RISK MANAGEMENT

TECH SPOTLIGHT SERIES

INNOVATION IN GOVERNMENT®

Streamlining Compliance and Enhancing Security with RegScale's Continuous Controls Monitoring Platform

ABOUT

RegScale overcomes limitations in legacy GRC by bridging security, risk, and compliance through our Continuous Controls Monitoring platform. Our CCM pipelines of automation, dashboards, and AI tools deliver lower program costs, strengthen security, and minimize painful handoffs between teams.

RESOURCES

Continuous Controls Management
carah.io/regscale-home

RegScale Blogs
carah.io/regscale-blog

RegScale
carah.io/regscale

Guide for Implementing RMF
carah.io/implementing-rmf-guide

CONTACT US

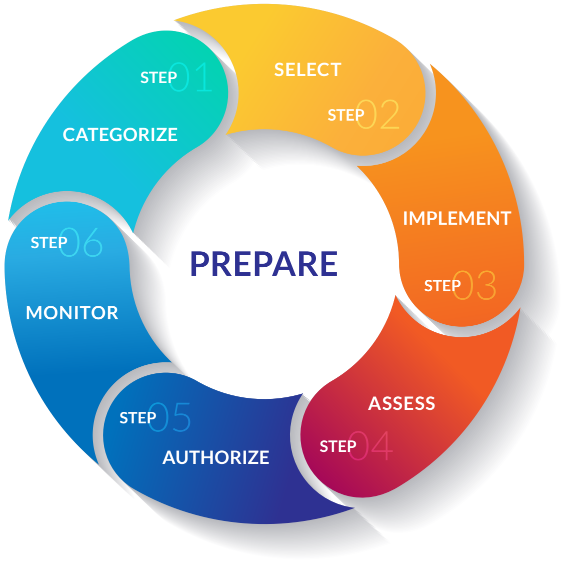
sales@regscale.com

regscale.com/contact

TECHNICAL SUMMARY

The National Institute of Standards and Technologies (NIST) Risk Management Framework (RMF) is a comprehensive framework that provides a process for integrating security, privacy and cyber supply chain risk management activities into the system development lifecycle. The framework presents a structured approach to managing risk through seven steps:

- Essential activities to **prepare** the agency to manage security and privacy risks
- **Categorize** the system and information processed, stored and transmitted based on an impact analysis
- **Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
- **Implement** the controls and document how they are deployed
- **Assess** to determine if the controls are in place, operating as intended and producing the desired results
- Senior official makes a risk-based decision to **authorize** the system (to operate); commonly referred to as an ATO
- Continuously **monitor** control implementation and risks to the system over time



The RMF approach can be applied to any type of system or technology, new or legacy, and within any type of organization regardless of size or sector.

Continuous control monitoring (CCM) supports the management of the control lifecycle by providing real-time visibility into the effectiveness of security controls, enabling proactive risk management and facilitating ongoing compliance. CCM allows agencies to continuously monitor the performance of security controls, identify potential issues or gaps and take corrective actions quickly. To establish a control baseline, agencies should leverage CCM to build a rationalized set of controls that takes into account compliance requirements, operational needs and cyber security risk.

RegScale is an automated, AI-driven platform that helps Government agencies implement NIST RMF, including continuous monitoring, to lower costs, strengthen security and maintain compliance. RegScale aligns compliance controls with risks that are present for a given system, tailors controls to balance risk and cost, analyzes risk to quantify business impacts, allow mitigations to be applied and aligns control implementations to the business risks they mitigate.

RegScale | carahsoft.

THE CHALLENGE

The Federal Information Security Modernization Act (FISMA) requires Government agencies to continuously monitor their risk posture and understand complex compliance requirements. Compliance requirements also vary depending on the agency, making it challenging to ensure consistency across the Government. To conduct accurate risk assessments, agencies must have a deep understanding of the organization's systems, processes and potential threats, which can be time consuming and resource intensive.

When agencies attempt to achieve continuous monitoring, it means they may examine a third of the controls every year for three years; however, many changes occur during that three-year period in addition to changes that occur in the cyber threat landscape. Increasingly, agencies understand that timeline is too long and nearer to real-time continuous monitoring is required to ensure their systems have an assured risk posture. This approach is not currently feasible using existing processes since it requires a lot of manual labor and significant resources to manage the rapidly changing vulnerabilities landscape. New approaches and tools are needed to move to a continuous assurance posture.

MARKETS TARGETED

Government Agencies: RegScale helps Government agencies streamline compliance processes, reduce costs and strengthen security through automated compliance management and continuous monitoring. By automating manual tasks and providing actionable insights, RegScale enables agencies to achieve rapid certification, anticipate threats and automate evidence collection, ultimately improving the return on investment of existing tools . Additionally, RegScale is the sole Government, Risk and Compliance (GRC) tool designed exclusively on OSCAL with full native functionality that provides one-click export to OSCAL and produces FedRAMP artifacts.

Financial Institutions: By seamlessly exchanging data with existing tools, RegScale empowers financial institutions to reduce audit preparation efforts, strengthen security and minimize handoffs between teams, resulting in faster compliance certifications and significant cost savings.

Healthcare Organizations: RegScale offers healthcare organizations a solution for managing and monitoring security controls by automating compliance processes and providing AI-driven insights. By leveraging RegScale to implement HIPAA related processes, healthcare organizations improve patient data protection and reduce regulatory risk.

THE SOLUTION

RegScale is the only CCM platform purpose-built on NIST Open Security Controls Assessment Language (OSCAL) with OSCAL-native compliance as code compatibility throughout the platform. This support includes ingestion and one-click generation of System Security Plans (SSP), Plan of Action & Milestones (POA&Ms), Security Assessment Plans/Reports (SAP/SAR) and Authority to Operate (ATO) packages and artifacts.

CCM pipelines are automation engines that speed up data exchange, output continuously updated artifacts for controls, and validate that these controls bolster security, manage threats (risks) and demonstrate compliance. RegScale is Application Programming Interface (API)-centric and includes over 1,200 APIs, a queryable Graph layer and 30+ pre-built integrations to leverage a customer's existing security stack, seamlessly exchanging structured and unstructured data into a centralized CCM data lake for streamline reporting and analytics.

Always Audit-Ready with Automated Compliance

RegScale streamlines compliance processes, automates evidence collection and facilitates continuous monitoring, ensuring that Government agencies are consistently prepared for audits with self-updating paperwork on demand.

Lower Costs with Intelligent Automation

RegScale's AI-driven platform automates manual tasks, reducing the amount of budget and resources required to accomplish compliance requirements.

Strengthen Security through Actionable Insights

By providing continuous monitoring of security controls and actionable insights, RegScale helps Government agencies strengthen their security posture. This proactive approach enables agencies to identify and address potential threats more effectively.

Scale Seamlessly Across Use Cases

RegScale's cloud-native platform is designed to scale seamlessly across various use cases within Government agencies. Whether it is managing compliance for different systems, technologies or operational constraints, RegScale provides a flexible and adaptable solution to meet the diverse needs of Government organizations.