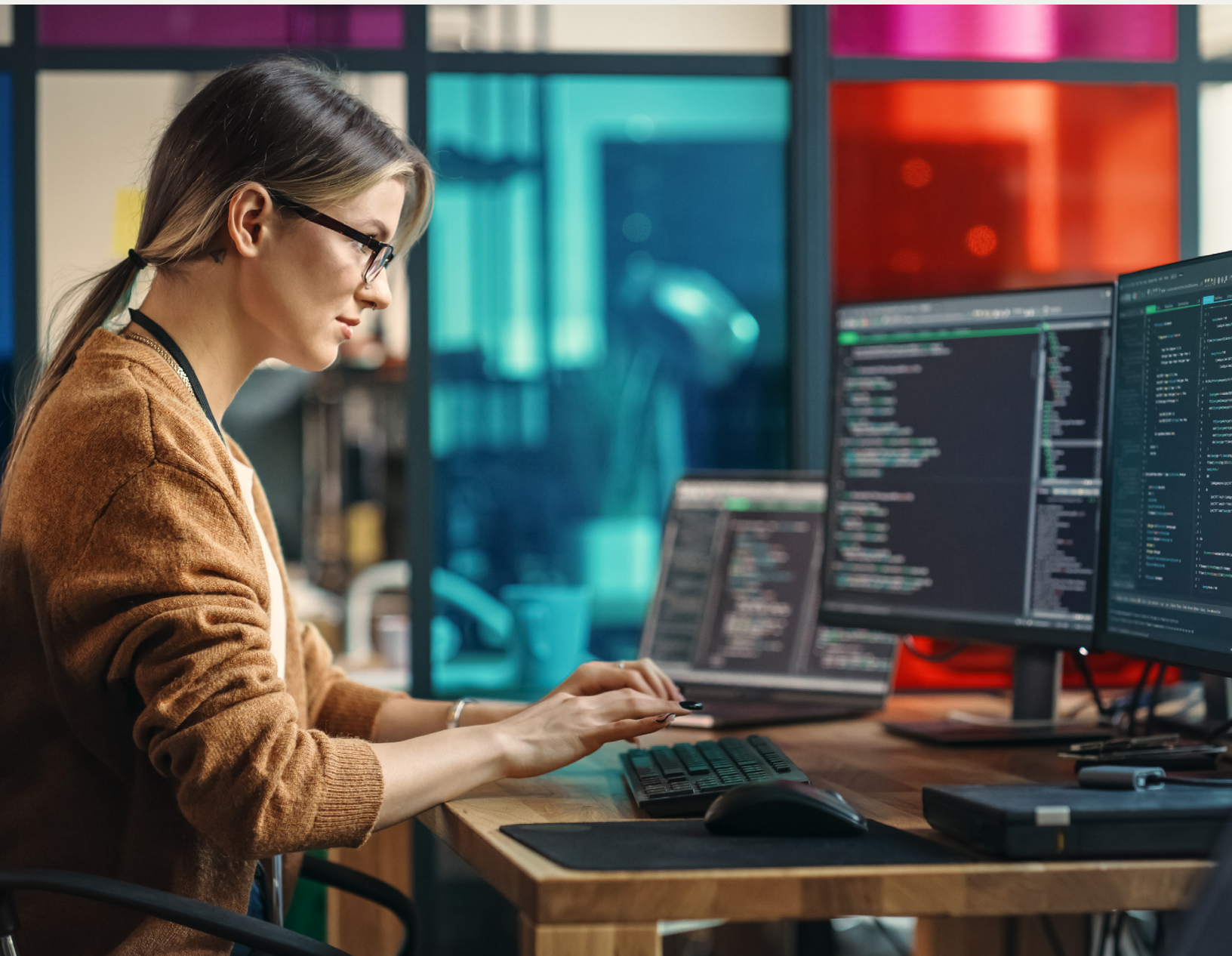
kyndryl

Continuous Control Monitoring

A proactive approach for a more resilient future



Contents

> “Businesses now operate in hybrid IT environments that combine both old and new technologies, which makes it harder to identify and manage risks.”

Market Context

In today’s technology-driven business environments, one thing is clear: enterprises face no shortage of hazards that can slow progress and disrupt their day-to-day operations.

To lower the likelihood of risks turning into actual problems, businesses establish risk policies that are, in part, executed through the implementation of IT controls. These controls can vary widely, including measures that restrict access to sensitive systems, promote accurate record-keeping, and aim to ensure data backups. The effectiveness of these controls is evaluated through routine monitoring and random checks, as organizations identify security gaps and address vulnerabilities.

Yet traditional methods of control monitoring are increasingly inadequate as technology environments become more complex. Businesses now operate in hybrid IT environments that combine both old and new technologies, which makes it harder to identify and manage risks. Additionally, the growing number of digital services that enterprises rely on for smooth and secure operations has created new opportunities for cybercriminals to execute more frequent, sophisticated, and damaging attacks. Moreover, due to greater scrutiny from regulators, leaders must now proactively manage enterprise risk.

Only 29% of business leaders feel ready to manage external risks, according to the Kyndryl Readiness report—and cyberattacks are their top concern. The report also found that three in five leaders struggle to keep up with the speed of technological advancements and one in two say regulations are changing too fast.

Many Chief Information Security Officers (CISOs) may be uncertain about which issues to prioritize as they navigate competing demands while working to secure a growing attack surface. Traditional control monitoring that fails to provide full visibility into complex IT operations will cause businesses to fall behind, potentially exposing them to significant security and compliance vulnerabilities.

Enterprises with effective IT controls are more resilient than their counterparts; inadequate controls are often a significant factor behind major cyber incidents. Enhancing control monitoring can also aid in adhering to both global regulations and internal risk management policies, creating a strong foundation that enables organizations to advance their cybersecurity strategies and address larger technological challenges.

Continuous Control Monitoring meets these requirements by offering enterprises the chance to integrate their security and compliance efforts. This integration enables proactive risk management, boosts cyber resilience, and facilitates a comprehensive transformation of their technology, processes, and work practices. As enterprises strive to innovate, grow, and remain competitive, Continuous Control Monitoring will be essential. By adopting this approach, organizations can build trust with key stakeholders regarding their ability to manage ever-evolving risks.

54%

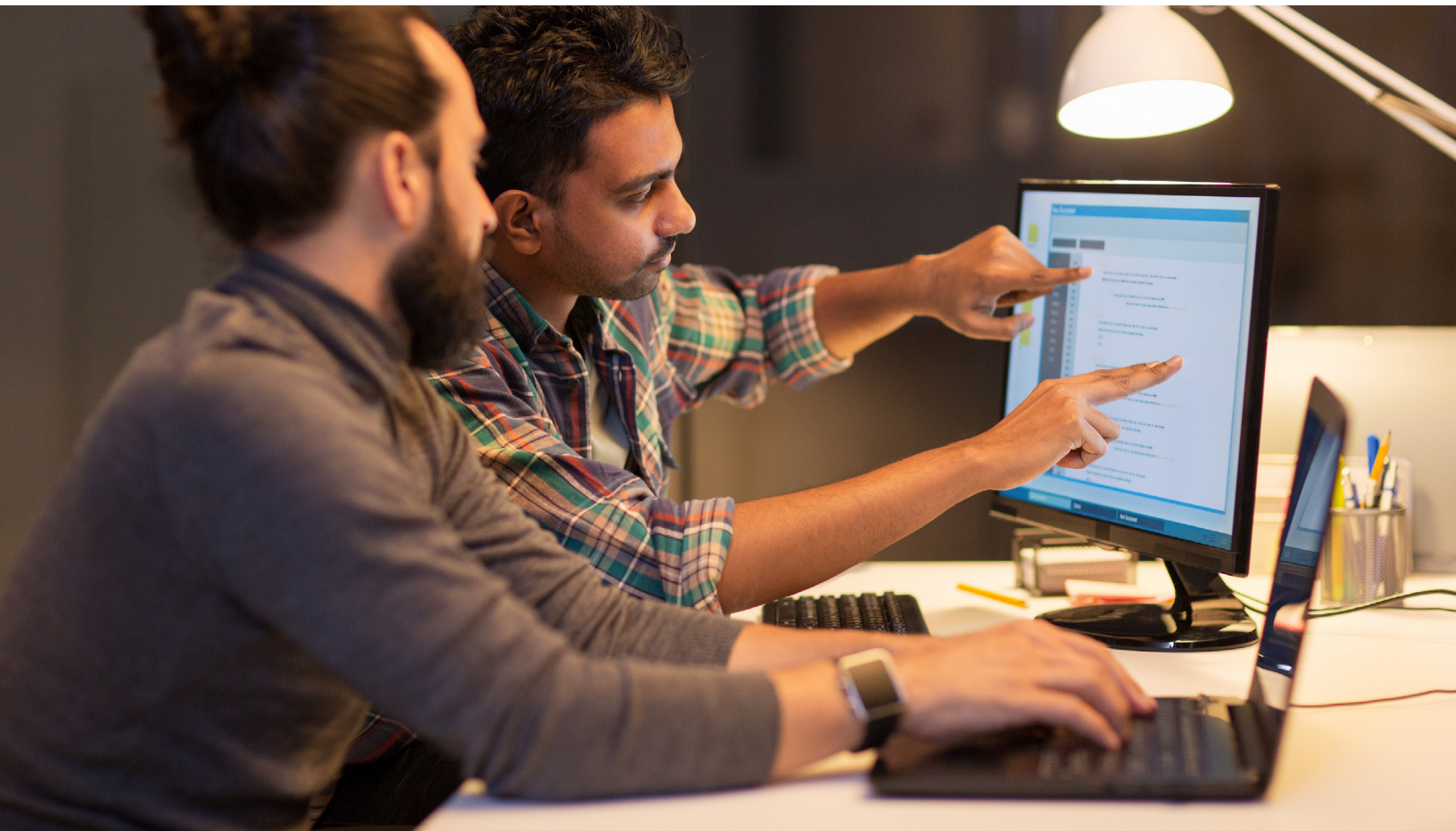
Large organizations that say a cyberattack disrupted their IT systems and data in a recent 12-month period[1]

78%

Organizations that report their security tools lack interoperability, meaning their tools are often unable to share security data or insights[1]

67%

Business leaders who don't feel their cybersecurity and resiliency measures are ready to manage future risks[1]



Continuous Control Monitoring

What is CCM?

Continuous Control Monitoring (CCM) refers to the ongoing, automated oversight of IT systems and business processes to monitor adherence to internal risk policies and regulatory requirements. CCM enables organizations to detect and prevent errors and inefficiencies in near real-time by continuously analyzing data and identifying anomalies or deviations from established controls.

Organizations typically implement a comprehensive set of controls to ensure the security and compliance of their IT environments. The range and scope of control policies are extensive, including but not limited to:

- **Inventory:** All devices and applications must be registered in the appropriate security inventory systems to ensure accurate tracking and management.
- **Identity and Access Management:** User access is authorized, revalidated regularly, and managed through unique IDs and the principle of least privilege to ensure accountability and security.
- **Configuration, Build, and Decommission:** Devices and systems are configured, built, and decommissioned following strict security controls and documented processes to maintain integrity.
- **Security Management:** Comprehensive security measures, including logging, monitoring, and incident response, are implemented to protect data and systems from unauthorized access and threats.
- **Disaster Recovery:** Detailed disaster recovery plans are documented, tested annually, and include data replication and risk mitigation strategies to ensure business continuity.
- **Backup and Restore:** Operational backup and restore capabilities are documented, regularly tested, and include procedures for data recovery in case of an outage.
- E**nterprise Privacy:** Privacy by design principles are integrated throughout the operational cycle, ensuring data is processed fairly and lawfully in compliance with privacy regulations.

CCM is a proactive approach to risk management that significantly strengthens the cyber resilience of large, complex, and often heavily regulated global organizations. To further enhance this approach, enterprises are increasingly using AI-powered services to simplify and automate control monitoring. These services include diagnostics, management insights, and compliance reporting.

Embracing CCM involves transforming teams, technologies, and processes. With CCM, enterprises can optimize key processes and increase collaboration among IT operations, risk management, and audit teams to boost productivity, drive efficiency, and improve transparency. Additionally, teams can use insights provided by CCM to consistently assess the effectiveness of their controls as threats change. This enables them to identify, prioritize, and address risks more quickly and accurately. As a result, CCM plays a crucial role in helping companies enhance their risk management efforts and comply with internal policies, external regulations, and industry standards.

The Business Value of CCM

With CCM, enterprises can improve cybersecurity, risk management, and operational efficiency.

Cybersecurity	Compliance and Risk Management	Operational Efficiency
Increased Resilience: Seamless security and compliance integration can increase adherence with internal risk management policies, cybersecurity frameworks, and cyber regulations, making enterprises more resilient.	**Data-Driven Decision Making:** With near real-time insights into control performance, management can make informed decisions quickly. This enables more agile responses to emerging risks and opportunities.	**Maximized Productivity:** CCM reduces overlaps and manual efforts between IT, security, and audit teams, enabling them to focus on higher-value tasks.
Enhanced Visibility: AI technology enhances automation and accuracy in control monitoring with real-time threat detection and compliance response.	**Greater Transparency:** A clear view of IT control effectiveness improves transparency, enhances stakeholder communication, and strengthens trust in the organization's risk management strategies.	**Reduced Costs:** By automating control effectiveness monitoring, CCM reduces the time and costs associated with manual security assurance tasks and audit processes.
Proactive Mitigation and Remediation: By providing immediate alerts for control failures and implementing advanced automation to address identified issues, organizations can tackle problems before they lead to significant disruptions, minimizing operational downtime and reducing financial losses.	**Faster Prioritization:** CCM automates risk assessments and alerts for quick remediation, enabling the prioritization of risks with context and metrics.	**Improved Accuracy:** CCM improves accuracy with preconfigured dashboards and reporting, helping security and risk management teams test and report on cybersecurity controls more effectively.

By integrating security and compliance activities, enterprises become more resilient to cyber disruptions. This integration allows for faster threat detection and response, as well as the automation of processes to proactively tackle issues.

CCM provides a clear view of control effectiveness across the organization and enables data-driven decision-making, empowering leaders to prioritize their most critical initiatives. Furthermore, setting clear roles and responsibilities between teams involved in risk management increases productivity. It reduces manual audit efforts, which are often time-consuming, error-prone, and costly, freeing up resources for more strategic work.

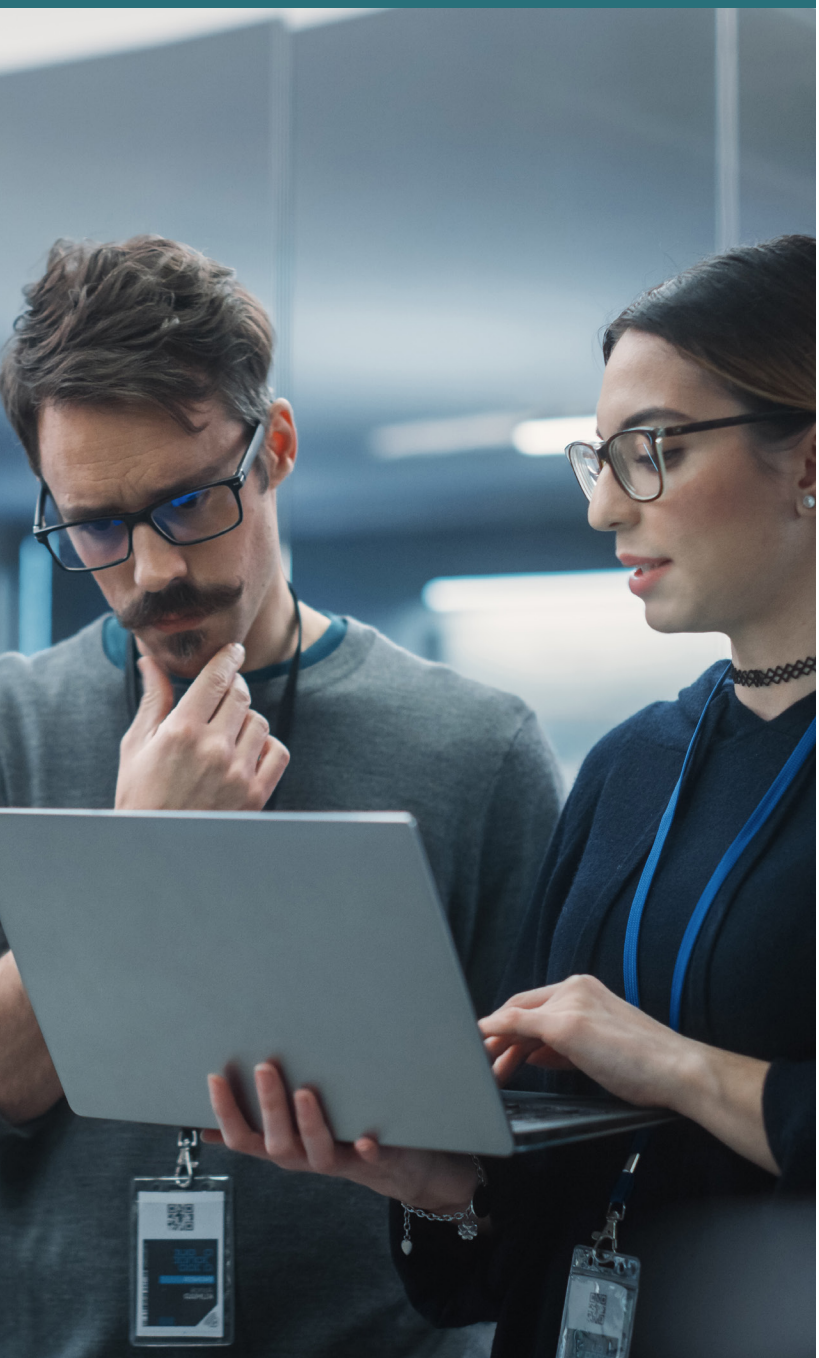
Complete and accurate compliance reporting provides greater transparency into enterprise risk, enhancing stakeholder communication and strengthening trust in the organization's risk management strategy.

Cyber Regulations and Frameworks

The global regulatory landscape continues to evolve, and enterprises are likely to find even more value from CCM as they strive to adapt. Such regulations include the Digital Operational Resilience Act (DORA), which establishes security requirements for EU financial entities' network and information systems; the Network Information Security Directive (NIS2), which establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU, including healthcare, energy, and digital infrastructure; recent Japan Financial Services Agency (JFSA) cyber guidelines; efforts by the Reserve Bank of India (RBI) to strengthen a cybersecurity framework; a recent Executive Order in the US intended to transfer cybersecurity responsibilities from federal to state government; and several others already in place for years, such as those in Canada.

Additionally, CCM aids in building a strong foundation for established frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, developed in the US.

> As part of a smart risk management approach, businesses will be able to leverage technologies including agentic AI for the discovery of assets, the analysis and validation of control data, and the operationalization of remedial actions."



CCM also helps enterprises achieve international security standard certifications, including ISO 27001, which provides guidance for establishing, implementing, and maintaining an effective and proactive information security management system. The CCM approach can also directly assist organizations in implementing and adhering to the Unified Compliance Framework (UCF), an international framework designed to help organizations manage compliance more efficiently by reducing redundancies and overlapping requirements across multiple standards.

The Future of CCM

Looking to the future, the business value of CCM has the potential to grow, driven by advancements in automation and artificial intelligence.

As part of a smart risk management approach, businesses will be able to leverage technologies including agentic AI for the discovery of assets, the analysis and validation of control data, and the operationalization of remedial actions. Designed to operate autonomously and use sophisticated reasoning to solve multi-step problems, AI agents can communicate their actions to other AI agents, focusing on IT controls or business processes. This collaborative effort will enable a coordinated response to collectively mitigate risks across the business.

This shift to an ecosystem of proactive, protective technology can significantly enhance enterprise risk management.

Market Imperative

Risk management has been elevated to a C-Level conversation, necessitating that enterprises take more fulsome and proactive approaches to protecting their operations. CISOs must prepare their organizations to avoid and withstand a long list of threats—from system failures and operational disruptions to security breaches, regulatory penalties, and more. However, they need help to assess and prioritize the most urgent risks across increasingly complex IT environments.

Maintaining a robust control environment can help them overcome this hurdle. With CCM, enterprises can keep pace with evolving threats and regulatory requirements, gain new insights into their complex IT estates, more efficiently allocate resources, improve collaboration, and balance security with innovation. By neglecting this more proactive approach, enterprises will find themselves increasingly susceptible to potentially devastating breaches and costly disruptions, especially as more businesses look to capitalize on emerging AI technology that expands their digital attack surface.

There's no single methodology for the implementation of CCM; every organization is unique and seeks to manage enterprise risk to suit its strategic business goals. However, as business leaders proceed in developing their risk management strategies, they should consider an integrated approach to control monitoring that unifies security and compliance activities and enables teams to collaborate in new ways. Trusted technology partners can tailor CCM to an organization's specific needs to support their compliance and security goals, helping them carefully comply with regulations and rapidly respond to emerging threats.

Successful outcomes depend on integrating tools and data sources across complex hybrid IT estates and applying AI and automation to continuously monitor and improve control efficacy. Enterprises must also seize the opportunity to strengthen collaboration between IT, security, and audit teams to drive productivity and close regulatory gaps.

Prioritizing CCM will be integral to bolstering resilience and ensuring compliance in a constantly evolving threat landscape. With CCM, enterprises stand to transform their reactive approach to risk management into a continuous, proactive, and streamlined effort, building a stronger foundation for a more secure future.

For more information

To learn more about how Kyndryl can help your organization achieve its goals, visit kyndryl.com or contact **Tony De Bos,** Vice President, Governance, Risk and Compliance, at anthonie.debos@kyndryl.com

kyndryl

1. Kyndryl's **Cyber Gauge 2024** report / Kyndryl's **Readiness Report**