Current state and ongoing evolution of financial institutions' GRC regimes

Sawako Haji

17 February 2023

Iakyara vol.367

Nomura Research Institute, Ltd.

Executive Summary

With the amended Act on Promoting the Protection of Personal Information fully in effect and a new economic national security law enacted last year, Japan now has an updated suite of GRC-related legislation in place. A recent NRI survey sheds light on how global financial institutions are approaching GRC in terms of developing tools, building organizations and reassessing key risks.

Sawako Haji
Expert
Digital Governance Platform Department

In 2022, the amended Act on Promoting the Protection of Personal Information fully took effect and the Diet passed an economic national security law, giving Japan an updated suite of legislation related to governance, risk and compliance (GRC). These events prompted NRI to conduct an interview survey of 11 US and European financial institutions regarding their GRC regimes in collaboration with Cutter Associates. The survey inquired about costs, tools and organization-building in the aim of elucidating the present state of the survey respondents' GRC programs and identifying their current priorities.

Compliance costs account for 3% of total operating expenses

GRC costs tend to be difficult to precisely quantify because GRC extends throughout companies' entire operations. Our survey accordingly inquired only about compliance costs, which account for the bulk of GRC budgets.

First, one major financial institution reported that its compliance costs account for 3% of its total operating expenses, a level in line with the findings of a decennial survey of financial institutions conducted by the European Commission. According to the EC survey, nearly 30% of financial institutions' compliance costs are incurred collecting data to be reported to regulatory authorities. Thirty percent is by no means insignificant and data collection costs could increase as additional regulations are imposed.

For the past few years, financial institutions have been endeavoring to reduce GRC costs. They are upgrading their compliance with increasingly complex

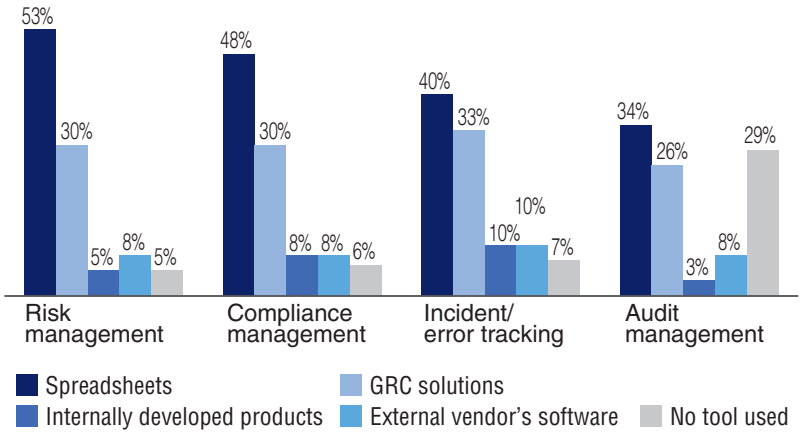
regulations through such means as integrating risk management and compliance processes and automating error detection and other internal controls. Our survey found that financial institutions expect to incur higher costs over the next several years as they adopt new technologies that will enable more sophisticated analyses and further automation of GRC processes.

GRC tool utilization

Next, our survey inquired about use of GRC tools, including ones for monitoring and analysis. A 2019 survey by Cutter Associates found that while many financial institutions use GRC tools, they use a mix of internally developed products and external vendors' software, not a single-product solution. This previous survey also revealed that spreadsheets with manually inputted data were widely used across GRC processes (see graph). Such mix-and-match software environments and manual processing not only impede risk categorization and detection of related risks, they also make it harder to ascertain the impact of changes in regulations and business processes.

In response to these shortcomings, many of the financial institutions we surveyed reported they are reassessing the GRC tools and services they are currently using. Their reassessments may lead to development of new tools. When asked about plans to use GRC tools going forward, respondents indicated that GRC data strategy, data collection and data architecting are key priorities. Senior management expressed keen interest in utilizing GRC tools and services, though our survey did not delve into the specifics of the respondents' monitoring and data analysis methods.

GRC tool utilization



Source: Cutter Research Survey on GRC practices, 2019

GRC organization-building

Depending on company size, GRC organizations differ substantially in terms of staffing (headcount, on-site vs. remote, etc.) and the extent to which they use external resources. All of the financial institutions we surveyed subscribe to the 3LD (three lines of defense) model. The three lines of defense are (1) line executives, (2) administrative staff, specifically risk management and compliance staff, and (3) internal audit staff.

Recently, however, some companies have been separating the second line of defense's risk management and compliance functions. A major financial institution we surveyed mentioned that separating the compliance function from the risk management is a key component of rebuilding its governance framework. This financial institution's CCO (chief compliance officer) is an independent officer who reports directly to the Group CEO. The CCO and CRO (chief risk officer) share responsibility for risk monitoring. They each lead separate teams within the financial institution's risk framework.

Another notable development is that financial institutions are building GRC organizations whose mandates include climate change risk and/or compliance with ESG-related laws and regulations. Nearly all of the financial institutions we surveyed are working on frameworks that assess ESG risks. They have mostly decided either to add ESG risk to their existing ERM committees' authority or to newly establish an internal team dedicated solely to ESG risk.

Our survey respondents included small/mid-sized financial institutions that do not have an organizational unit that adequately addresses GRC. Some of them are looking into outsourcing the internal audit or CCO role to an external consultancy. In the US, there are GRC-specialist consulting firms staffed entirely by former CCOs.

In addition to the topics discussed to this point, dealing with conduct risk has recently emerged as a new focal point. As remote work has grown in prevalence, companies are concerned about conduct risk manifesting in the form of, e.g., infringement of privacy or employee misconduct. A large majority of the financial institutions in our survey sample have likewise become more cognizant of conduct risk in addition to existing GRC priorities like cyber/information security risk, third-party supplier risk and AML.

One major financial institution we surveyed reported that its 2022 GRC priorities were managing increased conduct risk stemming from hybrid working arrangements and addressing new risks and issues related to supervising and monitoring remote employees. It was planning to continue to work on mitigating risks around remote employees in particular and figuring out how to fit such risks into its organization-wide risk framework. Risks around remote employees warrant recognition as key risks in addition to the aforementioned ESG risks.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.0 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Digital Business Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/