INSIGHTS

RegScale

Rewriting the Regulatory Exam Playbook

Banks are navigating an increasingly complex regulatory landscape, from challenges with operational resilience and AI implementation to global market uncertainty and evolving cybersecurity threats. Yet amid these high-profile challenges, one fundamental obstacle continues to fly under the radar: regulatory exam management.

For most financial institutions, regulatory compliance has become a perpetual cycle of manual activity that drains resources, stifles creativity, and pulls focus away from customer-facing innovation. The burden is significant and growing… but it doesn't have to be this way. Banks are beginning to flip the script, transforming regulatory exam management from an innovation killer into a genuine strategic advantage.

Out of Sync and Over Budget: The Regulatory Compliance Challenge

The gap between security, risk, and compliance continues to plague financial institutions. According to our 2025 State of Continuous Controls Monitoring Report, only 44% of CISOs describe their compliance and security programs as completely synchronized.

Only

44% OF CISOs

say their compliance and security programs are fully synchronized

While regulatory measures are absolutely essential for protecting infrastructure, they've created a complex web of challenges around exam management. These challenges are multilayered and increasingly demanding:

- ✓ Operational overhead has skyrocketed as banks are required to maintain extensive documentation, conduct regular assessments, and implement multiple control layers.
- ✓ Failed exams cascade into follow-up requests, Matters Requiring Attention (MRAs), Matters Requiring Immediate Attention (MRIAs), and heightened scrutiny, while inconsistent responses to regulatory bodies can trigger additional audits.
- ✓ Regulatory fragmentation forces institutions to integrate different — sometimes conflicting — requirements for different jurisdictions and frameworks.
- ✓ Rapidly evolving requirements demand constant adaptation.
- ✓ Cyber threats grow more sophisticated daily.

Technology leaders in banking and finance face an impossible tradeoff between addressing these regulatory exam management issues and delivering innovation. They have an essential obligation to meet policy and compliance requirements, but they also need to prioritize innovation for their long-term survival in a rapidly evolving industry.

Did you know? Out of 10 sectors surveyed, financial services had the most organizations devoting 50%+ of their current compliance workload to new requirements.

Learn more about the state of GRC automation across finance and other sectors in the 2026 State of Continuous Controls Monitoring Report.

Streamlining GRC with Continuous Controls Monitoring

Continuous Controls Monitoring (CCM) and compliance automation represent a fundamental shift in approach: moving from periodic, sample-based assessments to automated, real-time monitoring of controls.

At the core of CCM is comprehensive visibility across the control environment, the exam requirements, the organization's security posture, and more. It allows for a far more proactive approach to compliance and risk, and it frees up teams to focus on strategic priorities like driving innovation. It also offers automated evidence collection, self-updating paperwork, enhanced visibility, and more efficient drafting of SSPs and control statements.

Transforming the culture and tools around regulatory exam management is easier said than done. But there are tried-and-tested approaches that can help banks cut costs, slash manual processes, and future-proof their GRC programs.

One key step is to create an organizational ecosystem where security, compliance, and business objectives are naturally aligned, and not competing priorities. This kind of thoughtful alignment requires purposeful bridge-building between security, risk, and compliance departments, as well as a rigorous, intentional standardization of processes. Having clear, repeatable processes will ultimately create a common language for GRC that all stakeholders can understand and trust.

Common Controls Framework

Another key element of a successful compliance automation program is implementing a common controls framework. This approach creates an efficient foundation for Continuous Controls Monitoring by:

- ✓ Mapping controls once and applying them across multiple regulatory requirements
- ✓ Creating a unified compliance language that works across disparate tools and departments
- ✓ Eliminating redundant assessments through an "assess once, use many" approach

The Cyber Risk Institute (CRI) framework exemplifies this approach, particularly as part of its collaboration with RegScale's CCM platform. The CRI Profile v2.1 — a cybersecurity framework developed by and for the financial sector based on globally recognized standards — helps improve efficiency and harmonization among different standards. Organizations implementing the RegScale-CRI solution have seen dramatic improvements, including:

- ✓ 60% reduction in audit prep time
- ✓ 80% improvement in documentation accuracy
- ✓ 40% faster regulatory response times
- ✓ 10x scalability that frees up teams to focus on strategic priorities

> "Financial institutions have long been focused on point-in-time assessments and want to move to continuous control monitoring. We are excited to load the CRI Profile v2.0 into offerings like RegScale's to assist financial institutions in streamlining regulatory compliance."
>
> **- Josh Magri, Founder and CEO, CRI**

Compliance-as-Code and OSCAL

Banks can further accelerate their CCM transformation by embracing Compliance-as-Code, which is transforming GRC in much the same way that Infrastructure-as-Code revolutionized data center management. By implementing compliance requirements directly into the CI/CD pipeline, organizations can automate testing, streamline reporting, and adapt to regulatory changes with unprecedented speed.

One of the best ways to do so is with NIST OSCAL, a machine-readable format best known for its use in FedRAMP certification. Given its growing adoption, OSCAL represents the future of compliance across sectors, enabling dramatic improvements in efficiency and accuracy.

As a founding member of the OSCAL Foundation (a NIST-led initiative that aims to standardize and streamline compliance requirements) and the originators of OSCAL Hub, RegScale has architected its CCM platform to provide full support for OSCAL catalogs, profiles, security plans, POAMS, and more. We remain deeply invested in the future of Compliance as Code and OSCAL for their potential to simplify and accelerate compliance across the public and private sectors.

The Investment Question: Is Your GRC Future-Proof?

Of course, the real question isn't whether your GRC is compliant today, or whether your regulatory exam management is efficient this year; it's whether your programs are purpose-built to adapt and thrive. That includes:

- ✓ Automation as a force multiplier to slash control owner workload
- ✓ AI-enabled analytics to transform raw data into actionable insights
- ✓ Proactive audit preparation rather than reactive scrambling
- ✓ Consistent regulatory responses delivered with accuracy, speed, and confidence
- ✓ Enhanced collaboration between risk, compliance, and business teams
- ✓ Liberated tech leadership focused on customer-facing innovation

The financial impact is substantial. Every dollar and hour saved on compliance becomes a resource redirected toward developing innovation, managing security and risk, and handling new regulatory requirements with ease.

To learn more about transforming your regulatory exam management, explore our regulatory response resources.