components of NIST CSF. Gap analysis reports can be shared with the management and third parties

High Usability: Ignyte Assurance Platform provides input screens that you use to organize the data needed for CSF assessment process

- Executive Insight: access Ignyte real-time dashboards and reports designed to provide executive-level compliance insight including granular metrics for audit and compliance professionals. We also provide resources for NIST CSF compliance requirements to guide you during the compliance process.
- Track Ongoing Compliance: mitigate your organization's ongoing risk of potential violations. Measure and validate ongoing compliance through alerts triggered from changes to your internal environment. Continuously monitor your security performance and that of your vendors to ensure they align with NIST CSF
- Tailored Solution: our vendor-independent approach allows us to offer in-depth services and custom-made recommendations to ensure you get desired ROI.
- Improved Reporting: Ignyte Assurance Platform generates the required reports and documents when needed.

## WHY IGNYTE?

Do you struggle to understand your true state of cyber security of cyber risk? Does your organization face a challenge in managing complex security environment? How can you implement the NIST CSF in your organization? As you ponder about these questions, cybersecurity threats are continuously increasing, and there is no better time than now to implement the CSF.

We will walk with you to help position your business as a leader in forward-looking cybersecurity practices. Ignyte Assurance Platform is specially developed to address NIST CSF compliance automation, which is an effective solution for federal government contractors who use the framework to manage the mandatory NIST SP 800-171 standard. Ignite also provides appropriate evidence and artifacts to prove compliance when necessary.

As cyberattacks become more complex, and cybercriminals advance in their skillset, repelling them will remain a daunting task, especially without a cohesive strategy. NIST CSF provides the standardized practices to ensure enhanced protected of all cyber assets.

### Get Started Now!

Give us a call to setup a demo today at https://ignyteplatform.com/request-a-demo/

REQUEST A DEMO

### ABOUT IGNYTE ASSURANCE PLATFORM

Ignyte Assurance Platform™ is a leader in collaborative security and integrated GRC solutions for global corporations. For corporate risk and compliance officers who depend heavily on the protection of their resources, Ignyte is the ultimate translation engine for simplifying compliance across regulations, standards and guidelines. The Ignyte platform is used by leading corporations in diverse industries; such as, Healthcare, Defense, and Technology. Ignyte is headquartered in Miamisburg, Ohio and can be reached at **www.ignyteplatform.com**. PH: **1.833.IGNYTE1 or (937) 789-4216**