Trust, transparency, and continuous compliance

How a new approach to controls monitoring empowers security teams to build stakeholder trust, address hidden risks, and demonstrate compliance

February 2025

Cyber compliance demands are changing and provide an opportunity for a new approach

In this paper, KPMG LLP (US) (KPMG) and Panaseer explore the current pressures facing security teams and how a new approach to compliance can transform ways of working.

Chief information security officers (CISOs) face constant, around-the-clock external and internal pressures—be it ransomware, unpatched vulnerabilities, cloud misconfigurations, or inappropriate users with privileged access putting sensitive data at risk.

Meanwhile, the introduction of new legislation in the US and European Union (EU), such as the New York Department of Financial Services' (NYDFS) Cybersecurity Regulation and the EU's Digital Operational Resilience Act (DORA), are driving security teams to regularly demonstrate effective cyber governance and risk management to boards, internal audit, investors, regulators, and customers.

These constant demands combined with today's economic challenges, limited internal resources, and increasingly complex information technology (IT) environments are stretching security teams thin; 90 percent of security leaders feel they are being asked to provide more certification on security controls than ever before.[1] Teams are looking to find the right balance between provisioning services to manage cyber risk and delivering the oversight and compliance that business is asking for but sometimes lack the in-house expertise or automated approaches to help. KPMG cybersecurity services take an innovative approach to these modern challenges.

Under this increasing scrutiny, mature organizations are shifting their approach. Many are developing controls oversight functions to continuously monitor and assess the effectiveness of their cybersecurity controls. It gives these organizations the confidence, backed by evidence, that their cyber controls are effectively deployed and functioning as intended, and provides an efficient way to help ensure controls remain aligned with changes to regulatory standards.

Collating, analyzing, and reporting disparate data across multiple tools and for hundreds of controls is hugely time-consuming. This can often take almost half (46 percent) of a security team's time and resources in any given month.[2] An automated approach to continuously monitor controls aims to empower security teams and risk leaders to identify risks and prioritize remediation with greater speed and accuracy than traditional manual methods. CISOs can also quickly provide the oversight necessary to help meet today's demands for compliance.

---

[1] 2025 Security Leaders Peer Report, Panaseer
[2] 2025 Security Leaders Peer Report, Panaseer

This article explores three key challenges facing CISO functions and how an automated, continuous approach to controls monitoring can elevate the performance of security operations and transform the way security teams approach reporting, compliance, and risk management—now essential components of an effective cybersecurity program.

Incomplete view of cyber controls and performance

You can't protect what you can't see. Today's complex IT environments, with countless security tools in use across complicated organizational structures, mean unknown and hidden control gaps—leaving the business exposed to cybersecurity threats.

Regulatory and audit responsiveness

Increasing regulatory and audit demands mean security teams are having to face being "audit-ready" and able to rapidly produce reports from an overwhelming amount of data, demonstrating cyber governance, compliance, and industry leading-practice, without disrupting daily operations.

Fractured, point-in-time risk management

Prioritization of security operations by technical criticality alone is a one-dimensional approach to risk management, that doesn't consider the priorities and risk appetite of the business. Without direct access to performance data, control owners are unable to take accountability for the impact on an organization's risk management and security posture.

Incomplete view of cyber controls and performance

Complexity creates more opportunities for control gaps to go unnoticed

Incoming regulations in the US and EU—such as DORA, NYDFS, Securities and Exchange Commission Compliance and Disclosure Interpretations,[3] and others—require organizations to be more transparent around cyber resilience with robust risk management processes and assessments. It's forcing security leaders to continuously monitor and assess the state of an organization's security controls.

But complex IT environments are making manual reporting of controls effectiveness nearly impossible. The average business has over 75 security tools deployed,[4] producing an inordinate amount of invaluable—yet fractured and solitary—data.

Cybersecurity tools are often owned by different teams across the organization, creating data silos and making the process of manually gathering control performance data lengthy. Legacy tooling adds to the challenge by further separating the enterprise-wide security posture analysis.

It gets even more complicated when you consider that each tool tells its own story, often using different denominators to measure performance. Creating a single source of accurate, trusted data is not only time-consuming but also open to human error and misinterpretation.

Security operations are left attempting to effectively increase control coverage and reduce the chances of a control gap that can put the business at cybersecurity risk—but are often overwhelmed by data that can be difficult to make sense of.

79 percent of security leaders say they've been surprised by a breach that evaded a control they thought was operational.[5] CISOs are tasked with managing rapidly evolving risk and would benefit from continuous checks that security controls are deployed as intended and working as expected. Relying on tools that are focused on the collection of security event data fails to incorporate a proactive approach to cyber risk. Instead, a real-time independent view of control coverage and effectiveness can provide the confidence and reporting they often seek.

> CISO organizations would likely benefit from an effective, yet efficient way of analyzing and understanding controls performance data, limiting the impact of control failures.

---

[3] Securities and Exchange Commission Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

[4] 2023 Security Leaders Peer Report, Panaseer

[5] 2024 Security Leaders Peer Report, Panaseer

Regulatory and audit responsiveness

Intense demands for security teams to share data creates friction

Security teams are drowning in reporting requests from multiple sources—including internal audit; governance, risk, and compliance (GRC); and wider business teams.

With the challenges and constraints surrounding manually collating, normalizing, and analyzing necessary data, security teams often find themselves struggling to achieve their primary objective of protecting the organization and its critical assets.

Even after responding to numerous reporting requests, security teams often find themselves needing to answer follow-up questions and provide additional layers of insight.

In 2024, security teams spent on average almost half (46 percent) of their time on analysis and reporting.[6] The time taken to manually collate, correlate, and report necessary data means it is almost always out of date by the time it reaches its intended audience of either executive-level reporting or external regulators. This makes it difficult to draw meaningful conclusions, act on insight, and demonstrate compliance.

And this is all a repeat exercise. Teams must go through the same time-consuming process again when it comes to providing the next round of reporting or audits.

To put it simply: the growing need for routine reporting is using up valuable time security leaders could otherwise spend on helping operations to prioritize the actions that will drive progress in their security programs and protect critical services and data. Almost three-quarters (71 percent) of security leaders feel they could prevent more breaches if they spent less time reporting.[7]

> CISO organizations could maximize resources by moving from manual, point-in-time reporting to a continuous, automated approach.

Fractured, point-in-time risk management

A disconnect leaves control owners unable to prioritize cybersecurity risk remediation in line with business risk

The lack of real-time, contextualized insight is leaving organizations with little more to go on than technical risk for prioritization. The inability to link control gaps and failures to specific business context creates a lack of visibility regarding at-risk business services—and ultimately hinders efforts to protect the most critical services at highest risk.

This is especially true when considered in the context of an evolving threat landscape.

Bad actors are at work 24/7 and misconfigured tools and controls can often be the target of attacks. Security policies designed to protect an organization can often lack effectiveness and carry unmanaged risks.

Manually verifying each tool and control is configured correctly can be time consuming. With the prospect of an increasing number of attack vectors across a wider attack surface, one approach to support efficiency and effectiveness is the automation of control monitoring and reporting.

Security teams also rely on help and support from business teams to combat the evolving threat to critical services. By connecting control owners with insights into controls effectiveness, business teams can understand their impact on cyber risk.

With this enhanced visibility and continuous, real-time oversight, they can take responsibility for the cyber risk they own, prioritizing the actions that will both better protect critical services and help alleviate the constant pressure on security teams to be everywhere and fix everything.

Business teams can be empowered to protect critical services—but only if they have access to continuous risk and control insights

The emergence and unification of these challenges can be a driving force for change.

For organizations maturing their cyber controls oversight function and actively attempting to demonstrate compliance and build trust with a wider set of stakeholders, manually verifying, assessing, and reporting control effectiveness is quickly becoming untenable.

Instead, there is a growing trend for a trusted, transparent, and continuous approach to controls monitoring and compliance.

---

[6] 2024 Security Leaders Peer Report, Panaseer
[7] 2025 Security Leaders Peer Report, Panaseer

How an automated approach to compliance can transform ways of working

In the past, organizations have concentrated on developing their risk and control frameworks, aligning them with organizational entities, and conducting assessments through GRC tools to gain insights into risk and compliance.

While this approach provides a level of insight, it may be an incomplete view of an organization's cybersecurity risk and compliance posture. It provides only point-in-time insights that quickly become outdated and are not scalable with the evolving threat landscape and organizational changes.

Many organizations, without realizing it, possess vast amounts of data—a veritable gold mine that, when properly harnessed, can revolutionize their compliance and cybersecurity efforts. But manually collating, verifying, and analyzing this data is taking up a considerable amount of time and resource of enterprise cybersecurity teams.

Advanced organizations are empowering teams to utilize the data they hold with an automated Continuous Controls Monitoring (CCM) approach, which uses technology to monitor and validate the effectiveness of an organization's security controls, eliminating the manual and time-consuming data tasks and extracting actionable, trusted insights along the way.

Creating an effective CCM framework can be daunting—but the potential benefits of an automated approach are too significant to ignore. Extracting actionable insights from the data necessitates a well-designed framework. This involves establishing robust governance, creating a comprehensive data model, designing an effective solution architecture, and implementing seamless data integration and analysis processes.

Below are six crucial steps to implement CCM:

1 Define the overall strategy and governance structure

Establishing CCM can seem daunting, but it should begin with a clear vision and a pragmatic phased roadmap to enable CCM capabilities. This strategy should prioritize audit requirements, identify controls suitable for CCM, evaluate available data sets and optimal utilization, assess the tools available for facilitating CCM, and determine which organizational entities require continuous monitoring. Once the vision and strategy are in place, a phased roadmap can guide the implementation process.

2 Establish a comprehensive data model

A well-defined data model is essential for accurate data organization and interpretation. Given CCM's reliance on data, it is crucial to specify which controls will be automated, identify the necessary data to automate compliance checks, determine data sources, outline data transformation requirements, and establish compliance thresholds. This model serves as a rulebook for operationalizing the CCM solution.

3 Design a robust solution architecture

Creating a robust CCM solution architecture involves integrating diverse data sources and ensuring a seamless data flow into a centralized system. This setup may include integrating with various data sources, a centralized data lake, a GRC tool for issue and risk management, a business intelligence tool for advanced reporting, or a purpose-built CCM platform.

4 Define clear processes and workflows

Establishing well-defined processes for data collection, analysis, control failure response, and reporting is critical. Automated workflows can streamline these processes, minimizing manual effort and ensuring relevant stakeholders receive timely updates.

5 Define response strategies

Enabling CCM is great, but what happens if there is a control failure? Having roles, responsibilities, and mechanisms to handle these so that failures can get addressed in an efficient manner will help drive business value.

6 Implement advanced tools and technology

Enabling CCM requires sophisticated technology capable of integrating, processing, and analyzing large data sets to provide continuous compliance insights. Using a purpose-built platform can provide the accuracy, trust, and transparency required to realize the potential benefits.

Using technology and automation to empower continuous controls performance

Automated CCM technology leverages advanced technology to continuously monitor and validate the effectiveness of an organization's security controls.

CCM technology delivers the verified data and robust insight necessary for demonstrating compliance, withstanding board scrutiny, and addressing risks. By processing extensive data sets at scale, teams can seamlessly connect security operations to oversight and compliance, providing an accurate and quantified view of an organization's risk and compliance on an ongoing basis.

By bringing data together continuously and in near-real time, security teams can have a complete view of cyber controls and performance, addressing risks that were once hidden. They're able to respond more effectively to regulatory reporting and potential audits, without dedicating unnecessary hours and disrupting daily operations.

With a continuous source of trusted and transparent data, security teams can also prioritize remediation efforts in line with business risk and take the right action at the right time. Additionally, once armed with data, security teams can better embed themselves within the organization, holding relevant departments and individuals accountable, and offer the support and guidance to sufficiently protect data and services.

Using automation to address core challenges for CISOs and security teams

A continuous, accurate, and quantified view of an organization's cyber risk empowers security teams to focus. Areas that are often prioritized include:

Address hidden risks

▶ With oversight and performance insight, teams can proactively own efforts to improve the effectiveness of security controls, limiting the impact of control failures on the organization

Demonstrate compliance

▶ Become audit-ready with direct access to automated security control reports, releasing valuable time to focus on more meaningful tasks

Prioritize effectively

▶ Protect critical services and assets by focusing on the control gaps and failures that pose the biggest risk, using contextualized performance data mapped to an organization's thresholds and regulatory standards

How to advance your Continuous Controls Monitoring program

Combining multiple data sources to unearth hidden compound risks

Bad actors exploit vulnerabilities, often taking advantage of scenarios that link multiple weaknesses.

Alone, these weaknesses may not be critical. But together they can lead to serious breaches—they are toxic combinations that increase the level of risk and opportunity for an attack to be successful.

Addressing these interconnected vulnerabilities requires a detailed analysis of the entire attack chain. Security professionals must look beyond individual vulnerabilities and assess how they can be linked together in a multistep attack. It's a comprehensive approach that without continuous monitoring can be difficult to achieve.

Neil Hooper, Vice President of Alliances at Panaseer, says: "With the complexity of cybersecurity challenges, we see KPMG as the leader in providing advisory services to guide the organization. The Panaseer CCM platform is designed to support this approach by providing hundreds of out-of-the-box metrics and intuitive dashboards, which can be customized, with the support of KPMG's guidance, to individual use cases and needs. This includes compound risk metrics, which automatically identifies high-risk scenarios and areas of heightened exploitability across various cyber control domains."

Achieving success with CCM

By implementing a CCM framework, organizations can overcome the fatigue associated with manual assessments, reduce cybersecurity risk, and enhance their ability to meet regulatory and cybersecurity requirements. At KPMG, we offer solutions to help businesses design, implement, and optimize their CCM capabilities.

The KPMG approach to CCM, coupled with the implementation of a CCM platform such as Panaseer's, is centered on helping organizations unlock the full potential of their data, leveraging technology to automate and streamline compliance and risk management activities enabling businesses to achieve a state of continuous compliance, reduce risk, and enhance their overall security posture.

For more information on how to set up a CCM program and leverage your data effectively, reach out to our contacts. We are here to help you navigate the complexities of modern regulatory and cybersecurity landscapes.

About Panaseer

Panaseer is a CCM platform that empowers cybersecurity risk and compliance leaders in complex enterprises to manage risk and reduce control failures.

Daily, objective insights into controls coverage, effectiveness, and performance help cybersecurity leaders to address hidden risks, strengthen governance, speed up compliance reporting, and maintain continuous audit readiness. Unlike other solutions, Panaseer combines data science with best-practice cybersecurity expertise, offering an independent, flexible solution that's purpose-built for enterprise data volumes.

About KPMG Cyber Security Services

KPMG has experience across the continuum—from the boardroom to the data center. In addition to assessing your cyber security program and aligning it to your business priorities, we can help you develop advanced approaches, implement them, monitor ongoing risks and help you respond effectively to cyber incidents. So no matter where you are on the cyber security journey, KPMG can help you reach your destination.

Contact us

Neil Hooper
Vice President of Strategic Partnerships
Panaseer
neil.hooper@panaseer.com
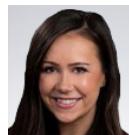
Angie Leggett
Managing Director, Cyber Security Services
KPMG LLP
aleggett@kpmg.com

Lavin Chainani
Managing Director, Cyber Security Services
KPMG LLP
lchainani@kpmg.com

Shamik Shukla
Director, Cyber Security Services
KPMG LLP
shamikshukla@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in   kpmg.com