ViClarity®

Report: Governance, Risk & Compliance Trends to Watch in 2024

Explore the Challenges & Opportunities Facing Financial Institutions This Year

Introduction

ViClarity's annual governance, risk and compliance (GRC) trends report is designed to help financial organizations and their risk and compliance leaders focus on the key trends impacting the industry as we progress into 2024. Our team of GRC technology experts reviewed the market and spoke with some key stakeholders to uncover topics that are front and center.

In this report we explore four of these topics, starting with an increased focus on third-party risks, consumer financial protection and cybersecurity. We also discuss the use of artificial intelligence (AI) in GRC and the quest to have one central location for all risk, compliance and reporting data.

We hope you find this to be a helpful guide to the year ahead. If you have perspectives to share or questions to ask about the topics presented here, please reach out!

- Miriam De Dios Woodward ViClarity Global CEO

What's Next:

1. *Regulator Focus on Third-Party Risks & Consumer Financial Protection*
2. *Testing Plans for Continuously Changing Cybersecurity Threats*
3. *The Use of AI in GRC*
4. *The Pursuit of a Single Source of Truth*

1 Regulator Focus on Third-Party Risks & Consumer Financial Protection

> ***"In the eyes of an examiner, a vendor's mistake is the financial institution's mistake, and it can be a costly one."***

Regulators are strengthening rules and focusing on operational resilience across sectors — particularly in the financial industry. Third parties, especially fintechs, are generating a lot of interest. The National Credit Union Administration (NCUA), for example, still has not obtained vendor oversight, but they are diving into credit unions' vendor due diligence processes.

The work of staff members leading third-party vendor management has never been more important to their organizations. As we move through 2024, we expect to see increased scrutiny on vendor connections to financial institution systems, as well as vendor compliance competency.

In the eyes of an examiner, a vendor's mistake is the financial institution's mistake, and it can be a costly one. Integrating technology automation to help manage third-party vendors can serve as a back-up to teams, ensuring process consistency, enabling them to spot outliers and alerting them to any missed deadlines and upcoming assignments — benefits that help to keep risks under control.

Among the most significant threats third-party vendors pose to financial institutions is non-compliance with consumer protection regulations.

People tend to think of vendor due diligence as a front-end process, something an organization does before deciding to acquire services or onboard a new vendor. In actuality, vendor due diligence is an ongoing initiative that goes beyond annual check-ins on the "usual suspects" of personally identifiable information (PII) compliance and cybersecurity protections. Frequent spot-checking or sampling of vendor processes is a due diligence best practice and something we expect regulators to pay close attention to in 2024.

ViClarity®

2 Testing Plans for Continuously Changing Cybersecurity Threats

Financial institutions handle sensitive consumer data every single day. Those consumers trust their banks, credit unions and other organizations to protect their data and take proper precautions to safeguard it. This is one of the most important duties of a financial institution and the subject of intense regulation.

Cyber incidents not only put consumers' sensitive information at risk, but also place strain on a financial institution's technology resources and may be compounded by financial losses, damaged reputations and legal repercussions. Although most organizations already have cybersecurity plans and incident response programs in place, in 2024 we expect to see a growing focus on testing those plans and programs to ensure they keep up with the continuously changing landscape of cybersecurity threats.

Organizations may look to outside consultants to assist with cybersecurity incident response policy development or review of existing plans to ensure compliance with regulatory requirements. Regardless of whether they seek outside assistance or tackle it internally, financial institutions should be constantly monitoring the evolution of cyber threats and updates from their regulatory bodies.

3 The Use of AI in GRC

Using natural language processing models, generative AI has the capacity to produce text, images and videos, making it a powerful tool for many industries, including those within the regulatory and compliance space. In recent years we have seen a significant amount of AI development within the regtech industry and believe the integration of AI can bring both opportunities and challenges to an organization.

AI can help businesses automate regulatory compliance tasks, contribute to more advanced risk assessment models, enhance data processing and simulate regulatory scenarios for training purposes.

However, there are many challenges that organizations must address before implementing AI. RegTech firms need to ensure the technology is used responsibly and ethically. They must also consider concerns related to data security and privacy when deploying AI for regulatory purposes. And finally, they need to make sure their AI tools or systems are capable of adapting to regulatory changes in order to stay compliant.

Ogie Sheehy, founder and Global CIO of ViClarity, recently commented in a Fintech Global article on how "companies are looking to see how AI can help them be more innovative, and with the use of algorithms it can help with manual tasks and predict outcomes for large volumes of data processing."

While there are areas of concern about the use of AI in certain industries, the trend we see now is that businesses are more open to exploring it than ever before.

ViClarity®

4 The Pursuit of a Single Source of Truth

As the stakes for non-compliance get higher and regulators scrutinize financial institutions more closely, organizations are seeking ways to provide a more comprehensive and centralized approach to data integrity, compliance and risk management. This includes creating “one source” of data — a single, authoritative source of truth that can be relied upon for risk analysis, proof of adherence to policies, reporting, analysis and compliance.

Currently, organizations have data silos where collections of information are not easily accessible because they are recorded or stored differently. This makes it difficult to get a complete picture of their data and to comply with regulations.

Historically, resolving this issue would have required a significant investment in time and resources. Now, modern solutions simplify the process by offering a more efficient path. Ultimately, having a single source of data will help financial institutions reduce costs, improve compliance and make better decisions. Those who continue to turn a blind eye to the issue will face financial penalties, operational risks and reputational damage.

To learn more about how ViClarity helps organizations streamline governance, risk and compliance processes:

+ Visit: *www.viclarity.com/us*
+ Email: *info@viclarityus.com*

ViClarity®