ignyte™
ASSURANCE PLATFORM

IGNYTE ASSURANCE PLATFORM™

THE NEXT ERA OF CYBER ASSURANCE IS HERE

Systematize, integrate, and assure corporate cybersecurity activities across the enterprise.

ignyte™
ASSURANCE PLATFORM

IGNYTE ASSURANCE PLATFORM OPERATIONALIZES ALL SIX STEPS OF THE NIST RMF TO GET YOU TO ATO FASTER

AT A GLANCE

- Simplify IT risk management and RMF Compliance, freeing corporate resources to focus on core business activities.

- Management of all RMF compliance activities and automation of the work flow process from system registration through system decommissioning.

- Maintenance of an enterprise baseline for security controls, which is stored in the Ignyte repository and updated with industry standards.

- Eliminate the need to manually track adherence to IT processes and lift the administrative burden.

- Achieve measurable risk reduction through simplified risk analysis and management that provide clear visibility into your organization's risks

OVERVIEW

Organizations working with the US Federal government are forced to adopt one or more security frameworks in order to meet compliance initiatives. A critical framework is the NIST Risk Management Framework (NIST RMF) which is the ultimate framework for any security officer explicitly and intently attempting to adopt high level controls and link them down to actual system level settings. However, most security officers do not like this framework due to its high level of complexity compared to other frameworks that allow for much more interpretation. The core content of this framework comes from NIST Special Publication 800-53 (controls catalog). It is also important to note that many professionals in the industry do not have a clear understanding between NIST CSF and NIST RMF. They most often use these frameworks interchangeably in their communication. NIST RMF has over 900+ controls and each control has many sub-requirements whereas CSF is only about 100 high level requirements and is not used formally for any certification & accreditation of high security systems.

Integrated GRC
Integrate seamlessly with other applications and existing business processes.

Cut Costs, Not Corners
Reduce errors, improve efficiencies and reduce security management costs overtime.

Time to Value
Ignyte Assurance Platform is built from the ground up by seasoned experts to get to value fast.

KEY BENEFITS

- Automatically maps other regulations, such as FedRAMP and CSF to existing RMF framework and control sets

- Tiered control architecture

- Tight integration with other Ignyte Assurance Platform modules

- Provides assessment and other compliance related workflows

- Supports both custom and all industry frameworks

- Provides work flow automation

- Monitors System Security During the Entire System Life Cycle

- Provides Real-Time Metrics on Authorization Activities

- Overlays and Artifacts are Easily Accessible

- Provides Management and Accurate and Timely Dashboard on Risk Health

- Data Driven – Policy and Validation Security Controls

- Can Be Easily Updated Across Enterprise or Tailored

- Provides a Collaborative Space for Solving Authorization Problems and Sharing Cybersecurity Principles

RMF & IGNYTE ASSURANCE PLATFORM™ WALK THROUGH

The platform has automated analysis capabilities that automatically maps RMF regulation to your existing control set to ensure ongoing compliance.

RMF STEP 1: CATEGORIZATION

The first step involves performing a risk assessment using NIST 800-30 & 800-60 guidance and completing a risk assessment report. The identified risks are categorized based on their impact due to a loss of confidentiality, integrity, and availability. Ignyte Assurance Platform allows users to register an instance and assigns qualified personnel to different RMF roles. We work with you to understand the organization's system operating environment, intended use, connections to other systems, or any other components that may affect the final security impact level determined for the system.

RMF STEP 2: SELECT SECURITY CONTROLS

The Information System Security Officer (ISSO) will select the security control baselines applicable to the IS. The selection is based upon the results of the categorization. The ISSO can tailor the controls as needed by supplementing, modifying, or tailoring out controls to effectively manage risk for any unique system conditions. The ISSO will then develop a strategy for continuous monitoring of security control effectiveness. Ignyte team helps boost confidence in the fact that the security controls selected within your information systems are effective in their application.

RMF STEP 3: IMPLEMENT SECURITY CONTROLS

This step involves the implementation of security controls and a description of how they will be employed within the information system and its environment of operation. Ignyte Assurance Platform helps you tailor policies to each device and system to align with the required security documentation.

RMF STEP 4: ASSESS SECURITY CONTROLS

Ignyte guides you in deploying the appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for your systems.

KEY BENEFITS CONT.

- Access real-time dashboards and reports designed to provide executive-level compliance insights including more granular metrics for audit and compliance professionals.

RMF & IGNYTE ASSURANCE PLATFORM™ WALK THROUGH CONTINUED

RMF STEP 5: AUTHORIZE

The SCA will submit the package for approval as other users can also review the package or can return for re-work. The SCA will assess the package and enter the "Security Controls Assessor Executive Summary" describing the overall System cybersecurity risk and provide an "Assessment Date" to the Security Assessment Report (SAR). When the package is submitted to the Approving Official (AO), Ignyte Assurance Platform will generate a task notification.

RMF STEP 6: MONITOR

The IS will be within the Ignyte Assurance Platform for on-going assessments and for any POA&M item that is addressed throughout the lifecycle of the system or IS. Users assigned to a package updates the live System. These updates include the following: System Details, Controls, Artifacts and POA&M items. The updates to current system pop-up window will display a count of POA&M items that have been added to the live System since package creation. Updated Controls displayed with a list of any changes to control compliance status since package creation. Ignyte Assurance Platform supports continuous monitoring that allow an organization to maintain the security authorization of an information system over time in a highly dynamic operating environment where systems adapt to changing threats, vulnerabilities, technologies, and business processes

WHY IGNYTE?

Ignite Assurance Platform allows a focus on risk to address the diversity of systems, components, environments. Our product is custom made to meet users' specific needs, as opposed to using a one-size-fits-all solution. The steps detailed within the Risk Management Framework prescribe a comprehensive approach to continuous risk management. Ignyte Assurance Platform effectively automates RMF security controls and allows continuous compliance to enable businesses to operate at unprecedented speeds that help reduce the vulnerabilities landscape

FOR MORE INFORMATION

To learn more about how Ignyte can help solve your business and IT challenges, contact your local representative or authorized reseller — or visit us at **ignyteplatform.com**. If you are an existing Ignyte Platform customer and have questions or require additional information about licensing, please contact Ignyte at support@ignyteplatform.com or call **1.833.IGNYTE1, (937) 789-4216**.compliance to enable businesses to operate at unprecedented speeds that help reduce the vulnerabilities landscape

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**