

LEVERAGING CONTINUOUS CONTROLS MONITORING (CCM) FOR COMPLIANCE AND SECURITY

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE, INC.


TAG

 RegScale

LEVERAGING CONTINUOUS CONTROLS MONITORING (CCM) FOR COMPLIANCE AND SECURITY

The TAG logo consists of the letters "TAG" in a bold, white, sans-serif font, centered within a solid blue rectangular background.

INTRODUCTION

Our assumption is that readers of this report work in enterprise cybersecurity and compliance and are seeking means to improve support for continuous controls monitoring. Our view is that commercial solutions in this area are beginning to emerge and that RegScale represents a solid choice for practitioners, as we will show. Our approach is to cover the area of CCM including its benefits and to provide a checklist (see Appendix A) for buyers seeking commercial CCM platforms.

LEVERAGING CONTINUOUS CONTROLS MONITORING (CCM) FOR COMPLIANCE AND SECURITY

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE, INC.

This book provides a detailed introduction and overview of continuous controls monitoring (CCM) from the perspective of the modern enterprise security and compliance practitioner. Guidance is offered on how to deploy and use CCM solutions such as RegScale to support compliance engagements and audit projects.

INTRODUCTION
PAGE 2

CHAPTER 1
UNDERSTANDING CCM
PAGE 4

CHAPTER 2
WHAT IS CONTINUOUS CONTROLS MONITORING (CCM)?
PAGE 5

CHAPTER 3
DEPLOYING CCM TO THE ENTERPRISE
PAGE 6

CHAPTER 4
CHALLENGES ADDRESSED BY CCM
PAGE 7

CHAPTER 5
CHOOSING A CCM FRAMEWORK
PAGE 8

CHAPTER 6
SUPPORTING COMPLIANCE ASSESSMENTS WITH CCM
PAGE 10

CHAPTER 7
ESTABLISHING AN ALWAYS-READY STATE
PAGE 12

CHAPTER 8
MASTERING SECURITY COMPLIANCE WITH CCM
PAGE 14

CHAPTER 9
KEY USE CASE
PAGE 15

CHAPTER 10
CCM ACTION PLAN
PAGE 18

APPENDIX A:
COMMERCIAL CCM BUYER'S CHECKLIST
PAGE 19

UNDERSTANDING CCM

Enterprise security and compliance practitioners are beginning to recognize the benefits of a powerful strategy known as *continuous controls monitoring* (CCM) to streamline their assessment and audit projects.¹ The most common challenge identified by practitioners who are beginning to consider CCM involves finding effective means for reducing the time and cost associated with their present and future security compliance projects and initiatives.

Motivations for adopting CCM in the enterprise include establishing more proactive risk management to drive more accurate security posture assessment, driving improvements in overall efficiencies beyond just audits, enhancing visibility and reporting of security and risk, creating heightened stakeholder confidence, and implementing more cost-effective controls that are also more adaptable to change.

Specifically, CCM involves the real-time assessment and verification of management and operational controls to manage risks, ensure compliance, and enhance decision-making across the organization. CCM platforms are well-positioned to address security, risk, and compliance. In the best case, they leverage automation to drive confidence that controls are working exactly as expected – and required.

While most security and compliance professionals fully understand that automation is certainly the right strategy to address this challenge, determining exactly how this can be done is not always clear. As we will explain in this report, CCM represents a promising means for replacing manual steps with automated processes to manage risk, achieve security certifications, and meet other objectives more rapidly and more predictably.

The right questions for enterprise security teams to ask regarding CCM include where to start, which frameworks to target, and which commercial vendors to select as partners for this work. As a result, throughout this report, we will reference our experience with commercial vendor **RegScale** to illustrate how the general concepts and strategies can be actually deployed in a live production environment to produce value today.

In addition, we will focus on preparation for assessments, and how this is made easier and more complete using CCM. We will also provide guidance on how to navigate and respond to assessment results faster and more accurately via CCM. As one might expect, the goal is to ensure audit-readiness and to ensure support for the on-going compliance cycle by being proactive through automated CCM mechanisms for security, risk, and compliance.

The right questions for enterprise security teams to ask regarding CCM include where to start, which frameworks to target, and which commercial vendors to select as partners for this work.

¹The ISACA membership organization references CCM as a discipline that auditors should recognize. An article on their view of CCM is available here: <https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/a-practical-approach-to-continuous-control-monitoring>.

WHAT IS CONTINUOUS CONTROLS MONITORING (CCM)?

The technique known as Continuous Controls Monitoring (CCM) represents a new approach to performing Governance, Risk Management, and Compliance (GRC) for enterprise security and risk.² CCM, perhaps more than most traditional GRC solutions, focuses on leveraging technology to proactively manage and monitor IT risks and compliance issues in near real-time. Such technology-enabled monitoring can complement existing GRC or create new GRC coverage.³

An advantage of CCM is that the traditional, reactive methods of handling IT risks and compliance are no longer sufficient given the rapid pace of DevOps, Agile enterprise management, and real-time cybersecurity. CCM represents a paradigm shift towards a more strategic, real-time, and proactive approach. This is important for deployments to critical infrastructure, including government environments driven by standards such as FedRAMP.

The best CCM platforms will support this shift by offering real-time data monitoring, enabling continuous surveillance of IT systems. This surveillance should not be just about collecting data on the present state but should also drive proactive management of compliance through real-time updates. Automated reporting and resource optimization should further enhance the efficiency and effectiveness of this process.

Such a system must empower decision-makers with real-time data for better judgment calls, not just in routine operations but also in crisis scenarios. In essence, CCM platforms provide a fresh new GRC solution that integrates with broader IT and cloud architectures, offering real-time awareness and insights into IT risk, compliance, and control. This adaptability ensures that organizations drive better resilience in their IT risk and compliance management strategies.

² The Wikipedia entry for Governance, Risk, and Compliance (GRC) includes useful general information about the approach and how it is deployed.

See https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance.

³ Much of the guidance on CCM is derived from discussions with commercial vendor RegScale, a platform leader in this category of cybersecurity and compliance support.

See <https://regscalestage.wpengine.com/> for more details on their commercial platform.

DEPLOYING CCM TO THE ENTERPRISE

Since CCM represents a new approach to GRC, it helps to identify the best practices associated with the deployment of a CCM solution. To start, we can identify two primary baselines that will involve the use of a CCM solution from a commercial vendor. Obviously, these scenarios depend on a prior source selection activity in which a CCM platform has been identified and procured. We will use RegScale as our platform example throughout this report.

RegScale customers report a 90% faster path to compliance certifications and a remarkable 60% reduction in audit preparation efforts

Overview of RegScale

RegScale overcomes limitations in legacy GRC by bridging security, risk, and compliance through its CCM platform. The company's CCM pipelines of automation, dashboards, and AI tools deliver lower program costs, strengthen security, and minimize painful handoffs between teams. RegScale helps customers achieve rapid certification for faster market entry, anticipate threats via proactive risk management, and automate evidence collection, access reviews, and controls mapping.

RegScale addresses improvements in return on investment (ROI) for GRC by seamlessly exchanging data with its centralized CCM data lake, thus enabling continuous monitoring of security, risk, and compliance controls. RegScale customers report a 90% faster path to compliance certifications and a remarkable 60% reduction in audit preparation efforts, strengthening security programs and reducing costs.⁴

CCM Scenarios

One scenario for CCM deployment involves the installation of the platform as a complement to an existing GRC system, perhaps from a major vendor such as ServiceNow or Archer, or alternatively from a smaller vendor such as ControlCase. In this situation, the CCM solution must provide added value by addressing weaknesses and complementing strengths in the existing GRC ecosystem.

A second scenario involves the CCM platform being deployed into an environment where GRC is either being performed using manual techniques or is not being attended to at all. Such so-called greenfield scenarios suggest that the CCM solution must not only add value but should also include sufficient capability to on-ramp an organization toward a more automated and continuous process for addressing risk and compliance.

⁴ Information from RegScale was obtained and used throughout the development of this report through technical reviews, feedback, and discussions with the team principals. Excellent information was also obtained from the company's published reports and website at <https://regscale.com>.

CHALLENGES ADDRESSED BY CCM

In the primary usage scenarios for CCM – namely, either complementing a GRC platform or introducing a new platform for risk and compliance – the challenges for the enterprise security team will be essentially the same. Such challenges tend to fall into three main categories: Cost-related issues, process inefficiencies, and time-related problems. All three of these challenges are addressed, even disrupted, by the introduction of CCM as will be explained below.

Cost Reduction

The rapid certification approach inherent in automated CCM support delivers immediate cost savings. Costs for compliance-related programs come in many different forms including the time spent by staff working issues that range from documentation support to meeting with regulatory officials or auditors. Reducing the amount of time necessary for such work will directly improve the bottom-line with reductions, including for consultants engaged to assist with GRC.

Data Management

CCM provides the opportunity for enterprise risk and compliance teams to address the challenge of disjointed data across multiple systems. Such complexity can be greatly reduced through the continuous automation inherent in a CCM platform. Enterprise teams can rely on CCM platform to roll up risk-related data into a common framework for better decision-making and management action.

Process Improvement

The use of CCM is well-suited to security and compliance teams with a sense of urgency to improve their end-to-end processes. This includes not just establishing compliance with a new framework but can also be useful for teams moving from one framework (e.g., NIST 800-53)⁵ to another (e.g., FedRAMP).⁶ It should also be emphasized that risk management and compliance reduce the potential for cyber threats, which reduces the need for response and reporting.

Time Savings

An additional benefit of CCM is that security teams can progress more quickly to compliance programs consistent with frameworks such as NIST 800-53, SOC 2, and FedRAMP Rev 5. This has always been a goal for GRC solutions, but the awkwardness and complexity inherent in most commercial platforms prompts risk and compliance practitioners to seek the complementary support of CCM solutions – always with the goal to reduce time spent on these tasks.

Costs for compliance-related programs come in many different forms including the time spent by staff working issues that range from documentation support to meeting with regulatory officials or auditors.

⁵ See <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final> for details on this important cybersecurity standard from the National Institute of Standards and Technology (NIST).

⁶ The General Services Administration (GSA) provides a useful resource guide to FedRAMP which can be accessed here: <https://www.gsa.gov/technology/government-it-initiatives/fedramp>.

CHOOSING A CCM FRAMEWORK

It is easy to make the mistake of viewing compliance as a goal, rather than a means toward effective, safe, and secure operation.

A major pillar of any compliance ecosystem is the selection of a governance framework (or frameworks) that will guide the functional and assurance aspects of the overall certification, monitoring, or improvement process. The task of choosing a CCM framework involves three specific situations – namely, selection of a single framework, selection of multiple frameworks, or extension from one framework to another.

In each of these cases, the goal is to dictate an information technology (IT) and cybersecurity architecture that includes controls deployed once and then used as the basis for managing risk and establishing compliance across whatever frameworks have been selected. It is easy to make the mistake of viewing compliance as a goal, rather than a means toward effective, safe, and secure operation. The three framework selection scenarios are discussed below.

Single Framework

The use of a single framework has the great advantage of being simple, and in many cases, a specific use-case such as a government agency deal, will dictate the framework. It's been our experience at TAG that many teams often opt to use NIST 800-53 as a baseline because it includes such a comprehensive set of requirements. The importance of the NIST Cybersecurity Framework (CSF)⁷ also tends to guide many organizations toward use of NIST as a baseline.

Multiple Frameworks

The use of multiple frameworks has unfortunately emerged as the more likely situation for any non-trivial organization. Even small businesses find themselves with the obligation to support frameworks such as the Payment Card Industry (PCI) Data Security Standard (DSS),⁸ along with security framework requirements that might come from a large buyer. Such need to map and normalize multiple frameworks is additional evidence for the need to deploy CCM.

⁷ Useful operational and technical information for practitioners on the NIST Cybersecurity Framework (CSF) is available on-line here: <https://www.nist.gov/cyberframework>.

⁸ The PCI Security Standards Council publishes information about its important cybersecurity framework here: <https://www.pcisecuritystandards.org>.

CHOOSING A CCM FRAMEWORK

Framework Extension

The case in which an organization shifts from one framework to another is more likely to involve the decision to use a new baseline framework as a principal guide for security decisions. The trend toward multiple risk and compliance frameworks, along with the common need to integrate cyber risk with other business risks, typically dictates deployment and use of automation, since manual methods will not scale across complex frameworks.

Some examples in which framework extension is particularly important include companies using SOC 2 as a baseline, and then extending to add NIST CSF or ISO 27001. Alternatively, a company might have PCI-DSS compliance and would rely on CCM to assist in transitioning to include NIST CSF or some other framework. These are common examples that should help to illustrate common usage scenarios that emerge in practice.

SUPPORTING COMPLIANCE ASSESSMENTS WITH CCM

The essence of successfully supporting any compliance audit, especially in the context of cyber risk, involves the proper collection of evidence. In the past, this was done using manual methods, face-to-face discussions, crude data analysis, and human-generated summary reports. While some of this remains common (e.g., in-person discussions), the best compliance teams have shifted their evidence focus to automation.

When done optimally, and CCM platforms are especially well-suited for this non-manual approach, the automation is done through application programming interfaces (APIs) which enable connections to data sources. Such integration can be complex, so practitioners usually spend time interrogating technology vendors – and this is a key benefit of CCM – to ensure that the integrations are straightforward and also heavily automated.

A key benefit of CCM is to ensure that the integrations are straightforward and also heavily automated.

The result is a machine-to-machine communication and coordination indicative of how modern systems such as cloud workloads and containerized applications are designed to operate. The goal obviously is to produce an always-ready state for compliance audits and reporting. The advantage of CCM integration either to complement, replace, or serve as the GRC platform is that it drives this continuous readiness from a risk and compliance perspective.

Some examples in which this readiness state can be helpful include collection of real-time data regarding employee actions. It is not uncommon for security teams to struggle to maintain compliance with hiring, firing, changes, and other staff actions that must be synchronized with identity and access management (IAM) systems. When this is attempted using manual methods such as spreadsheets, the result is a lag in data collection and bad audits can occur.

By the way, bad audits could involve incorrect conclusions being drawn based on the audit testing that was done, presumably using some manual means. When this occurs, such unfavorable results can lead to misinterpretation of risk, wasted management effort, and even damage to the careers and reputations of team members involved. Automation carries considerable value in preventing these situations.

SUPPORTING COMPLIANCE ASSESSMENTS WITH CCM

Another example involves the measurement of vulnerability remediation and patch status across an enterprise. This has always been a challenge due to the unpredictable nature of when and where vulnerabilities arise. Every enterprise CISO is familiar with the serious problems that can occur when an auditor is reviewing a spreadsheet that shows partial patching of some critical issue.

Automation using CCM platform is an excellent means for avoiding such problems, if only because the tracking will be more accurate, up-to-date, and referenced with suitable contextual data. Without understanding the context of some issue such as an unpatched system, auditors might misinterpret a reasonable management decision, perhaps based on careful consideration of pros and cons, with what might be viewed as neglect.

ESTABLISHING AN ALWAYS-READY STATE

Ultimately, a CCM platform will drive a continuous model in which the readiness state is established and updated toward always-on readiness.

While it's straightforward to reference the benefits of an always-ready state for enterprise risk and compliance teams preparing for audit, in most cases, establishing such a state requires more than just deployment of a CCM platform. Generally, a significant shift is required in the mindset of the individuals and groups involved. Specifically, such a mindset should be adjusted toward focusing on establishing machine-to-machine automation.

Experienced risk and compliance professionals dealing with security and privacy assessments and audits will often refer to the challenge of "navigating through the review process" with their internal or external auditor. This is precisely the type of challenge that requires rethinking toward a more readiness-state orientation. For anyone who has worked in this area, such an approach is nothing short of revolutionary in its impact on risk and compliance.

Continuous Model

Ultimately, a CCM platform will drive a continuous model in which the readiness state is established and updated toward always-on readiness. This changes the nature of audits and assessments since it effectively removes, or at least greatly reduces, the need for manual preparation in advance of a review. Instead, the readiness can be used to feed audit inquiries and this continuous model saves time, money, and effort.

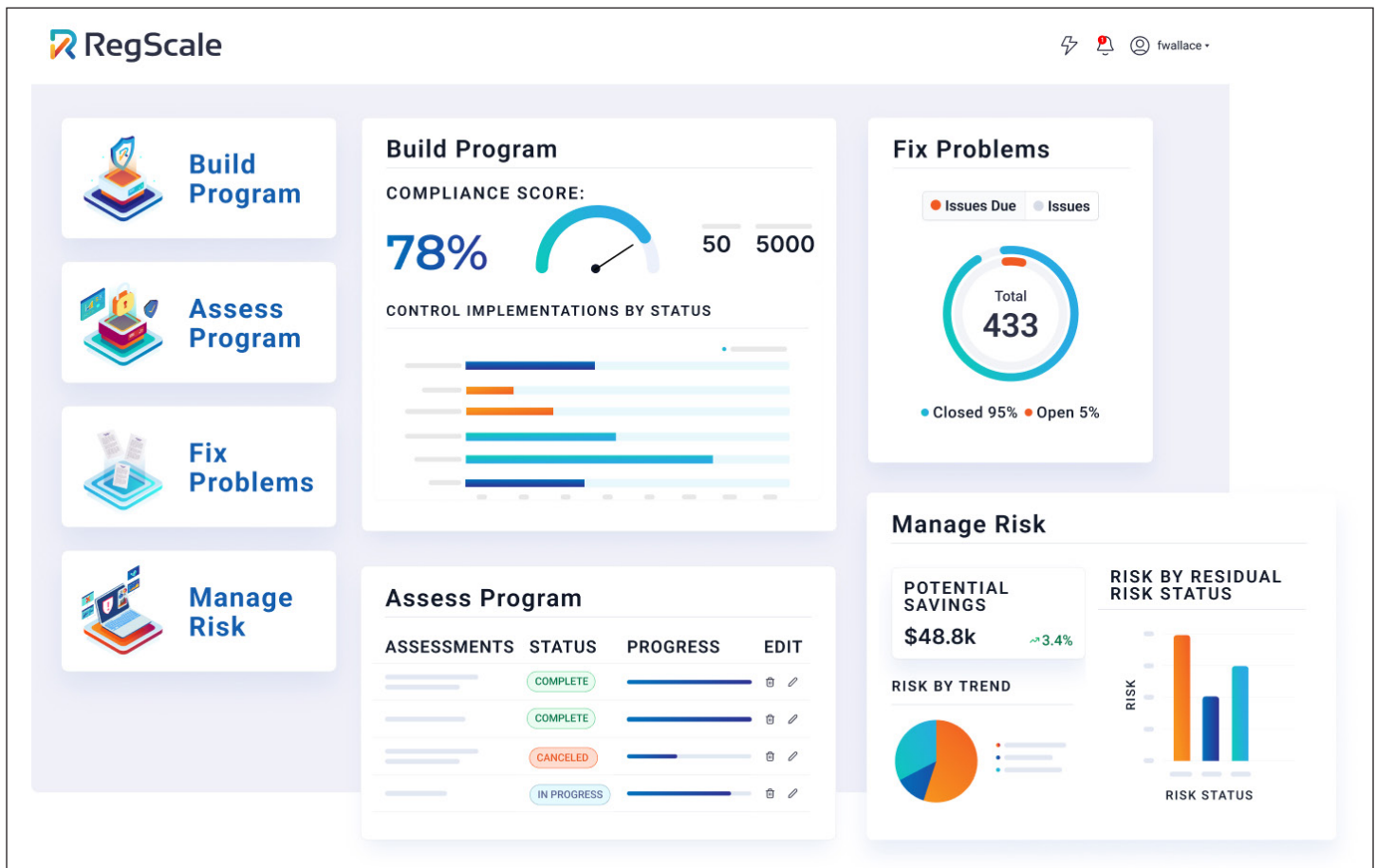
Benefits of Streamlined Audit

More specifically, the primary benefit of streamlined audit is that the pain points associated with risk and compliance efforts are directly addressed. That is, the deployment of a CCM platform and its always audit-ready state deliver lower costs (e.g., reduced auditor fees), shorter timelines (e.g., auditors have shortened projects), and better transparency (e.g., the CCM delivers accurate data on-demand).

ESTABLISHING AN ALWAYS-READY STATE

RegScale Platform Example

Commercial vendor RegScale provides a great example of how CCM can produce such value through a process it refers to as a lightning assessment. This involves establishing a unified resource center as part of the RegScale platform that contains everything the auditor needs for an assessment including the requirements, control implementations, control evidence, and assessment testing (plans and results). The result is a type of “one-click” auditor package.



MASTERING SECURITY COMPLIANCE WITH CCM

Enterprise security strategies, for example, can utilize CCM reporting to drive more proactive mitigation of the highest priority risks.

A major benefit associated with the automation and continuous readiness associated with CCM deployment is that security threats are reduced. Compliance teams can often miss this obvious value in the midst of their day-to-day process working answers to audit inquiries, gathering data, and producing reports. Nevertheless, the operational benefits to security risk reduction can be considerable.

The best security and compliance teams will take the time to connect the dots regarding how continuous compliance strengthens security. Enterprise security strategies, for example, can utilize CCM reporting to drive more proactive mitigation of the highest priority risks. It can also help to determine when and where visibility is required into areas in which vulnerabilities can produce the highest consequence impact.

Even complex enterprise security areas such as third-party risk management (TPRM) can be simplified by having continuous compliance support using CCM. Most GRC efforts struggle to obtain accurate information about suppliers and partners, but connectors can be developed that will collect data for CCM processing, and the resulting views can inform TPRM tasks such as risk quantification or supplier risk mitigation.

Finally, it is worth mentioning that the current trend toward the use of artificial intelligence (AI) in cybersecurity will only work in the presence of data. CCM directly addresses this need by collecting and aggregating data in a safe and secure manner that can be used to train models and improve the accuracy of predictive output associated with the best modern platforms using machine or deep learning to reduce operational risk.

KEY USE CASE

By automating the hand-off to auditors with always audit-ready documentation, organizations experience a more efficient, transparent, and error-free experience, reducing costs and enhancing productivity.

Several key use cases emerge in the context of most practical deployments of CCM. Below we outline the more common scenarios we've seen where organizations have made effective use of commercial CCM platforms, especially from commercial vendors such as RegScale, to solve real business problems. Each of these scenarios involves the use of CCM and its attendant automation to complement or extend the GRC goals of the organization.

FedRAMP Compliance

Rapid certification for FedRAMP, enabled by CCM platform deployment, can revolutionize compliance timelines. Such deployment, for example, can significantly reduce the time to secure an Authority to Operate (ATO). By integrating an automated, end-to-end monitoring process, every phase of FedRAMP can be streamlined, from program establishment to evidence collection, control assessment, issue remediation, risk management, and ongoing surveillance.

This automated continuum, an important aspect of the RegScale solution, not only expedites the initial FedRAMP certification, but also ensures that continuous compliance is maintained with minimal manual intervention by compliance teams or auditors. Organizations thus benefit from a much faster and more reliable path to FedRAMP compliance, thus allowing enterprise teams or vendors to meet stringent security standards with agility and confidence.

Evidence Collection

Instead of juggling documents, resolving conflicts from multiple sources, and manually deciding on evidence types, an automated CCM system offers a centralized, consistent, and real-time approach. This ensures that evidence tracking is accurate and complete. By automating the hand-off to auditors with always audit-ready documentation, organizations experience a more efficient, transparent, and error-free experience, reducing costs and enhancing productivity.

KEY USE CASE

Leveraging RegScale's compliance frameworks and controls mapping features, a Fortune 500 company eliminated redundant controls and related testing, identified and closed control gaps, and reported a more complete and transparent security posture to their Board.

A food retailer saw a 89% Reduction of the time spent on SOX controls by using RegScale to gather evidence, conduct user access reviews, and report status.

Risk Management

Simplified risk management, when integrated within a CCM platform, becomes a dynamic and proactive component of an organization's risk strategy. At the heart of this approach is the understanding that controls are central to both detecting and mitigating risks. By continuously monitoring controls for effectiveness and compliance, a CCM platform can ensure that risk management is not a periodic or reactive process but a constant, vigilant guard against potential vulnerabilities.

This continuous oversight extends across enterprise risk, third-party interactions, and investment portfolios, providing a consistent gauge of risk exposure. With CCM at its core, simplified risk management transforms from a static checklist into a strategic advantage, enabling organizations to anticipate risks and adjust controls in real-time, thereby ensuring a robust and resilient business framework.

Controls Mapping

CCM presents a transformative approach to compliance management. By mapping a single control across multiple compliance frameworks, organizations can streamline their compliance efforts, eliminating redundant tasks and ensuring a harmonized compliance posture. This integration allows for a one-to-many relationship between controls and regulations, ensuring that when a control is updated or reviewed, its status is simultaneously reflected across all applicable compliance frameworks.

The result is a significant reduction in the complexity and labor traditionally associated with compliance management, leading to increased clarity, cost savings, and an agile response to the ever-changing regulatory landscape. This means organizations can focus more on strategic compliance initiatives rather than getting entangled in the minutiae of individual regulation requirements.

Access Reviews

Access reviews are a critical component for maintaining robust security and compliance within an organization. They serve as a safeguard against the risks associated with inappropriate or outdated user access to sensitive systems and data. Regular reviews, especially through an automated platform, ensure that only the right people have the right level of access, aligned with their current roles and responsibilities.

KEY USE CASE

94% Less Effort to complete initial SOC 2 Type 2 using RegScale, compressing a typically months-long endeavor into 25 hours inside of one month.

This not only protects your organization from potential internal and external security breaches but also ensures adherence to regulatory standards, thereby reducing the risk of costly non-compliance penalties. In an era where data breaches are both common and damaging, investing in effective access review processes is not just a matter of best practice; it's a necessity for safeguarding your organization's integrity and reputation.

Rapid Certification

Rapid certification expedites the attainment of compliance for frameworks such as SOC 2,⁹ CMMC,¹⁰ or NIST CSF, by harnessing technology to streamline the entire process. This approach reduces the mean time to compliance, leveraging a smart, integrated system for building compliance programs, gathering evidence, assessing controls, and managing risks, all while ensuring ongoing vigilance through continuous monitoring. The result is a more efficient certification cycle that not only speeds up compliance but also yields cost savings by minimizing manual effort and mitigating the risk of financial penalties from non-compliance. This strategic, technology-driven method delivers both agility and accuracy in maintaining up-to-date compliance standards.

⁹ SOC 2 is explained here: https://en.wikipedia.org/wiki/System_and_Organization_Controls.

¹⁰ See <https://dodcio.defense.gov/CMMC/about/> for information on CMMC.

CCM ACTION PLAN

As the world accelerates to hyper-speed, CCM solves the complexity of the past and meets the speed of the future:

- **AI everywhere**
 - **Self-updating paperwork & compliance as code**
 - **On-demand, audit-ready documentation**
 - **Unified security, risk, and compliance**
-

CCM enables transition from traditional GRC methodologies to an enhanced process that lower costs, creates stronger security, and provides for compliance process efficiencies. The team from RegScale regularly works with clients on an action plan for deployment of CCM either to complement an existing GRC platform and program or to serve as the basis for a new risk and compliance practice.

We highly recommend that security and compliance teams review their existing posture to determine if CCM would be a useful means to bridge security, risk, and compliance. Any selected CCM platforms should leverage automation, dashboards, and AI tools to deliver lower program costs, strengthen security, and minimize painful handoffs between teams. We highly recommend inclusion of RegScale in any source selection process for 2024.

During the action planning process, teams should keep in mind that CCM platforms must help teams achieve rapid certification for faster market entry, anticipate threats via proactive risk management, and automate evidence collection, access reviews, and controls mapping. As should be evidenced from this report, we believe RegScale does an effective job in this regard for enterprise teams.

APPENDIX A: COMMERCIAL CCM BUYER'S CHECKLIST

The TAG analyst team strongly recommends that readers adapt this checklist to their local organizational requirements, constraints, and priorities when evaluating and selecting a commercial CCM platform – and obviously, we strongly endorse the inclusion of RegScale in the source selection process.

1. Preparation Steps:

- **Define Objectives:** Determine and define the goals for implementing a CCM solution, whether for compliance, risk management, or security.
- **Understand General CCM Concepts:** Familiarize yourself with the core concepts of Continuous Controls Monitoring in the context of your own environment.

2. Commercial Engagement Steps:

- **Assess Vendor Capabilities:** Evaluate various commercial CCM vendors to understand their automation, dashboards, and AI.
- **Determine Deployment Scenarios:** Define whether you are complementing an existing GRC system or starting from a greenfield scenario.

3 Risk and Challenge Steps:

- **Identify Challenges to Address:** Define cost and process inefficiencies and time challenges within your organization that CCM can help address.
- **Evaluate Cost Reduction Potential:** Assess the cost savings achieved with automated CCM support, including reduced auditor and consultant expenses.

4 Data and Process Steps:

- **Consider Data Management:** Determine how CCM can help streamline data management by aggregating data from multiple sources.
- **Focus on Process Improvement:** Understand how CCM can improve security and compliance, especially when transitioning between frameworks.

5. Project Management Steps:

- **Assess Time Savings:** Estimate the time-saving benefits of CCM in achieving compliance with frameworks like NIST 800-53 and SOC 2.
- **Choose a Suitable Governance Framework:** Select a governance framework that aligns with your organization's needs, whether single or multiple frameworks.

6. Use Case and Example Scenario Steps:

- **Explore Key Use Cases:** Investigate various practical use cases where CCM can be applied effectively, such as FedRAMP compliance.
- **Evaluate Vendor Examples:** Consider real-world examples from vendors like RegScale that simplify processes, reduce audit effort, and more.

APPENDIX A: COMMERCIAL CCM BUYER'S CHECKLIST

7. Action Planning Steps:

- **Prepare an Action Plan:** Create an action plan for deployment of a CCM solution, either as a complement to existing GRC or new.
- **Verify Automation and AI Integration:** Ensure that the selected CCM platform leverages automation, AI tools, and dashboards.

8. Consultative Steps:

- **Consult with Stakeholders:** Involve key stakeholders in the decision-making process to ensure alignment with organizational goals and objectives.
- **Obtain Vendor References:** Request references from CCM vendors to validate their track record and customer satisfaction.

9. Budget, Cost, and Compliance Steps:

- **Budget and Cost Analysis:** Assess the budget required for the procurement, implementation, and ongoing operation of the CCM platform.
- **Data Security and Compliance:** Ensure that the selected CCM solution meets security and compliance requirements for your industry and region.

10. Training and Improvement Steps:

- **Implementation and Training:** Plan for the implementation process and consider training requirements to effectively utilize the CCM platform.
- **Monitoring and Continuous Improvement:** Establish processes for ongoing monitoring of the CCM platform's effectiveness and continuous monitoring.

11. Licensing and Legal Steps:

- **Licensing and Support Agreements:** Review the licensing terms and support agreements with the chosen CCM vendor to ensure alignment with your own environment.
- **Legal and Regulatory Considerations:** Be aware of legal and regulatory considerations related to CCM implementation.

ABOUT REGSCALE

RegScale overcomes speed, timeliness, and cost effectiveness limitations in legacy GRC by bridging security, risk, and compliance through our Continuous Controls Monitoring platform. Our CCM pipeline of automation, dashboards, and AI tools deliver lower program costs, strengthen security, and minimize painful handoffs between teams. Achieve rapid certification for faster market entry, anticipate threats via proactive risk management, and automate evidence collection, access reviews, and controls mapping. Improve the Return on Investment (ROI) of existing tools by seamlessly exchanging data with our centralized CCM data lake, enabling continuous monitoring of security, risk, and compliance controls. Heavily regulated organizations, including Fortune 500 enterprises – both financial institutions and other sectors – as well as the government and entities that serve them, use RegScale to enhance stakeholder trust, lower costs, adapt to evolving risks, and start and stay compliant. Our customers report a 90% faster path to compliance certifications and a 60% reduction in audit preparation efforts, strengthening security programs and reducing costs. For more information, visit www.regscales.com.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.

LEVERAGING CONTINUOUS CONTROLS MONITORING (CCM) FOR COMPLIANCE AND SECURITY

TAG

 RegScale