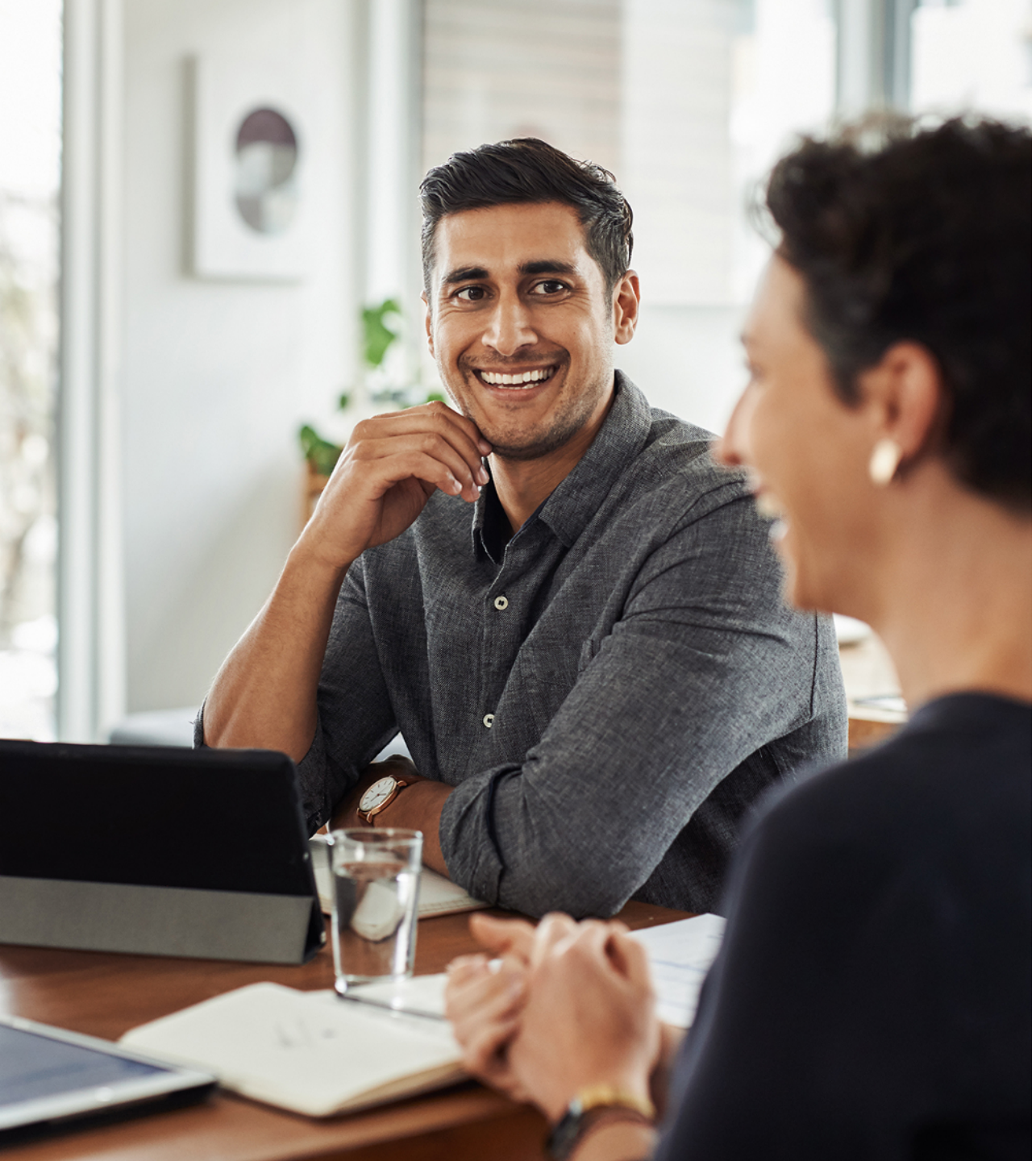
CISO Cross-Industry

Expert Exchange

Q3 Executive summary
July 15, 2025

kyndryl



Overview

The discussion centered on common challenges and innovative approaches within Governance, Risk, and Compliance (GRC), emphasizing its rapidly evolving nature due to changing regulatory scrutiny, technological advancements, and sophisticated cyber threats. Key themes included effectively translating GRC data into strategic actions, integrating cyber risk into broader corporate strategies, leveraging AI and automation, and enhancing risk visibility and communication.

Host

Justin Haney
Kyndryl, USA Vice President – Security and Network Leader

SME

Anthonie (Tony) DeBos
Global Leader for Data Protection, Privacy and (Responsible) AI

Key topics

PAGE

Translating GRC Data into Actionable Strategy

- Organizations commonly struggle to convert extensive risk data into clear strategic priorities and repeatable planning cycles, often resulting in resource allocation that does not directly address documented risks.

- One executive highlighted that while their large GRC program successfully identifies risks, the main challenge lies in converting risk register data into actionable information for strategy setting, seeking a repeatable process that meaningfully builds year over year. Another participant expressed a similar difficulty, noting that despite identifying and documenting risks, cyber consistently remained a top risk on the register. This led them to ask what specific actions the business is looking for to move cyber out of that top slot.

- Implementing cyber risk within broader corporate risk frameworks is crucial for elevating its strategic importance and fostering shared responsibility beyond the security team. One executive shared that for their organization, cyber risk has consistently been among the top five corporate risks reported to the board for the past decade, mainly because their cyber program was integrated into a long-standing overall risk management framework that historically focused on safety and compliance.

- While strategy is often not driven by cyber posture, with cyber frequently "tailing" other business priorities, success has been found by forming a cross-functional "privacy, data, and risk management committee" to collaboratively identify and address top risks. A multi-year budgeting cycle has also been instrumental in elevating cyber risk, as complex remediation efforts often span beyond a single budget period, reinforcing sustained strategic attention.

> "Where we have had the most challenge is translating data that goes into a risk register into actionable, insightful information consistently used in setting our strategy."
>
> — CISO Expert Exchange Member

Unifying GRC with AI-powered insight and control

Learn more

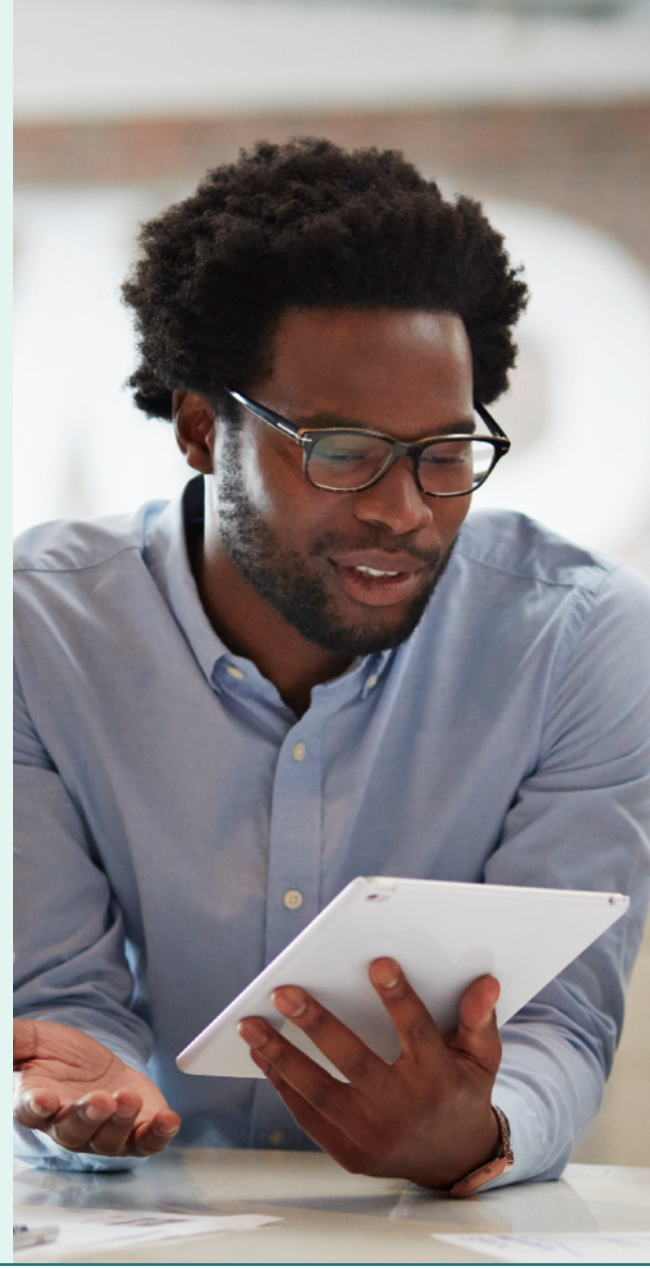
Leveraging AI and Automation in GRC

- Organizations are actively exploring artificial intelligence and automation to enhance efficiency, scale, and proactive management within Governance, Risk, and Compliance functions. Several participants are investigating agentic AI for compliance, with potential use cases including automating routine tasks like recertification processes. One executive shared success using an internal AI tool to draft initial responses to regulatory inquiries by synthesizing information from policies, standards, and past responses, saving significant labor.

- Another CISO described their journey in re-architecting GRC functions with agentic AI, aiming to dramatically increase the scale of risk assessments and control testing from annual reviews to multiple times a year across all cloud environments. Someone highlighted agentic AI's potential for proactive risk management, where the system detects issues, initiates actions, such as checking third-party data transfers for compliance or determines necessary controls.

"We are looking at automation as much as possible within our compliance area, including agentic AI... current agentic AI capabilities still face a 'last mile' challenge, requiring substantial prompt engineering and data grounding to achieve perfect, fully automated outputs."

— CISO Expert Exchange Member



Improving Visibility and Communication of Risks

- Enhancing the visibility and understanding of risks across all organizational levels significantly boosts engagement and resource allocation for risk mitigation efforts. One executive highlighted a challenge where risk information was overly segmented, limiting visibility even for top directors, which hindered effective resource allocation for addressing high-priority risks. To simplify the process economically, a dedicated risk management team successfully implemented a manual procedure to create a monthly "risk scorecard" for individual leaders. This was then shared quarterly with the CIO and audit committee.

- This increased transparency unexpectedly fostered a greater willingness among non-security personnel to acknowledge and address risks, as they observed issues being actioned and prioritized, creating a positive feedback loop. However, a participant cautioned against widely sharing physical risk registers due to the theoretical risk of compromise or public disclosure, advocating for sharing information via screen share to maintain control over the document.

- Managing GRC in regulated industries involves navigating a complex landscape of diverse external requirements and understanding how various auditors interpret risk information. One participant articulated operating under the scrutiny of over 20 governments, 6 US agencies, 44 states, and numerous customer requirements, necessitating roughly 18 independent audits annually. The conversation emphasized tailoring reports to the specific audience, acknowledging the "human touch" required when compiling and sharing information with regulators, despite efforts to automate control testing across multiple global frameworks.

> "We're making it very visible to everybody in the organization. So, when it comes down to resource planning and making sure that we have US dollars and cents allocated, the business is much more motivated now to help us work the plan."
>
> — CISO Expert Exchange Member

kyndryl

The CISO Expert Exchange is hosted by Kyndryl. Please contact Justin Haney with any questions about Kyndryl or this Exchange.

© Copyright Kyndryl, Inc. 2025

Kyndryl is a trademark or registered trademark of Kyndryl Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.