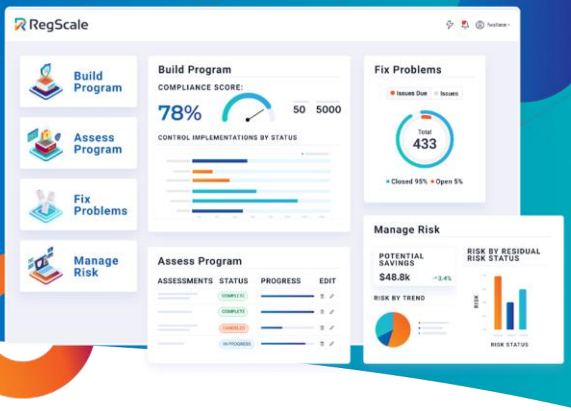
RegScale

SOLUTIONS BRIEF

Automation & CCM: Generate GRC Outcomes



The primary goal of GRC is to ensure that an organization is operating with responsibility, adhering to compliance standards, and effectively managing risks to support corporate objectives. This originates from documenting objectives, processes, and actual results that must be executed, reviewed, verified, and shared across multiple internal and external stakeholders. The entire end-to-end lifecycle of conducting these activities can be considered GRC, but what really matters here are the **outcomes from the GRC processes.** Outcomes include affirmed results, credible evidence, decisions that are made, and artifacts like reports, dashboards, attestations, systems security plans, metrics, and certifications.

Why GRC Tools Fail

- **Slow** to deliver outcomes
- **Expensive** to implement and sustain

If GRC tools are responsible for generating GRC outcomes, then why do they fail to deliver?

- **Speed:** GRC solutions are slow in attaining these outcomes and are not engineered to keep pace with the ephemeral, dynamic speed of tech and business today.
- **Cost:** Deployment and maintenance of GRC systems is expensive and grows over time with ballooning development costs and dedicated teams required to keep pace with increasing risk and compliance demands.

CCM: supercharge enterprise GRC and say goodbye to spreadsheets

With the nature of risk and compliance activities being dynamic and perpetual, they must be supported with **Continuous Controls Monitoring** (CCM) capabilities and benefits that extend beyond the means of traditional GRC tools. Organizations that have spent years and millions to customize their legacy GRC can still meet business needs by supercharging their IRM platforms with the nimble automation from a CCM platform. The processes that are slow and burdensome to execute can be automated and the outputs fed to the GRC so the investments in workflow, visualizations, and reporting can continue to deliver value, while not being restricted by the cost and lethargy of legacy systems. CCM delivers extreme automation by combining the ability to keep information always current with the predisposed knowledge of the desired GRC outcomes end state, meaning that quality data can be fed to the legacy tool, enhancing it to deliver GRC outcomes at scale.

RegScale

SOLUTIONS BRIEF

The 5 areas where CCM delivers great outcomes

1 Automation

Integrated automation capabilities into a purposeful digital thread that aggregates and extends inputs from existing control systems and owners. This enables decisions and affirmation of critical activities in the way the recipient–human or machine– needs to see it.

The Mechanism: CCM pipelines

A CCM pipeline is a set of bespoke end-to-end processes, tools, and integrations that combines CCM automation engines and purpose-built application modules to seamlessly automate critical processes in the compliance and risk management journey.

2 AI-Driven

AI-driven everything including explaining, authoring, extracting, and auditing of compliance, risk, and security controls, statements, and status.

3 Artifact Generation

Outputs and artifacts are native capabilities in a CCM platform. Decisions and Affirmations are made available in traditional formats and digital assets, allowing for efficient machine-to-machine leverage of the outputs. Compliance as code, for example, allows DevSecOps, IT, and security to improve the speed and accuracy of generating compliance artifacts using OSCAL/ machine-readable formats on command.

4 Scalable and Extensible

Conducting all the underlying processes needed to produce GRC outcomes is nimble in how it connects with existing tooling and scales for new use cases and system load. Walk-up user friendly ensures users know what to do at every stage in the process so maximum efficiencies are achieved.

5 Highly Secure

Built to the highest standards that embody the objectives of security and compliance integrity, like persistent cloud container reconstruction, that support the highest levels of certification, including SOC 2, FedRAMP High, and DoD IL 5.

What CCM Pipelines automate:

- **Package generation – from creation to submission** – tailored for regulatory environments demanding precision and speed.
- **Evidence gathering and validation,** ensuring an always-ready state for audits, assessments, and regulatory exams. They streamline evidence collection, updating, and organization using real-time APIs and pre-built integrations boosted by event-triggered actions and alerts.
- **Rapid certification by leveraging pre-built frameworks and offering dynamic dashboards for real-time status updates.** They conduct AI-powered audits and generate compliance packages in NIST-OSCAL (Open Security Control Assessment Language). Leveraging compliance as code, CCM pipelines feed a platform to create a proactive environment for compliance management by reducing manual data entry and providing continuous feedback through AI-enabled capabilities.
- **Cross-functional collaboration by integrating seamlessly with ITIL tools –** like Jira and ServiceNow – to automate and streamline the remediation process for compliance findings, issues, and to save costs.
- **End-to-end vulnerability lifecycle management, integrating the traditionally fragmented and manual process, including DevSecOps.** By leveraging automation, CCM Pipelines dramatically simplify the assessment, prioritization, remediation and associated reporting of security vulnerabilities for a proactive security posture.

How is it done today? The manual way.

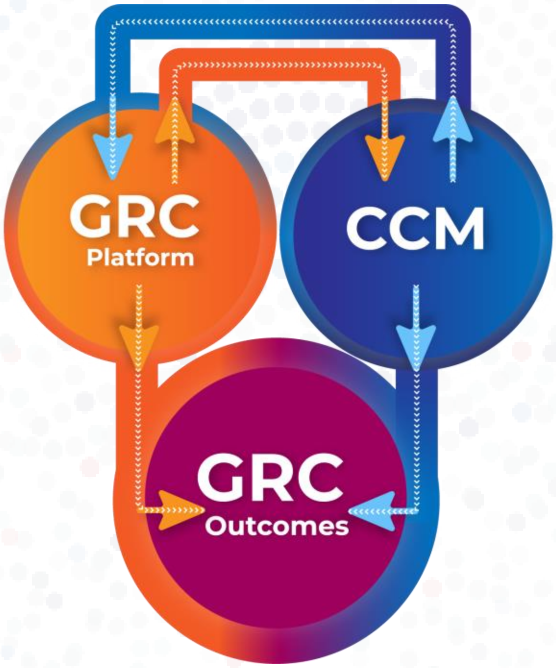
- **Collaboration Blockers:** conventional document-based collaboration methods are prone to staleness, version control issues, and significant productivity loss.
- **Lengthy Audit Preparation:** traditional methods extend audit preparation significantly, causing increased workloads and delayed certifications.
- **Manual Error and Rework:** manual errors are common, requiring significant time for correction and leading to delays, additional scrutiny from assessors, and potentially a failure to obtain authorization.
- **Slow Regulatory Adaptation:** keeping up with evolving regulations manually is slow and cumbersome, risking non-compliance and missed opportunities for market entry.
- **Productivity Disruption:** constantly responding to evidence requests decreases efficiency, contributes to audit fatigue, and increases team stress levels.
- **Continuous Monitoring Challenges:** establishing and maintaining continuous monitoring and package generation in a manual ConMon process is resource-intensive and complicated, hindering timely and effective security assurance.

Choosing CCM extreme automation means:

- **Accelerated Compliance:** customers on the CCM superhighway have reduced audit preparation and response time by 60%.
- **Intelligent Automation:** benefit from AI features that identify issues and suggest corrections, offering an “open book test” for your Security Plan / Compliance Documentation before submission.
- **Regulatory Alignment:** automate control mapping and leverage the power of assess once, satisfy many. Powerful reporting and visualizations of control and policy status in one-to-many format.
- **Collaborative Environment:** say goodbye to document staleness and copy/paste errors; step by step guide of every step in the process accompanies by real-time multi-level status boards.
- **Continuous Monitoring by Design:** use near real-time data to drive better, more timely decisions; schedule, monitor, report and act with confidence and urgency via continuous monitoring.

SOLUTIONS BRIEF

How do GRC and CCM solutions play together?



GRC Platforms

- Reduce costs and speed results by feeding legacy GRC platform with efficient, automated data to create faster GRC Outcomes
- Increase agility with real-time data and control information while maintaining a single pain of glass for centralized accountability and leveraging existing workflows and reporting while
- Improve security operations and security posture with near real time risk and compliance information, delivered with extreme automation
- Utilize the benefits of CCM engines and Compliance as Code to modernize legacy GRC and support cloud and serverless worlds without wholesale lift-and-shift effort

GRC Outcomes

- Audit/Assessment Management
- Governance and Decision Support
- Compliance Posture
- Cyber Hygiene visibility
- Risk and Compliance Posture
- Remediation workflows
- Risk quantification
- Issues Management
- Reporting and Dashboarding
- Cyber Risk Quantification

CCM

- API first, integrates everywhere
- AI driven, smart automation
- Compliance as Code / OSCAL
- Flexible yet prescriptive; rapid time to value
- Highly Automated and near real time with event-driven architecture
- Purpose built to generate regulatory reports; always audit ready
- Cloud-native, resilient, and scalable
- Walk-up User Friendly
- Works seamlessly with your cyber security stack
- Highly Secure, highly scalable

Ready to get started?

RegScale

✉ Sales@RegScale.com RegScale.com

July-2024-V1