RegScale

WHITE PAPER

Continuous Controls Monitoring

GRC in 2030

A CISO SURVIVAL GUIDE

RegScale.com

Why You Want to Read This White Paper

Governance, risk, and compliance (GRC) sits at a turning point for disruption. CISOs face a number of issues that were once mere annoyances or inefficiencies—but now pose an impending crisis for organizations. This is a must-read guide for CISOs to help you pinpoint near-future pain points and educate and upskill your teams by leveraging a continuous controls monitoring (CCM) solution.

Today's GRC programs suffer from three main problems:

1. **Sprawl.** As a result of digital transformation, Chief Information Security Officers (CISOs) are managing a growing portfolio of applications that commonly exist outside of the environments traditionally managed by a Chief Information Officer (CIO). This combination of more applications—being managed with less rigor and located in more places/cloud environments—has dramatically increased complexity. So, too, has the continuously growing list of compliance frameworks, from open source (like NIST) to proprietary (like ISO). This white paper will address how CCM can reduce these complexities.
2. **Lack of boundaries.** Corporate computer networks used to be on-premises or air-gapped: discrete and accessible only through a firewall—tightly controlling access to sensitive data. Today's cloud-native world has our data spread across multiple online networks, accessed from many device types and a wide range of people (employees, partners, suppliers, customers, etc.). As a cloud-native solution, CCM provides an ideal interface for integrating, monitoring, and reporting on all these data sources in real time.
3. **Decays over Time.** Due to the scale, complexity, and fluidity mentioned above, risk and compliance paperwork gets stale, atrophied, and backlogged. As more applications, frameworks, and environments emerge, this paperwork decays even faster, creating a burden that traditional tools of the trade (documents, spreadsheets, and legacy GRC solutions) cannot overcom, CCM can.

And if you think it's challenging now…it will get worse. The technological world in 2030 promises a landscape radically transformed by unprecedented advancements. As the cloud engulfs everything, organizations will grapple with **ephemeral technology**, **a surge in regulations, AI/artificial general intelligence (AGI), and an unrelenting need for speed** that most organizations aren't ready for.

This white paper discusses the ongoing evolution of compliance, the advantages of a CCM methodology, and the steps that organizations, CISOs, and their teams will need to take to assure security—and threatscape survivability—in the year 2030 and beyond.

What is Continuous Controls Monitoring (CCM)?

A critical aspect of modern governance, risk management, and compliance (GRC), continuous controls monitoring (CCM) involves the continuous assessment and surveillance of internal controls within an organization's processes, systems, and data to ensure compliance with regulatory requirements, mitigate risks, and maintain operational effectiveness. At its core, CCM aims to provide real-time visibility into the effectiveness of internal controls by leveraging automation, data analytics, and risk-based monitoring techniques. Instead of relying solely on periodic audits or manual assessments, CCM enables organizations to proactively monitor their control environment, identify anomalies or deviations from expected norms, and take corrective actions promptly.

RegScale

Table of Contents

CHAPTER 1

Ephemeral Technology: How Do You Keep Up?

The first challenge that compliance and security professionals must face is the ephemeral nature of IT infrastructure. "Most of today's regulations were built for an old world, where everything was client-server based, behind a firewall, and relatively static," says Travis Howerton, Co-founder and CEO of RegScale. "You could document it. You could harden it."
The reality is that IT will never be this simple and easy to contain again.

The trend of everything moving to the cloud

In today's world, workloads are increasingly ephemeral. Everything is becoming cloud native, hosted on "serverless" systems that auto-scale up and down based on load. In addition to data systems residing everywhere and all at once, they are very much a moving target.

Unfortunately, while these data systems have evolved, the static process that many CISOs and compliance teams have been using for documenting inventory and asset management has not. The traditional approach of using documents, spreadsheets, and legacy GRC tools lacks the agility, speed, and intelligence needed for tomorrow's dynamic environment.

"In the past and even today, many GRC teams end up generating a lot of paperwork that nobody wants to write, and nobody wants to read—just to basically be able to pass audits and demonstrate to regulators that you're meeting your compliance obligations," recalls Howerton. "But as cloud systems have become dominant, managing compliance manually using Word documents and Excel spreadsheets quickly degrades from being 'this cost center nobody enjoys' to being something that doesn't work at all."

> "Most of today's regulations were built for an old world, where everything was client-server based, behind a firewall, and relatively static. You could document it. You could harden it."
>
> **-Travis Howerton | Co-founder and CEO | RegScale**

Moving to CCM as a Cloud-Native Version of GRC

Organizations are already prioritizing digital transformation initiatives and moving IT components from on-premises data centers to the cloud.
As this process accelerate, CISOs will need a better way to continuously monitor security, identity, and access management across their public and private environments. This complexity makes it imperative for CISOs to adopt CCM as a Cloud-Native Version of GRC solutions, and CCM provides the greatest advantages.

By harnessing CCM, organizations can optimize their GRC processes, enhance operational efficiency, and achieve greater resilience in an increasingly sprawling, boundaryless, and interconnected business landscape.

CCM eliminates data gaps—enabling continuously-accurate documents

CCM as a Cloud-Native Version of GRC solutions can eliminate data gaps and unify disparate tools, controls, evidence, and even legacy and third-party systems. Previously, such data sources were often locked in silos due to disconnected manual processes that relied on point-in-time snapshots. That prevented a clear picture of overall compliance posture and risk.

CCM as a Cloud-Native Version of GRC architecture enables the creation of data lakes that can then be managed using continuous controls monitoring (CCM)—providing near real-time visibility of security, risk, and compliance with those controls. The eventual transition would shift from creating static, paper-based regulatory documentation to a more dynamic process that accurately reflects an organization's current state and outputs continuously-accurate documents on the fly. That would be a welcome change for compliance teams, auditors, and regulators alike.

What is Continuous Controls Monitoring (CCM)?

A critical aspect of modern governance, risk management, and compliance (GRC), continuous controls monitoring (CCM) involves the continuous assessment and surveillance of internal controls within an organization's processes, systems, and data to ensure compliance with regulatory requirements, mitigate risks, and maintain operational effectiveness. At its core, CCM aims to provide real-time visibility into the effectiveness of internal controls by leveraging automation, data analytics, and risk-based monitoring techniques. Instead of relying solely on periodic audits or manual assessments, CCM enables organizations to proactively monitor their control environment, identify anomalies or deviations from expected norms, and take corrective actions promptly.

CHAPTER 2

Rising Regulatory Burden and Scope Creep

The second challenge facing CISOs now and into the next decade is the growing number of regulations and the compliance scope creep that comes with them. Every day it seems there is a regulatory update, a new framework published or updated, EU legislation, SEC rules, specified state regulation, DHS CISA guidance, or an OMB memo/mandate that compounds the compliance demands of organizations.

On top of updates to existing rules and frameworks, this burden will only increase as new threats emerge and lawmakers pass new legislation. Organizations can anticipate more complex, comprehensive regulations. These new rules will be bigger and have sharper teeth—against threats that come at greater speed and across a vastly more complex technology landscape. Such complexity will demand continuous monitoring, and automated GRC tools that function far beyond the human capabilities of CISOs' teams.

Here are some examples of recent, evolving, and predicted regulations that promise to impact CISOs and the compliance processes they manage:

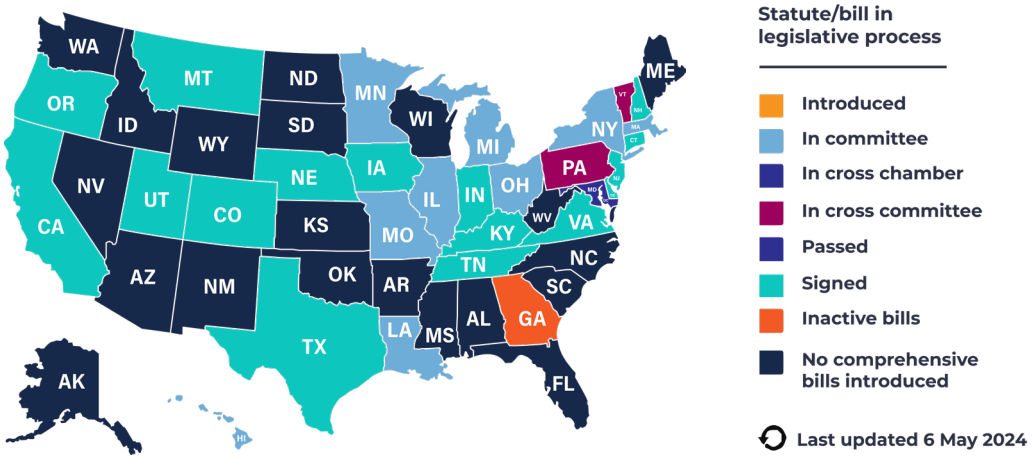
Getting bullish on SEC regulations

Organizations will see more attention from the Securities and Exchange Commission (SEC). More than two decades since its passing, the Sarbanes-Oxley Act (SOX) continues to evolve, with new and proposed rules. Other near-term legislation includes the SEC's Landmark Climate Disclosure Rule. Of special interest to CISOs is the SEC's recent mandate for cyber report cards—since cybersecurity is being viewed increasingly as a material risk to the business that needs to be disclosed so people can make better investment choices. This trend will continue.

Data privacy and consumer protection laws

More stringent data privacy laws are on the horizon. The SEC approved updates to the Privacy Act, which is the principal law governing the handling of personal information in the federal government. The California Consumer Privacy Act (CCPA)—which closely mirrors Europe's General Data Protection Regulation (GDPR), gives consumers more control over the personal information that businesses collect about them. As seen recently with the CCPA, new updates happen fairly regularly.

US State Privacy Legislation Tracker 2024



Today's current state-by-state patchwork of privacy laws makes it very difficult for companies to maintain compliance, so a more nationwide approach to consumer privacy would likely be a welcome change leading up to 2030.

- Organizations can also expect to see more critical infrastructure mandates and reporting coming out of the U.S. This includes more things around business resiliency for critical infrastructure. You're already seeing that with the Digital Operational Resilience Act (DORA) in Europe.

AI related regulations on the rise

The United States is examining the regulation of AI at both a state and federal level. Since 2019, 17 states have enacted 29 bills focused on regulating the design, development, and use of artificial intelligence.[2] These bills primarily address two regulatory concerns: data privacy and accountability. Legislatures in California, Colorado and Virginia have established regulatory and compliance frameworks for AI systems. According to research by the Brookings Institute, the focus of these regulations is on oversight of the impact of the algorithm on people's civil rights, opportunities for advancement, and access to critical services rather than specific AI or machine learning (ML) tools themselves.[3]

While the U.S. does not yet have federal legislation regulating AI, the path has been laid. In the 118th Congress, more than 80 bills have already been introduced this session, with many more coming down the pike.[4]

In March of 2024, the Office of Management and Budget issued Memorandum M-24-10 directing agencies on how they must implement the President's recent Executive Order addressing use of Artificial Intelligence. This Memo underscores the huge impact of AI on government operations and requires all federal agencies to "seize the opportunities AI presents while managing its risks."[5] This OMB Memo requires agencies to prioritize and put AI in the same category as other important information technologies. Among the more than one dozen stipulations, this memo requires each agency, on an annual basis, to conduct risk assessments and individually inventory each of its AI use cases.

"AI is here. Embrace it. Use it. Have a policy for it, " says Ron Sivonda, CISO for ScaleSec, during the 2024 ISC2 GRC Virtual Summit. "Figure out where you're going to put your data, because if you're a private company with a bunch of proprietary data, do you want to be stuffing your blueprints into ChatGPT? Because then they're going to live there and it's going to eat them. So be aware of that and have a policy for that."

> "AI is here. Embrace it. Use it. Have a policy for it."
>
> **- Ron Sivonda | CISO | ScaleSec**

Faced with ever-increasing regulations, escalating cyber threats, stringent data privacy regulations, the impacts of AI, and other disruptions, GRC software providers will continue bolstering their solutions with robust cybersecurity and privacy management features. This ensures continuous monitoring and enforcement of compliance standards, meeting the evolving needs of organizations in safeguarding their data and operations.

CHAPTER 3

Harnessing Artificial Intelligence for the Good of GRC

AI, generative AI (GenAI), and artificial general intelligence (AGI) will play an increasingly disruptive part in information security and compliance leading up to 2030. These technologies are a double-edged sword for CISOs.

AI as a tool to alleviate workload

While AI may lack the nuanced context provided by skilled professionals, its potential to alleviate burdens is evident in streamlining business operations. AI holds the unprecedented power to free compliance practitioners from doing tedious and manual tasks.

"I think a whole bunch of things we count on humans to do are stare-and-compare exercises," says Howerton. What I think will not be replaced by machines is strategic decisions for their business. We are supercharging humans. They've got a huge backlog of more valuable work they could be doing."

Krista Arndt, CISO for United Musculoskeletal Partners, highlights the value of AI-generated templates in saving time, resources, and money, enabling organizations to tailor policies effectively to their specific business needs. This approach fosters greater efficiency and customization while ensuring alignment with organizational objectives and regulatory requirements.

Christian Schnedler, Managing Director, Cyber Practice Lead, at PE firm WestCap Management, believes the "disruption" caused by AI is largely due to finally having a user interface—ChatGPT—that was approachable and lowered the bar for mass adoption. "I am extremely interested in what happens when the machines start talking to each other and you're seeing some novel uses… and becoming much more efficient in a variety of different arenas," says Schnedler.

How AI Supports GRC Duties

- **Answering canned questions** via MS Teams, Slack, and other intranet apps.
- **Writing documents** such as policies customized for the organization.
- **Drafting control implementation statements** in minutes.
- **Reviewing documents** such as policies, procedures, for compliance.
- **Train and explain** policies for the organization.
- **Internal auditing** to highlight errors and augment human auditors.
- **Creating a control gap analysis scorecard** with suggested improvements.
- **Updating compliance documents** by automatically proposing changes.
- **Monitoring intranet conversations** for alerting to non-compliance issues.
- **Optimizing meetings** by generating agendas, transcripts, and more.
- **Answering customer questionnaires** such as cybersecurity surveys.

AI as a tool to supercharge compliance

AI and ML technologies are already transforming GRC software capabilities, facilitating predictive analytics, anomaly/gap detection, and trend analysis. Future advancements will proactively empower risk anticipation and enhance decision-making processes, marking a significant evolution in how organizations approach governance, risk management, and compliance.

> "AI will be leveraged to help simplify the management of your security posture and to help identify the signal from the noise in terms of which risks are acceptable versus which ones are absolutely critical for you to address."
>
> **- Christian Schnedler | Managing Director, Cyber Practice Lead | WestCap Management**

In the realm of security, functionalities like continuous auditing contribute to cultivating more effective CISOs and teams by dismantling siloed views on threats and defenses.[6] Moreover, properly programmed AI tools offer significant advantages in policy development, addressing the repetitive nature of standardized frameworks.

Other high-impact areas where AI can help include:

- **Automated risk identification and continuous risk management.** Leveraging AI for risk management-including those risks linked to third parties-lets organizations bolster resilience, compliance, and strategic decision-making amid growing uncertainties. GRC software will continue to provide ongoing monitoring, assessment, and mitigation of risks in real-time to help security operations centers timely identify emerging threats and maintain compliance with regulatory requirements.
- **Enhanced predictive analytics.** AI and ML algorithms embedded within GRC software platforms will help organizations better detect patterns of over-testing or under-testing of controls and prioritizes risk assessments more effectively.

Schnedler predicts that over the next five or six years, AI will have a clarifying effect on risk assessment. "AI will be leveraged to help simplify the management of your security posture, and to help identify the signal from the noise in terms of which risks are acceptable versus which ones are absolutely critical for you to address."

With its powerful AI-driven automations, CCM is posed to replace numerous human workloads, freeing them to perform more strategic tasks while completing these processes in less than a quarter of the time compared to human practitioners. Having used RegScale's AI engine, RegML, Tom Volpe, Jr., Vice President of C2 Labs, says "You get your cup of coffee and by the time you're done, it completed 80% of the work."

ScaleSec's CISO, Ron Sivonda, has experienced this firsthand. "I watched an AI chatbot at Google Next go through a security command center and tell me what all the findings meant," he recalls. "You could just type in a chat window and say, 'Hey, do I have to worry about this finding, or is that a misconfiguration?' and it was answering me like a human SOC analyst would answer me."

Meanwhile, widespread AI adoption also represents plenty of green fields for threat actors.

Alleviating AI's threat to cybersecurity

According to a leading analyst firm, the popularity of using GenAI applications by businesses —both in their strategic use cases as well as in unmanaged ways by their employees—creates new attack surfaces, poses privacy risks, and threatens organizations' sensitive data and intellectual property. The report also warns that threat actors leveraging GenAI for sophisticated phishing and other attacks will create new requirements for AI application security.

All these trends build on technology that is already available. AI technologies are already widely adopted in hybrid and cloud-native IT environments. That's both a benefit and a problem. "It's a very interesting solution that's both helping and harming in terms of the complexity that security leaders have to deal with," says Schnedler.

Along with the efficiencies of AI, its mass adoption by organizations also represents an entirely new attack vector. "That's leading to an expansion of scope where (security teams) are being asked by their leadership to also contemplate different methods of attacking or otherwise leveraging AI as a way for adversaries to gain access to intellectual property and hurt things."

Striking a balance

Many industry analysts admit that businesses will embrace generative AI, regardless of security. As a result, CISOs should put guardrails in place to assure safe usage—and defense from—AI.

Rather than waiting for government regulations around AI, organizations can develop their own internal policies and controls. One good starting point for self-governance would be a framework such as the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF).[7] Finally, organizations can gain an advantage by educating their employees on the inherent risks of AI tools—and upskilling them in their appropriate usage.

CHAPTER 4

Solving the Skills Gap Problem

One of the classic challenges of digital transformation—like the one happening in governance, risk, and compliance—is preparing your team for the future. Upskilling is very important to stay relevant. Auditors also need to keep themselves upskilled, so they are less dependent on legacy compliance programs providing them with reports in outdated formats and have the current knowledge of what AI-driven capabilities are possible to help them make better risk-based decisions.

Technical skills gaps will pose an exponential problem for organizations' compliance teams. This world won't slow down to allow a company's risk and compliance programs to catch up. The big organizations that can't embrace these trends won't exist in the future.

According to a report by Deloitte, "Many of the hard skills to do a job well will be obsolete in just a few years."[8] Upskilling is a win-win for organizations and their teams. People have a chance to add more value to their careers and what they do, and how they're compensated. This change can be a positive if they embrace it and be part of it.

"When I was hiring for my security teams years ago, I never really expected any of my people to have Python," recalls Gary Hayslip, CISO, SoftBank Investment Advisers. "But in today's day and age…you're doing a lot of stuff with APIs and generative AI and a lot of ChatGPT's stuff. We are building internally, so Python and PowerShell and being able to script are huge. That's where the future's leaning."

> "You're doing a lot of stuff with APIs and generative AI and a lot of ChatGPT stuff. We are building internally, so Python and PowerShell and being able to script are huge."
>
> **-Gary Hayslip | CISO | SoftBank Investment Advisers**

"This is one of those areas where it's very easy to see yourself getting left behind," cautions Howerton. "When your staff doesn't know what compliance as code means, or asks 'What is a YAML file? What is this JSON thing? Just give it to me in Excel like I always had it,' then they are either going to get disrupted by this trend—or they're going to hold your organization back from taking advantage of all these new emerging technologies."

What is Compliance as Code?

Imagine being able to deliver machine-readable RMF/ATO/FedRAMP artifacts on demand at the push of a button. That's just one example of the advantages of compliance as code.

Compliance as code refers to the practice of integrating compliance requirements directly into software development's code and infrastructure deployment processes. This approach ensures that compliance rules and regulations are automatically enforced throughout the development lifecycle, from code creation to deployment and beyond.

By embedding compliance checks and controls into the code itself, organizations can streamline the compliance process, reduce manual effort, and mitigate the risk of non-compliance. Compliance requirements, such as security standards, data protection regulations, and industry-specific mandates, are translated into code-based policies that are applied consistently across the development environment.

Using compliance as code tools and practices, developers can automate compliance testing, monitor for violations in real-time, and respond promptly to any issues that arise. This approach helps organizations achieve greater agility, security, and reliability in their software development processes while ensuring adherence to regulatory requirements.

To learn more, visit:

RegScale.com/continuous-monitoring-built-on-oscal

Solving staff shortages in the future

An organization's cybersecurity strategy is only as strong as its employees—and those employees are becoming harder to find.

Cybersecurity Skills Gaps by the Numbers

92% of organizations reported skills gaps—including in cloud computing security roles.

ISC2 Cybersecurity Workforce Study

56% of organizations have trouble recruiting cyber talent, and 54% have trouble retaining it.

2023 Fortinet Cybersecurity Skills Gap Report

67% of cybersecurity professionals reported that their team is understaffed.

ISC2 Cybersecurity Workforce Study

Upskilling security teams to mitigate the skills gaps

Here is a very real business case for an automated GRC solution: to not only free up the organization's cybersecurity and compliance staff to do more impactful projects, but to bridge many skills, especially in mundane tasks.

"Even if you were blessed with tons of resources, good luck finding skilled and qualified cyber security staff to execute these functions," warns Howerton. "There is more supply (of jobs) than demand (skilled people) and even if you could find them, this isn't the fun and exciting cyber work," says Howerton. "The market doesn't have enough people with these types of skill sets—which is where software augmentation can really help, by overcoming the need to apply human labor to the problem."

The goal of GRC automation into the year 2030 is not to eliminate all the people in the compliance industry. It's going to supercharge them—so they can get all the work done with the same number of people.

CHAPTER 5

Anticipated Trends in GRC by 2030

Those who follow the field anticipate an ongoing evolution of GRC practices and tooling that reflects a more interconnected, automated, integrated, and user-friendly approach by 2030.

Among the anticipated trends:

Continuous controls monitoring

The emergence of AI-powered, automated GRC solutions marks a significant advancement in the capability to monitor controls. Leading the way towards this transformation is continuous controls monitoring (CCM), defined by a leading analyst firm as "a set of technologies to reduce business losses through continuous monitoring and reducing the cost of audits through continuous auditing of the controls in financial and other transactional applications."

CCM streamlines GRC audits and outcomes, providing real-time assessment, analysis, and reporting about the status of an organization's security controls. Controls are at the center of policies, risk management, and compliance. By enabling always audit-ready documentation, this CCM methodology reduces audit fatigue and saves practitioners weeks (even months) of time preparing for such time-intensive compliance frameworks as:

- **Federal Risk and Authorization Management Program (FedRAMP)**
- **International Organization for Standardization (ISO)**
- **System and Organization Controls (SOC 2), and**
- **Other business-critical certifications**

"One of the most painful processes today in an organization-not only from the time intensity that it takes to complete granular audits but getting the resources to do so-is going to be that paperwork of checks and balances," says Arndt. "Having continuous, automated audits is just one small (but very important) piece of that puzzle towards getting continuous risk management in your security program."

SOC 2

A SOC 2 (System and Organization Controls 2) certification is especially valuable to organizations that provide cloud computing and Software as a Service (SaaS) solutions, attesting they meet a high, independent standard for the controls they in place to ensure the security, availability, processing integrity, confidentiality, and privacy of customer data.

To complete an initial SOC 2 Type 1 audit, the process typically takes organizations about 300 hours (almost eight work weeks if conducted manually. Also using traditional manual methods, the additional SOC 2 Type 2 report takes approximately 400 hours.

Howerton suggested another advantage of using CCM to "supercharge" employees during certification and audit preparation was that this could help organizations stop villainizing compliance professionals, despite the audit fatigue they might induce. "Compliance professionals and auditors do great work, and they help you a lot," Howerton said "The part we all hate is the amount of time, money, and energy it takes to feed them. It's a good thing to have somebody doing those checks because they're helping you make better risk-based decisions."

The advantages of CCM go far beyond speeding and simplifying audit prep. CCM improves the capability of organizations to make better business decisions. Much of what human compliance practitioners do amounts to "stare-and-compare exercises". These are mundane, error-prone tasks that make the ideal application of CCM's AI-powered automations. More important tasks that will not be replaced by machines include strategic business decisions for the organization. CCM represents the machine taking workload off the organization's top minds—Informing them with better data so they can now spend more time making the right decision.

Ongoing, real-time risk assessment is another game-changer CCM brings to the table. "I love the ability to scan our resources and understand where they lie when it comes to a compliance perspective as well as a security posture perspective," Arndt says, regarding the organization's use of a CCM solution.

As more and more organizations lean into the API economy, automated risk identification and continuous risk management will be especially critical to success.

"The problem is that we have 'stack overload', where we have too many tools and so it's about really being better at our workflows—how we use that data to make the right decisions," says Howerton. "I think the future is going to see a trend towards platform consolidation… combined with solutions to sift through all this data and make sense of it, along with better workflow solutions to make sure we're assigning the work correctly and getting the human eyes on the right targets faster.

Compliance as code

In addition to continuous controls monitoring, an increasing number of software providers are integrating compliance as code into their development processes to bolster risk management practices for their clients. Compliance as code involves the use of automated infrastructure and tools to enforce regulatory and security standards within an organization's IT infrastructure.

(More about compliance as code in chapter 4)

"The industry is built on massive amounts of paperwork that nobody wants to read, nobody wants to write, and is out of date the day it was published," says Howerton. "Having machines attest to their own state to create self-updating paperwork is the future. We are fans and supporters of emerging compliance as code standards such as NIST OSCAL, which is moving compliance and risk processes towards a more modern DevOps approach."

Today, manually creating compliance artifacts in documents and spreadsheets to describe dynamic environments is increasingly impractical. Not only does compliance as code facilitate machine-to-machine attestation, but it also provides the foundational technology necessary for CCM. This seamless integration of compliance as code into the development pipeline not only streamlines processes but also enhances overall risk management capabilities.

Compliance as code empowers security analysts to make risk-based decisions based on timely and accurate data, which is continuously updated rather than relying on snapshots collected at specific points in time. This approach ensures that decisions are grounded in the most up-to-date information available, providing greater context and reliability. Additionally, incorporating third-party validation further enhances the credibility and robustness of the data-driven decision-making process.

> "The industry is built on massive amounts of paperwork that nobody wants to read, nobody wants to write, and is out of date the day it was published. Having machines attest to their own state to create self-updating paperwork is the future."

-Travis Howerton | Co-founder and CEO | RegScale

CHAPTER 6

The Path to 2030 Through Innovations in GRC

As GRC and cybersecurity teams discover new tools to generate accurate, timely, and actionable insights, we can expect risk managers, compliance officers, and the documentation-driving audits also to change. That's going to happen more rapidly than you may think.

> "The ones who are deniers of what's coming, who don't think deeply about what's coming are ones that get disrupted."
>
> **-Travis Howerton | Co-founder and CEO | RegScale**

By 2030, Continuous Controls Monitoring will replace legacy GRC and will be indispensable to organizations, by integrating advanced AI and automation to provide real-time risk insights, streamlining compliance processes, and facilitating proactive decision-making.

In fact, the role of CCM will extend beyond mere governance, risk, and compliance management to become a strategic enabler for achieving business objectives-and fostering a culture of transparency and accountability throughout the organization.

"The ones who are deniers of what's coming, who don't think deeply about what's coming…are ones that get disrupted," Howerton says. "But if you think deeply about what's coming and you've got a plan, you're going to be much further ahead of those who don't."

Your adversaries are paying attention and adapting to change. You should too, Schnedler said. "This is coming whether you like it or not-whether it comes via an auditor and regulator, or it comes in a much more damaging way. We all must understand that change is afoot and it's not going to go back."

CCM makes a great place to start

Like all things in the future, there is an opportunity for it to be a better place and an equal opportunity for it to break everything we have. The key to picking which side you end up on is to build a strategy now to enable these key capabilities for your future.

"I had an old boss who told me, "The best plans start with the truth. You can accept it now, or you can accept it later, but it will still be true. It is always faster and cheaper to accept it now,'" recalls Howerton. "The truth is that the world is changing faster than it ever has and our legacy risk and compliance programs will never be able to keep up. We have to do something different, and the time to do it is now."

If you want to learn more about how to prepare your risk and compliance programs now and for 2030, our experts at RegScale can help. Contact us today to get a demo on how our continuous controls monitoring platform can deliver AI-powered automations, compliance as code, and self-updating paperwork to best position your organization for the future.

RegScale.com

Endnotes

1 Andrew Folks. "US State Privacy Legislation Tracker." International Association of Privacy Professionals (IAPP). April 29, 2024. https://iapp.org/

2 Rachel Wight. "Artificial Intelligence in the States: Emerging Legislation." The Council of State Governments (December 2023). http://www.csg.org/

3 OMB, Memoranda: https://www.whitehouse.gov/omb/information-for-agencies/memoranda/

4 Jeremy D'Hoinne, Avivah Litan & Peter Firstbrook. "4 Ways Generative AI Will Impact CISOs and Their Teams." Gartner ID G00793265 (June 29, 2023).

5 David Barnes. "The future of regulation: Navigating the intersection of regulation, innovation, and society: Regulation, disruption and the future of work". Deloitte. https://www.deloitte.com/global/en/issues/trust/future-of-regulation.html. Accessed May 2024.

6 "How the Economy, Skills Gap and 2023 Artificial Intelligence are Challenging the Global Cybersecurity Workforce." ISC2 Cybersecurity Workforce Study, 2023. 2023.

7 "2023 Cybersecurity Skills Gap: Global Research Report." Fortinet Training Institute. March 2023.

8 "AI Risk Management Framework". NIST. https://www.nist.gov/itl/ai-risk-management-framework. April 2024.

9 Michael Kranawetter, Sema Yuce & Arthur Sivanathan. "CISO Effectiveness: Handling Security Audits, Part 1: Before an Audit". Gartner. February 28, 2024.

RegScale

About RegScale

RegScale is a continuous controls monitoring (CCM) platform that enables positive GRC outcomes. Using RegScale, organizations overcome speed, timeliness, and cost-effectiveness limitations in legacy GRC tools by bridging security, risk, and compliance through controls. Our CCM automation engines and AI tools operate independently but are tightly coupled, lowering program costs and eliminating the corrosion that grinds current GRC programs to a halt. Improve ROI of existing tools, achieve rapid certifications, anticipate threats via proactive risk management, automate evidence collection, integrate compliance into DevSecOps processes, and map controls faster. Heavily regulated organizations, including Fortune 500 enterprises and the Federal government, use RegScale to enhance stakeholder trust, adapt to evolving risks, and stay compliant. Our customers report a 90% faster path to certifications and a 60% reduction in audit preparation efforts.

Contact Us

Phone **(202) 991-7881** | **Regscale.com**

Address **1775 Tysons Blvd. Fl. 5, Tysons, VA 22102**

Ready to get started?