2024

RISK IN FOCUS

Cyber Risks Round Table

The 2024 Edition of Risk in Focus highlights again **cybersecurity** as the top #1 Risk for auditors and internal controllers.
To discuss this, Risk in Focus gathered **a panel of European auditors** and risk controllers in October 2023 to delve deeper in the nature and evolution of this critical challenge.

WHAT CYBERSECURITY RISKS ARE STILL OF HIGH CONCERN?

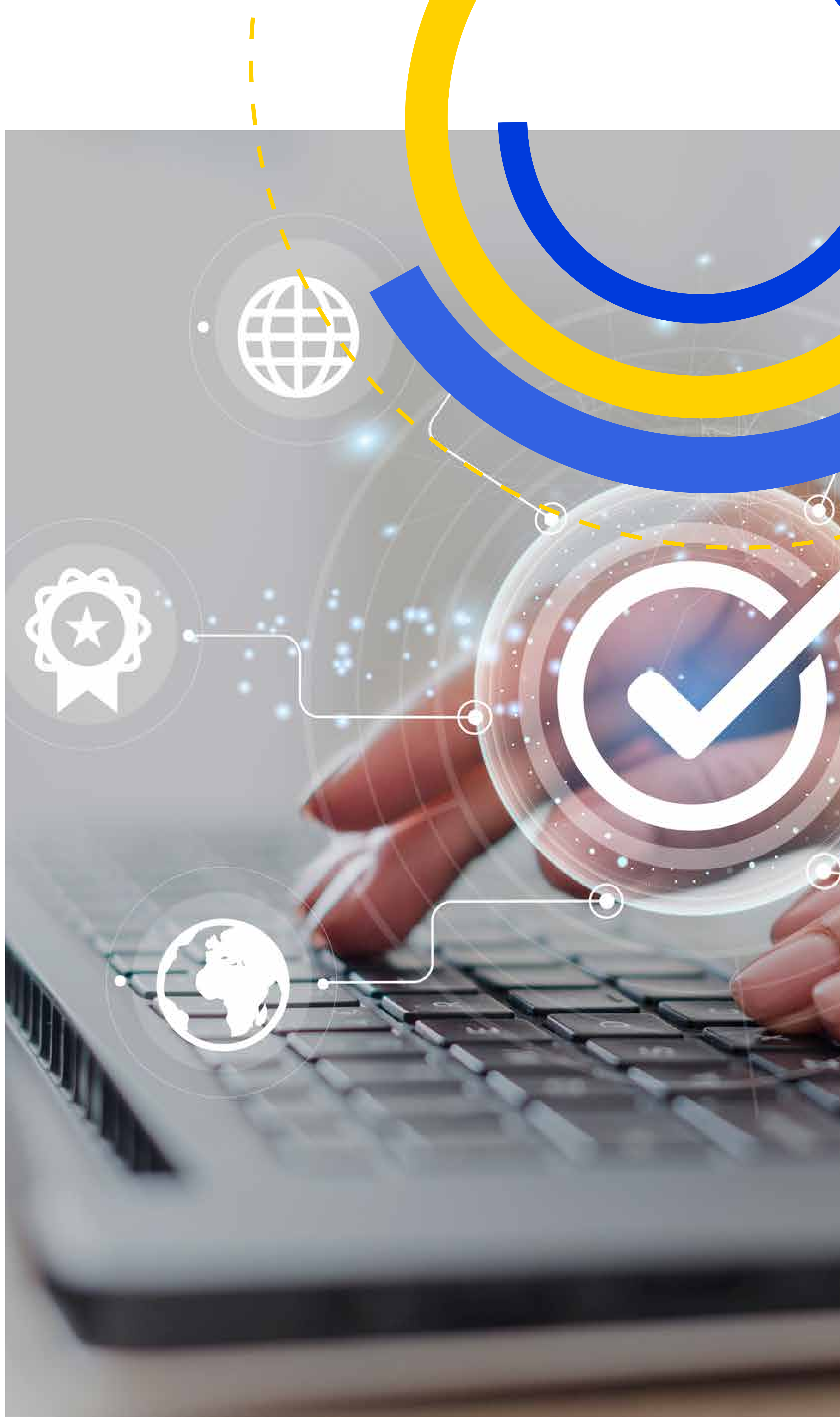
Overall, there is no one single risk but actually a common feature: the pace of adaptation of the corporate organization, with all its technological, human and organization complexity to a risk that is itself subject to change due to new technological breakthroughs such as Generative AI.

- One principal risk is **the technological debt of IT systems**. Companies with older IT systems face significant technical challenges. As mentioned by one participant, "I think the businesses that have the most challenges are the ones with the oldest IT systems and the greatest obsolescence.", not the least of which being the difficulty to find the right competences to maintain these older systems. Modernizing these systems is imperative, but it requires substantial investment in terms of money, time, and human resources.

- Another prominent risk is **human vulnerability**. Despite concerted efforts in training and awareness campaigns, there's a considerable level of susceptibility to threats like phishing attacks. "Even if you invest a lot of energy in trainings, on awareness, cetera, but it's really a pain because it's never ending." Indeed, in phishing exercises, it’s not rare to have “only” 10-15% of users clicking on the wrong link; yet this is a level of residual risk that cannot seem to be brought down. Despite all best efforts, there will always remain a “still too high” residual human risk.

- In the wake of evolving technological landscapes, **organizations** grapple with the **complexity** and governance of their IT ecosystems and their own human organizations. When internal new cyber organizations come of age, and strip away say patching responsibilities from the IT staff (the initial 1st line of defence), this can be problematic as the IT Staff may have had knowledge that may not have been passed to the cyber staff. Meanwhile, with AI, business employees now also want to use more IT tools. Yet, they lack the right awareness in terms of cybersecurity. The whole structure of the internal organization does create frictions, which yields cybersecurity risks.

- **New technology breakthroughs** are an issue. For example, Generative AI poses new problems, in part because it remains often a black box hard to audit; also because finding the right skills to run these audits is hard. Not to mention the control framework, which is still to be defined.



CURRENT INVESTMENTS IN CYBERSECURITY & CONTROLS

○ Organizations are allocating a significant portion of their budgets to cybersecurity, reflecting its growing importance. "Us, for internals this year, it would be 20% [of staff]" This percentage indicates the resource commitment towards cybersecurity within internal audit departments. A diverse approach is observed, with some entities investing nearly 50% of their budgets in collaborations with external third-party companies, demonstrating a varied strategy in cybersecurity investment across different organizations.

○ The discussion also emphasized the importance of robust business **continuity plans** and resilience against potential disasters. The organizational agility to recover and maintain operations amidst unforeseen adversities was underscored as a pivotal aspect of cybersecurity readiness.

○ The dialogue also touched on **the significance of certification** in fostering a cybersecurity culture. Certifications like ISO 27001 were seen as foundational tools that set basic cybersecurity parameters, aiding in governance and investment justification. "Certification can help the CISO justify investment in IT security."

○ Overall, **governance** plays a crucial role in shaping organizational cybersecurity. A well-structured governance framework is essential in managing technological integrations securely and effectively, ensuring that organizations can navigate the complexities of evolving cyber landscapes with resilience.

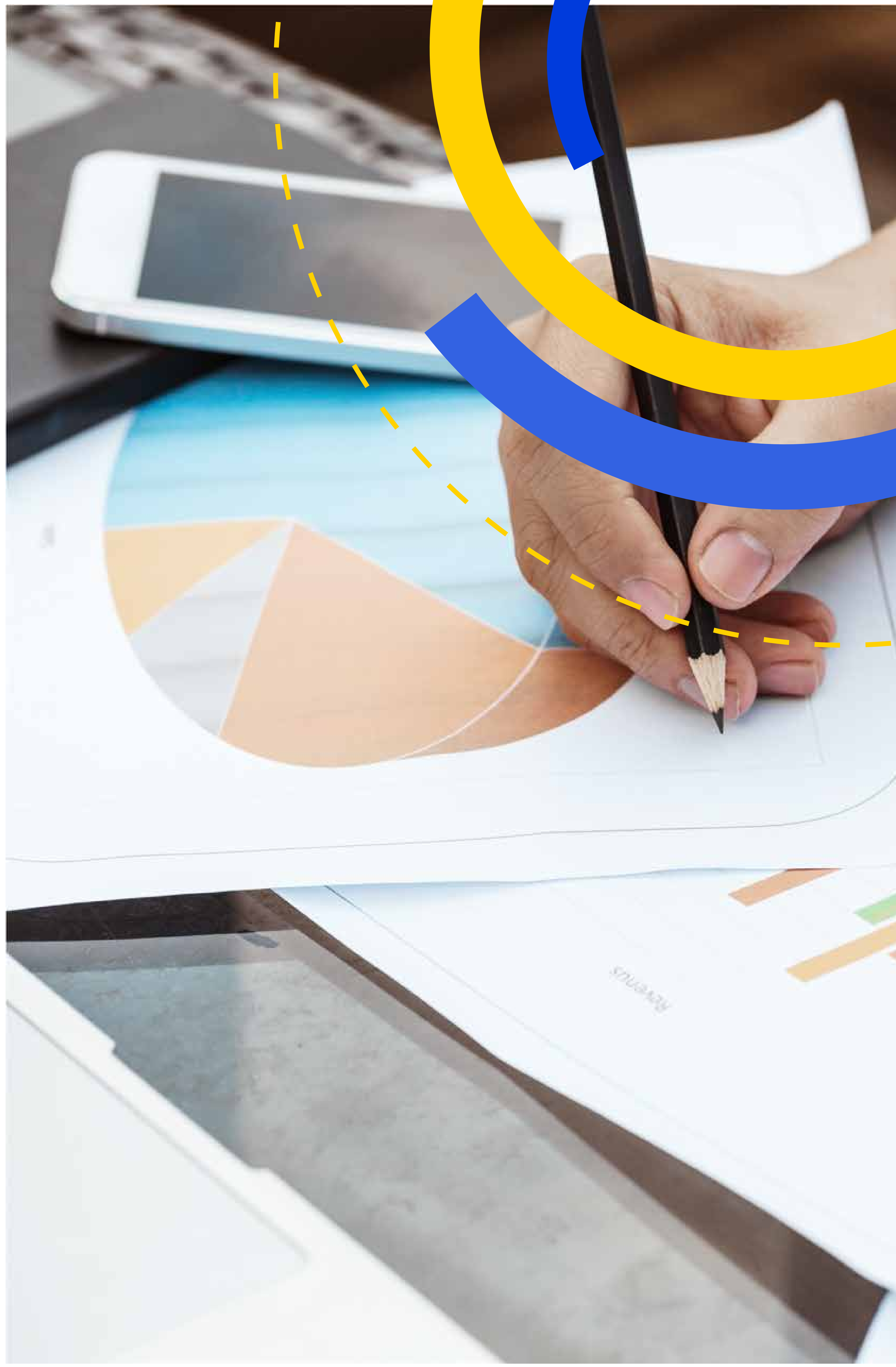
STATE OF TECHNICAL RISKS

○ **Cloud technology** presents an intricate ecosystem that brings new dimensions of cyber risks. "It's not only the cloud itself, it's the ecosystem of the cloud." This emphasizes the complexity and comprehensive nature of risks, ranging from infrastructure to software development methodologies like DevSecOps. The cloud's ecosystem requires a nuanced understanding and robust strategies to navigate the associated risks and ensure organizational cybersecurity.

○ **Artificial Intelligence (AI)** is a frontier that organizations are navigating with caution. "We said, look, the organization does not have an AI policy." This statement underscores the importance of governance and a well-established policy framework in exploiting AI's potential while mitigating associated risks. Establishing solid governance structures is crucial before engaging extensively in AI technologies.

○ In connexion to all of that, **talent in IT** is also (again) a critical problem. Indeed, the talent landscape in IT is experiencing shifts due to cloud adoption. "We are losing a lot of the IT guys!" This reflects the challenge of talent retention and the emerging dependency on external expertise and third-party services. It illustrates the pivotal role of internal talent in sustaining and enhancing cybersecurity postures within organizations.

○ **Physical security** remains a critical aspect of comprehensive cybersecurity strategies. "There are still a lot of basic failures in terms of physical security." This highlights the persistent challenges and the necessity of robust measures to ensure the physical security of organizational IT assets, complementing cybersecurity initiatives.resilience.



OTHER ISSUES

- **Geopolitical tensions**, particularly in relation to technology supremacy between nations, were recognized as influential in shaping cybersecurity strategies and approaches. Concurrently, climate change and related natural catastrophes were acknowledged for their disruptive potential on global IT value chains and operational continuity..

- On the **new regulations** (ex: NIS2, CRA, DORA in the financial industry) – as one participant stated “there is a kind of tsunami of new laws and regulation not only specific to cybersecurity, but which covers many other aspects.” To prepare for that, before law enforcement, one can set an exploratory audit, usually one or two years before, and then already put in place the assessments. To add to that, evidently, there are different regulations around the world. And while in Europe, evolutions are known well in advance – in other jurisdictions, sometimes, it is much harder to follow through.

- As per the new role of audit and internal control departments – there is a need to continue information exchange with the first and second line of defense. That can include regular meetings with CISOs, for example. There is also a need to develop a **dedicated technical team**, often augmented with external expertise; and it is not only, or not necessary about knowledge of technical controls, but also about data analytics – an element that is becoming critical. Along this, in some organizations, there is a sort of move to go back to “integrated audit”, because cybersecurity cuts across different disciplines and different expertise. This actually is starting to impact audit works even on not related cybersecurity topics, since all systems are digital and thus cybersecurity always emerges as one element of attention.