CXO Roundtable - Key Takeaways

GRC Summit, Baltimore 2019

Chaired By:

Jim Quigley
CEO Emeritus of Deloitte, Wells Fargo Audit Committee Board Chair

William Onuwa
Chief Audit Executive, Royal Bank of Canada

Jim Boehm
Expert Associate Partner, McKinsey

Hosted by

MetricStream
PERFORM WITH INTEGRITY™

Overview

A combination of thirty chief risk officers (CROs), chief audit executives (CAEs), chief compliance officers (CCOs), and chief information security officers (CISOs) took time out from the MetricStream GRC Summit 2019 in Baltimore to participate in our inaugural CXO roundtable. We discussed three topics: integrated risk management, the future of internal audit, and cyber risk management. Participants shared their insights on the challenges encountered, successes faced, and best practices learned. Some of the areas that were covered included:

- How integrated risk management programs are evolving with new technologies like AI
- How to get the first line more involved in risk management
- How digitization is transforming internal audit teams, tools, and processes
- How to define critical assets, and prioritize cyber risk investments
- Why relevance-oriented decisions in cyber risk management are replacing probability-based decisions

The following pages of this report provide a brief summary of the three main topics, along with key takeaways.

1 Integrated Risk Management

Jim Quigley, CEO Emeritus of Deloitte & Wells Fargo Audit Committee Board Chair, led off the discussion around attendees' integrated risk management (IRM) programs. Continuing from his keynote on the "known unknowns," he began a discussion by polling the group on the challenges they faced in implementing IRM programs.

One member of the CXO group, referencing the keynote by MetricStream CEO, Mikael Hagstroem, stated that AI will be as transformative as electricity was a century ago. The discussion then spread to how IRM or GRC programs were striving to keep up, and how it was necessary to train, teach, and embed the practice of leveraging AI in risk management across firms.

To further amplify the point, and to highlight the scale of the change we are facing, one CXO noted that the way specific risk management activities have been performed over the past 25 years is now almost redundant. He said that while it was culturally challenging to accept this, he was proud that his firm now needed to re-tool and take a different approach to risk management while responsibly leading employees through the change.

One CAE noted that the current way of doing things had to change. The typical approach of crafting a narrative around the audited process was described as cumbersome and inefficient. It left auditors unable to quickly identify where the process had changed period by period. She was clear that structured data, rather than unstructured text, would be the path to efficiency by leveraging technology more easily and affordably.

As the conversation pivoted to data collection and the three lines of defense model, a question was posed to the audience by the moderator: "how many of your firms see more than 50% of your issues or risks identified by the first line of defense"? Approximately 20% of attendees raised their hands. Quickly, those in the room discussed the desire to improve in this area and remove associated cultural and technological impediments. MetricStream CTO, Andreas Diggelmann, talked in his technology keynote about addressing just this issue with a co-innovation solution to a customer's specific problem. There was great debate in the room, and another quick poll suggested that very few firms had leveraged gamification, compensation, or other popular change management techniques.

Overall there was huge pride in how far people had progressed on their risk management programs from just a few years ago. They also acknowledged that there was still a long way to go. This was a journey and not a destination, they reaffirmed.

2 The Future of Internal Audit

William Onuwa, Chief Audit Executive of the Royal Bank of Canada led off the discussion around attendees' internal audit programs. He began by polling the group on internal audit resource models. Approximately 50% of attendees stated that their resources were wholly constituted from internal resources, while the remaining 50% indicated that they had some hybrid model bringing in third-party resources for specialized purposes.

The question was designed to unearth how the audience was dealing with the rapidly changing landscape surrounding the advent of new technology including AI. In fact, one CAE stated that there used to be three sources of truth (one for each line of defense), and now with GRC technology ever present, there is one source of truth – the machine. While there may be multiple interpretations of the data inside GRC, the data itself is constant. The target state: spend more time on analysis and debate rather than aggregation.

As the conversation pivoted to testing concepts, one CRO stated that it was his vision to leverage technology to test 100% instead of sampling. While some others' thinking had not evolved to this extent, the point was appreciated, and it was accepted that only through large-scale standardization and digitization of data can 100% testing be accomplished.

Switching back to resources, how is the internal audit function of today staffing up for the future? Aware that not all processes are going to be immediately impacted by technology or AI, the attendees agreed that a mix of people with accounting and engineering skillsets would be needed in their teams. Robust training programs, peer knowledge sharing events, and conferences aimed at the first line should be attended by oversight functions. It was also made clear that where we can, we should automate. Where there are "known knowns," we should employ machines to do the heavy lifting – anomalies are then the focus of the auditors. This will drive efficiency and efficacy up.

Overall the position in the room was that the internal audit vision was clear, and some had already begun making changes to adjust. There was also acknowledgement that change management was a critical skill to have in one's arsenal to ensure that technology and AI were not met with fear but welcomed.

3 Cyber Risk Management

Jim Boehm, Expert Associate Partner, McKinsey, led off the discussion talking primarily about cyber risk and the importance of taking a holistic approach to cyber risk management. He noted that technical cyber defense can be sound, but human error or a lack of robust controls can undo it all and lead to a significant system breach, resulting in data or financial loss. The key to holistic cyber risk management is understanding and prioritizing a cyber program according to both dimensions – the many potential things that can lead to a loss, and the actual business assets (information, processes, applications, teams, etc.) that can yield that loss.

An informal poll in the room let us understand that all respondents were still building cyber defense, cyber resilience, and cyber awareness programs. Different firms were at different stages on the journey, but one clear standout issue was a lack of clarity and agreement within firms on which assets to protect most vigorously, and in which order to go about building that protection. Only 15-20% of those in attendance stated they were using process criticality as an input for resource allocation.

A lack of process or capability framework agreed upon and approved at the management or board level has led to differing opinions of where the most critical controls should be employed, the respondents stated. Categories such as financial, regulatory, reputation, operational, and productivity impacts were identified as possible ways to think about defining critical assets.

Whether to, and in which order to deploy controls such as multi-factor authentication or dual authorization of transactions, was discussed. More mature firms indicated that they were tying these types of controls directly to risk appetite to ensure that awareness of critical processes or assets was understood across the firm, and so the board knew the firm was actively addressing key risks tied to corporate strategy.

The discussion quickly pivoted to achieving this objective. The concept of moving away from probability-based decisions to relevance-oriented discussions was of great interest. In this context, relevance refers to a set of factors used together to understand which threats were relevant for which vulnerabilities, and how that combination of factors affected the potential impact of business assets.

Risk Out come = Potential Impact (of risk events to valuable asset(s)) * Threat (which is a function of Attacker Motivation * Attacker Sophistication) * Vulnerability

If the attacker's motive and/ or sophistication is low (perhaps because the value of the target is low), then the vulnerabilities associated with the potential risk outcomes related to that threat would also become less relevant. If you cross-reference this low relevance with the criticality of your internal assets or processes (once agreed upon), you could be efficient with your resource deployment. Why spend millions of dollars on something that is not relevant?

The concept of relevance was also debated when those in the room discussed scenario analysis. The prevailing notion was that simply because an attacker can penetrate doesn't necessarily mean they will. This should be taken into account when creating plausible scenarios.

In addition, methods such as overlaying the 'most phished' people, processes, or assets onto your critical list will give you some data to feed into the above equation. The more targeted the phishing, the more the 'relevance'. As such, one should prioritize controls to close vulnerabilities, such as applying an application patch.

Overall, there was consensus in the room that the journey was just beginning, and the horizon of the risk-based approach was the desired end-goal. Only through constant investment, structural agreement across business units, as well as continual training to raise awareness and technical ability will one be able to achieve this objective and keep pace with cyber risk management needs.

Key Takeaways

- Change management should be an integral part of any GRC program
- Getting the first line of defense more involved in risk identification will require creative solutions
- Automation will be key to the success of internal audit in the future
- Human error can weaken even the most robust cyber defenses
- Understanding the relevance of an asset or process can lead to more optimal allocation of cyber risk resources

To catch excerpts from the roundtable plenary recap, watch the panel in action at the GRC Summit.

To learn about MetricStream's perspective on GRC trends and predictions, read: GRC 2019: THE KNOWN UNKNOWNS

Contact us
Email: info@metricstream.com