BLOG

RegScale

Top GRC Challenges for Banks & Financial Services

Regulatory scrutiny in the finance industry has intensified, with constantly evolving compliance requirements creating a complex landscape of over 2,500 distinct regulatory expectations. Institutions that fail to automate and accelerate their GRC programs face more than just fines and sanctions; they risk competitive irrelevance.

The following challenges represent the most pressing issues facing GRC professionals in banking and financial services. Organizations that develop effective strategies to address these compliance challenges will be positioned not just for checkbox success but for genuine competitive advantage.

1. The AI balancing act

Banks and financial institutions are walking a precarious tightrope between innovation and compliance. Increasing regulatory complexity has created an unsustainable workload: there just isn't enough time for compliance teams to handle both regulatory responses and their core responsibilities. In this environment, AI implementation is a must-have.

But AI adoption is complex for GRC teams. Financial institutions must determine what security guardrails to put in place, how often to validate and update models to remain compliant, and how to implement continuous monitoring systems that keep pace with evolving AI capabilities. It's all too easy to become stuck between the need for efficiency and the fear of compliance missteps, data security issues, and even output validity.

The banks that fail to resolve this balancing act quickly will find themselves overwhelmed by manual compliance processes while more agile competitors pull ahead.

2. The looming possibility of deregulation

Financial services are at a potential regulatory inflection point with the looming possibility of federal deregulation. Instead of enabling efficiency, this deregulation is likely to trigger a cascade of state-level regulations, each with its own unique requirements and enforcement mechanisms. With existing state-level regulations (including StateRAMP, NYDFS Part 500, CCPA, and more) already in place, the addition of new frameworks threatens to overwhelm even the most efficient organization.

Financial institutions operating across multiple jurisdictions will potentially face the daunting task of trying to satisfy several dozen different regulatory regimes: a compliance nightmare that could dramatically increase costs and operational complexity.

In this scenario, standards organizations like the Cyber Risk Institute (CRI) will take on greater importance. These organizations may become de facto standards bodies, with their frameworks serving as the only common ground in an otherwise chaotic regulatory environment. The time to prepare is now, before the full impact of deregulation becomes apparent.

3. Threat intelligence

With increasing geopolitical uncertainty comes new threats for financial institutions. State-sponsored attackers are increasingly targeting financial infrastructure in sophisticated attacks. Backed by nearly unlimited resources and advanced technical abilities, these threats continue to grow in both frequency and severity.

Unfortunately, financial institutions continue to confront these existential threats in isolation. Despite years of discussion about industry collaboration, meaningful sharing of threat intelligence remains limited by competitive concerns, legal constraints, and technical incompatibilities.

The uncertainty around ongoing funding for MITRE's Common Vulnerabilities and Exposures program, a threat intelligence database, is also contributing to the situation. Although funding was temporarily reinstated at the last minute, it's unclear whether the database will continue to be supported long-term.

The unpredictable, fragmented state of threat intel creates systemic vulnerabilities that attackers are all too happy to exploit. Without a major improvement in industry-wide threat intelligence sharing, the financial sector will remain unnecessarily exposed to threats that no single institution can effectively counter alone.

4. Risk visibility

Banks and financial institutions find themselves overwhelmed by the sheer volume of risk data they generate, yet paradoxically remain risk-blind at the executive level. Financial providers urgently need ways to aggregate their complex risk and compliance data without getting bogged down in technical details: a.k.a. a strategic, top-down view of their risk and control environments to support informed decision-making.

This visibility gap is a pressing challenge. Without comprehensive risk visibility, financial institutions make critical business decisions based on incomplete information, and they miss vulnerabilities that lie hidden in siloed data systems. The traditional approach of manually aggregating risk data simply doesn't work anymore given the complexity of modern financial operations and the expanding threat landscape.

RegScale's Continuous Controls Monitoring (CCM) platform offers a solution with cyber hygiene reporting and customizable dashboards. These tools allow organizations to visualize their compliance posture across different frameworks like NIST CSF or CRI Profile 2.1 and quickly identify compliance gaps and control weaknesses. From there, they can drill down to specific control requirements that need attention.

5. Regulatory exam management

The regulatory exam burden has reached crisis levels, consuming unprecedented resources and threatening to overwhelm compliance teams. What was once a periodic necessity has morphed into a near-continuous state of examination prep, response, and remediation. We have it on good authority that at least one major American bank has dedicated a chunk of their information security team solely to managing regulatory exams, a sign of how unsustainable the situation has become.

The traditional manual methods of preparing for and responding to regulatory exams — including document collection, evidence gathering, interview preparation, findings management, and remediation tracking — simply can't scale to meet today's exam volume and complexity. Financial institutions can no longer afford to handle these processes through spreadsheets and email chains.

Automation offers a promising path forward. Institutions that fail to leverage these technologies to streamline their regulatory exam management will find themselves perpetually behind, diverting critical resources from other essential functions while still struggling to meet compliance requirements.

AI and automation: the future of GRC

It's not just regulatory exam management that needs automating; it's every part of the compliance lifecycle. One solution is Compliance-as-Code: embedding regulatory requirements directly into CI/CD pipelines using OSCAL (NIST Open Security Controls Assessment Language) and automation. By integrating automatic compliance checks into their DevSecOps, organizations can shift from manual, point-in-time compliance to a real-time, proactive approach.

Implementing automation successfully requires a strategic, phased approach. For financial organizations looking to transform their compliance programs with automation, we recommend the following steps:

- ✓ Identify which controls are technically feasible to automate. Then, prioritize the ones that will save your team the most time. You'll never automate 100% of everything, so aim for the controls that consume the most manual effort.
- ✓ Set realistic expectations. Even high-performing organizations may only automate 10 or 15% of controls in their initial year. Focus on steady, meaningful efficiency gains while allowing time to refine your processes.
- ✓ Directly integrate automation into your CI/CD pipeline. The goal is to ensure compliance assessments occur automatically with each build rather than as an afterthought.
- ✓ Connect to the RegScale platform. Align the assessment outputs with the corresponding controls so that compliance issues can be continuously identified and addressed.
- ✓ Implement ongoing monitoring. Gain real-time visibility into the control environment, and immediately be alerted to failures and drift instead of discovering problems during high-stakes regulatory examinations.

To learn more, explore our resources on rewriting the regulatory exam playbook, the RegScale-CRI collaboration, and CCM for the finance industry.