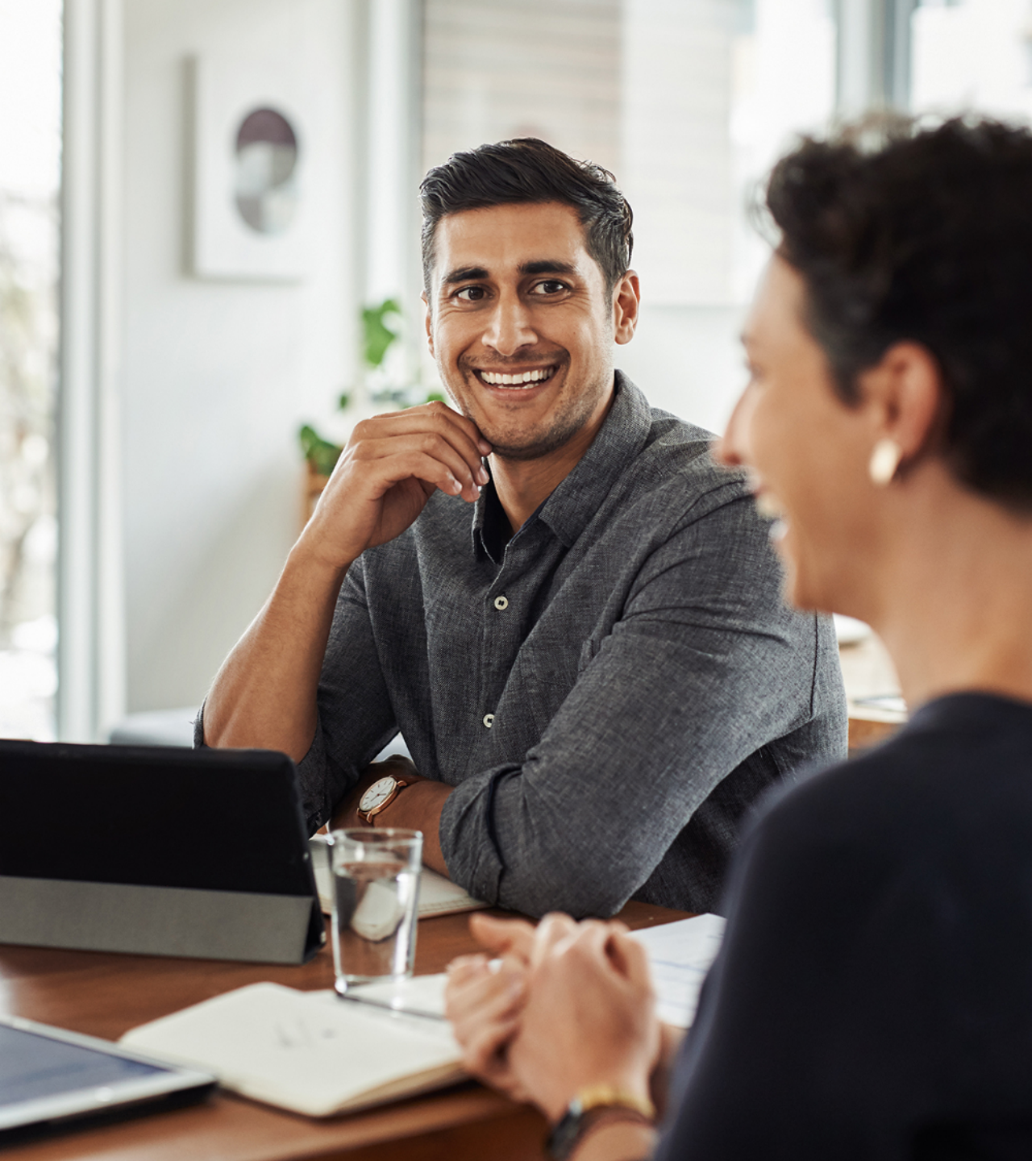
Executive Summary

Security and Resiliency Expert Exchange

February 27, 2025

kyndryl



Overview

In the Kyndryl Security & Resiliency Expert Exchange held on February 27, 2025, security executives from multiple industries and countries convened to discuss regulation, risk, and vendor compliance management.

Key discussion areas included the importance of top-down approaches to compliance, the challenges of operational risk management, and the complexities of third and fourth-party risk management.

Host

Conal Hickey
Kyndryl, Vice President – Security and Resiliency

Key topics

Security executives are shoring up resilience measures to meet regulations

- Security leaders are bolstering their resilience efforts in the face of increasing regulations, including DORA, NIS2 and others.

- For global companies, these efforts are essential as there are more than 160 countries with more than 100 different regulatory requirements. To keep pace, companies need to be working at three different levels: The European Union level, the country level, and the industry level. Several of the members pointed out that, although they may be headquartered in, or operate in, countries that are not in the EU (e.g., Switzerland or Poland), they must still maintain compliance for the rest of Europe, even if they aren't technically part of the EU.

- Many CISOs are under pressure to ensure their companies are compliant, especially as the risk of not complying may become prohibitively costly. Furthermore, for many board members compliance is personal because they can be held personally responsible for a security breach, and its financial repercussions.

- Regardless of whether their company is directly subject to DORA regulations, executives are proactively taking steps to ensure the necessary compliance is in place, that helps them to enhance their business' operational resilience. Some companies in highly regulated industries already have security measures in place to meet other requirements, while others are recognizing the security risks of not taking proactive steps, even if DORA compliance is not mandatory.

"At the end of the day, it's binary, right? You are compliant or not. And if you're not compliant, somebody's going to come after your pocket, so we'd better be compliant"

— Kyndryl Security & Resilience Expert Exchange Member

Can One Managed Security Service Provider Handle All Security Operations?

Learn more

Maturity journeys vary by industry and company

- The attending executives from various industries are at different stages of their compliance maturity journeys. Those in highly regulated industries, such as banking and finance, tend to be more advanced in their digital maturity due to their prolonged engagement with digital regulations. Several executives highlighted that their industries are not only addressing DORA but are also responding to various other regulations, leading to a more mature approach to compliance.

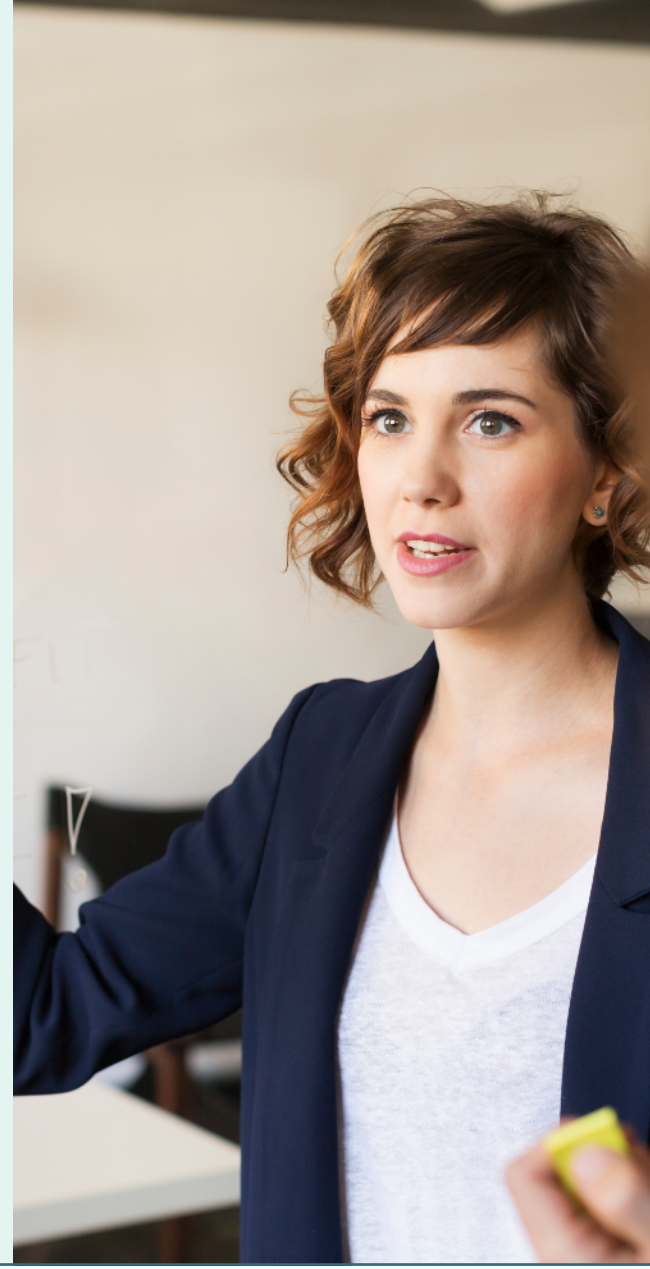
- In response to a question about initiating their compliance journey, a couple of executives recommended engaging one of the consulting firms to conduct a gap analysis. Leaders emphasized the importance of approaching compliance and resilience from the "top-down" rather than the "bottom-up." This strategic approach involves identifying the most mission-critical, "minimum viability" business operations first and expanding outward, rather than starting from the point of a breach and playing "catch up"

- A new discipline is emerging in security and resilience, focusing on operational risk management. Executives expressed that many employees in regulatory organizations of certain countries are merely public servants and lack understanding of the technological aspects of operational risk, resilience, and security. This deficiency in background and security skills leads to confusion and ineffective engagement within the country.

"I think one of the main challenges is you need to be able to showcase and evidence from the top down that everything you have done and designed is based on your business needs. And if you are trying to exclude some of the dollar requirements using the proportionality principle, you will fail dramatically. If you take the pragmatic approach of bottom up, you will fail because you cannot afford to be DORA compliant."

— Security and Resilience Expert Exchange Member

Learn more



Navigating Complexity and Challenges in Third and Fourth Party Risk Management

- A major hurdle for companies striving for DORA compliance is that their operations often rely on third-party vendors, whose security measures they cannot control or enforce. As a result, a company may be compliant, but a vendor or partner might not be.

- The size of the vendor can impact compliance but doesn't guarantee security. Most companies are using one of the major tech companies as vendors (e.g., Microsoft, Google, Salesforce, etc.) In the example of the CrowdStrike breach, many companies that use those third-party vendors were affected, even those that are already highly regulated, such as the airlines.

- An executive pointed out that once fourth-party vendors are involved, tracking and reinforcing resilience becomes nearly impossible, as many of these vendors may not even be aware of how their work is used or which companies are using it. This highlights the importance of approaching compliance and resilience from a "top-down" rather than a "bottom-up" perspective. This strategic approach focuses on identifying the most mission-critical, "minimum viability" business operations first and expanding outward, rather than starting from the point of a breach and playing "catch-up."

- The conversation highlighted the necessity for clear communication and contractual obligations with third-party providers to mitigate risks. It was noted that smaller vendors might struggle to meet these standards, creating a balance between maintaining high security and not overburdening smaller suppliers.

"It's one of the more challenging areas. It's important to know how your critical third-party providers are running their operations, right? And if you think about the application development, and application co-development that's done—how are they managing that security when they're doing that co-development? There are a lot of smaller players, and they can't necessarily afford the same level of security or controls in how they operate

— Security and Resilience Expert Exchange Member

Learn more

kyndryl

The Security and Resilience Expert Exchange is hosted by Kyndryl. Please contact Conal Hickey with any questions about Kyndryl or this Expert Exchange.