TAG CYBER

ACCELERATING CYBERSECURITY COMPLIANCE WITH MEAN TIME TO COMPLIANCE (MTTC): AN OVERVIEW OF REGSCALE

CHRISTOPHER R. WILDER, TAG CYBER
JOHN J. MASSERINI, TAG CYBER

RegScale

TAG CYBER

ACCELERATING CYBERSECURITY COMPLIANCE WITH MEAN TIME TO COMPLIANCE (MTTC): AN OVERVIEW OF REGSCALE

CHRISTOPHER R. WILDER
JOHN J. MASSERINI

INTRODUCTION

As organizations increasingly migrate to cloud computing solutions to streamline IT operations and reduce costs, ensuring the security and integrity of sensitive data becomes paramount. The Federal Risk and Authorization Management Program (FedRAMP) has become a critical consideration for many companies, especially those that sell cloud-based services to the U.S. federal government. However, achieving compliance can be complex and challenging. RegScale, the world's first real-time governance, risk and compliance (GRC) platform, specializes in helping organizations achieve compliance with multiple cybersecurity frameworks, such as the Cybersecurity Maturity Model Certification (CMMC), the Service Organization Controls 2 (SOC2), and FedRAMP. This e-book provides an in-depth overview of RegScale's GRC platform; outlines the key stages of the FedRAMP compliance process; and highlights how RegScale's expertise can help organizations achieve compliance faster and more efficiently, using the mean time to compliance (MTTC) metric.

WHAT IS MEAN TIME TO COMPLIANCE (MTTC)?

Mean time to compliance, or MTTC, is a performance metric measuring the average time that it takes for an organization to achieve compliance with a specific cybersecurity framework. This metric is valuable for organizations because it helps identify areas where improvements can be made to expedite the compliance process, ultimately leading to better security posture, reduced risk, and increased operational efficiency. By focusing on MTTC, organizations can prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance.

WHY MTTC MATTERS

Compliance with cybersecurity frameworks such as FedRAMP, CMMC, SOC2, and others is essential for mitigating risks and maintaining the trust of clients and partners. However, achieving and maintaining compliance can be a resource-intensive process that diverts time and attention from other critical business functions. Every cybersecurity executive overseeing compliance will tell you that the journey is frustrating and labor-intensive, and requires endless hours to continuously adapt to new threats and regulatory requirements in today's rapidly evolving cybersecurity landscape. By focusing on MTTC, organizations can make data-driven decisions about where to allocate resources and how to improve processes to reduce the time and effort required to achieve compliance.

REGSCALE'S GRC PLATFORM FOR REDUCING MTTC

RegScale offers a comprehensive technology platform that streamlines and automates many aspects of the compliance process. As the world's first real-time GRC platform, it provides a centralized location for managing compliance activities and tracking progress, including documentation, policy, risk, and audit management. The platform provides real-time reporting and dashboards that give organizations visibility into their compliance status and progress toward reducing their MTTC.

RegScale's GRC platform is highly configurable, allowing organizations to tailor their compliance activities to their unique business requirements and compliance objectives. The platform is also cloud-based, enabling organizations to access compliance activities and progress from anywhere, at any time, and on any device. With RegScale's platform, organizations can manage compliance activities more efficiently, reducing the time and resources required to achieve compliance and, ultimately, reducing their overall MTTC.

Key strategies for reducing MTTC, using RegScale:

1. *Compliance Strategy and Road Map*: RegScale works with organizations to develop a tailored compliance strategy and road map that identifies the necessary steps to achieve compliance and reduce MTTC. This process begins with understanding the organization's unique business requirements, risk tolerance, and compliance objectives. From there, RegScale creates a customized plan that outlines the specific actions required to achieve compliance within the desired timeframe.

2. *Gap Analysis Support*: Once the customer performs a thorough gap analysis to identify areas where the organization's security posture falls short of the requirements of the desired compliance framework, RegScale supports the efforts to evaluate the organization's policies, procedures, and technical controls against the requirements of the relevant cybersecurity framework. The gap analysis results provide a clear picture of the areas that need improvement and a path forward, enabling organizations to prioritize their efforts and allocate resources effectively.

3. *Remediation Support*: RegScale supports implementing the necessary changes to address identified gaps, ensuring that the organization meets compliance requirements as quickly as possible. Compliance requirements may involve updating policies and procedures, implementing new technical controls, and providing employee training and awareness programs. RegScale's experienced cybersecurity professionals offer comprehensive and hands-on assistance and guidance throughout the remediation process, ensuring that organizations can achieve compliance as efficiently as possible.

Further, RegScale's "white glove" service features a proficient customer success team providing tailored, current information to its clients. Through updated tickets and discussions, customers can access specialized training and demonstrations of new capabilities, maximizing the benefits to its customers.

4. *Continuous Monitoring and Improvement*: RegScale offers ongoing customer support to maintain compliance and continuously improve the organization's security posture, reducing MTTC for future compliance efforts, including regularly reviewing and updating policies and procedures, monitoring changes in the cybersecurity landscape, and ensuring that organizations stay current with evolving regulatory requirements. RegScale also provides periodic assessments to measure progress and identify any new gaps that may have emerged. This continuous improvement approach helps organizations maintain a strong security posture while minimizing the time and effort required for future compliance initiatives.

THE FEDRAMP COMPLIANCE PROCESS AND HOW REGSCALE HELPS ITS CUSTOMERS REDUCE THEIR MTTC

The FedRAMP framework, known for being one of the most comprehensive and cumbersome, necessitates a meticulous approach to achieve compliance, typically taking 18-24 months. RegScale, with its GRC expertise and special focus on FedRAMP, assists organizations in navigating this complex process more efficiently, ultimately speeding up their entry into the federal market. By swiftly identifying and addressing security gaps, RegScale streamlines compliance activities and empowers organizations to make data-driven decisions that optimize their efforts. This targeted approach reduces MTTC and minimizes resources expenditure, while providing a strategic advantage in a competitive landscape.

1. *Initiation and Creation of the Master Security Plan (MSP)*: The FedRAMP certification process begins with organizations identifying the appropriate authorization level (Low, Moderate, or High) corresponding to the sensitivity of the data they manage. This crucial step establishes the compliance process's scope, ensuring that organizations concentrate on the most relevant controls and requirements. By aligning with the appropriate FedRAMP level, RegScale's expert guidance assists clients in developing a robust master security plan, streamlining the compliance journey, and reinforcing their commitment to protecting sensitive federal information.

2. *Assessment*: Once the MSP is in place, a thorough evaluation is conducted by a third-party assessment organization (3PAO) to evaluate the organization's security posture against the FedRAMP requirements. This process includes a review of documentation, interviews with key personnel, and technical testing of the organization's systems and controls. The 3PAO then produces a detailed report outlining the organization's compliance status and any identified gaps.

3. *Authorization*: If the assessment demonstrates compliance, the organization receives an authorization to operate (ATO) from a federal agency, granting it the right to provide cloud services to the federal government. Obtaining an ATO is a significant milestone in the FedRAMP compliance process, as it signifies that the organization has met the stringent security requirements necessary to protect sensitive government data.

4. *Continuous Monitoring*: Organizations must monitor their security posture and report any changes to the authorizing agency, ensuring ongoing compliance. Continuous monitoring is essential for maintaining FedRAMP compliance and demonstrating a commitment to protecting sensitive government information. Continuous monitoring also includes regularly updating

system security plans, conducting periodic assessments, and implementing any required remediations.

REGSCALE'S GRC EXPERTISE IN IMPROVING MTTC

RegScale has significant GRC expertise in and emphasis on not only FedRAMP, but most other cybersecurity frameworks. The platform assists organizations of all sizes to efficiently navigate the complex cybersecurity compliance process, reducing their MTTC and accelerating their entry into the federal market. This targeted approach streamlines compliance activities, empowering organizations to make data-driven decisions that optimize their efforts, while minimizing resources expenditure and providing a strategic advantage.

Initially, RegScale helps clients determine the appropriate FedRAMP authorization level (Low, Moderate, or High), according to the sensitivity of the data that they manage. This step is vital in setting the compliance process's scope, focusing on the most relevant controls and requirements. RegScale's expert guidance enables clients to develop a robust MSP, expediting the compliance journey and solidifying their commitment to protecting sensitive federal information. Once the MSP is in place, RegScale supports organizations during the third-party assessment organization (3PAO) evaluation, ensuring a thorough review of the organization's security posture against FedRAMP requirements. This support results in a comprehensive report outlining the organization's compliance status and identifying any gaps.

Upon successful assessment, organizations receive an authorization to operate (ATO) from a federal agency, granting them the right to provide cloud services to the federal government. RegScale continues to support maintaining FedRAMP compliance through continuous monitoring of security posture, regular updates to system security plans, periodic assessments, and the implementation of required remediations. This ongoing guidance helps organizations protect sensitive government information and maintain a strong security posture, minimizing the time and effort required for future compliance initiatives from FedRAMP and other cybersecurity frameworks.

EXPANDING MTTC TO OTHER CYBERSECURITY FRAMEWORKS

In addition to FedRAMP, organizations often face the challenge of maintaining compliance with other cybersecurity frameworks, such as CMMC and SOC2. RegScale's expertise extends to these frameworks, allowing it to help organizations optimize their MTTC across multiple compliance initiatives. RegScale can guide organizations through the complexities of achieving and maintaining compliance with various cybersecurity standards by applying the same principles of gap analysis, remediation support, and continuous monitoring.

WRAPPING IT UP

Mean time to compliance (MTTC) is a valuable metric for organizations seeking to improve cybersecurity compliance. By focusing on MTTC, organizations can prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance. RegScale is the only real-time GRC platform on the market today tailored to each organization's unique needs. It helps to achieve and maintain compliance with various cybersecurity frameworks, including FedRAMP, CMMC, SOC2, and others. With its expertise in reducing MTTC, RegScale is well-positioned to guide organizations through the complex compliance landscape, leading to better security posture, reduced risk, and increased operational efficiency.

Embracing MTTC as a key performance metric is the first step toward a more proactive and streamlined approach to cybersecurity compliance, ensuring that your organization stays ahead of the curve and protects its valuable data assets. In a world where cloud computing is increasingly popular and sensitive data is constantly at risk, partnering with a cybersecurity company like RegScale can make all the difference in achieving compliance with the ever-evolving regulatory landscape. By allocating the budget to the RegScale platform, organizations can improve their mean time to compliance, leading to a more secure and efficient operation that meets the stringent requirements of federal agencies and other stakeholders.

KEY TAKEAWAYS

- Mean time to compliance (MTTC) is an essential performance metric that can help organizations optimize cybersecurity compliance across various frameworks, including FedRAMP, CMMC, and SOC2.
- RegScale is the world's first real-time GRC platform. It offers to guide organizations through the complexities of achieving compliance, from developing tailored strategies and road maps to providing remediation support and continuous monitoring.
- By focusing on reducing MTTC, RegScale enables organizations to prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance.
- RegScale's expertise in reducing MTTC and navigating the compliance landscape for multiple cybersecurity frameworks positions it as a valuable partner for organizations looking to improve their security posture, reduce risk, and increase operational efficiency.

TAG'S TAKE

For CISOs and security teams, achieving compliance with cybersecurity frameworks can be daunting, but it is critical to ensuring the security and integrity of sensitive data. By partnering with a cybersecurity GRC software company like RegScale, organizations can improve their mean time to compliance and more effectively navigate the complex compliance landscape.

If your organization seeks assistance with FedRAMP, CMMC, SOC2, or any other cybersecurity frameworks, RegScale should be a viable solution. Its platform and expertise can help you develop a tailored GRC and compliance strategy, identify gaps in your security posture, and provide the support needed to achieve compliance as efficiently as possible. Companies in regulated environments such as health care, financial services, and the government utilize RegScale to ensure compliance with compliance requirements. RegScale's platform and commitment to helping obtain compliance framework faster through MTTC, organizations can be confident that your organization can protect their valuable data assets and maintain the trust of clients and partners in today's ever-evolving cybersecurity landscape.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Chris Wilder, John Masserini

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Disclosures: This paper was commissioned by RegScale. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.