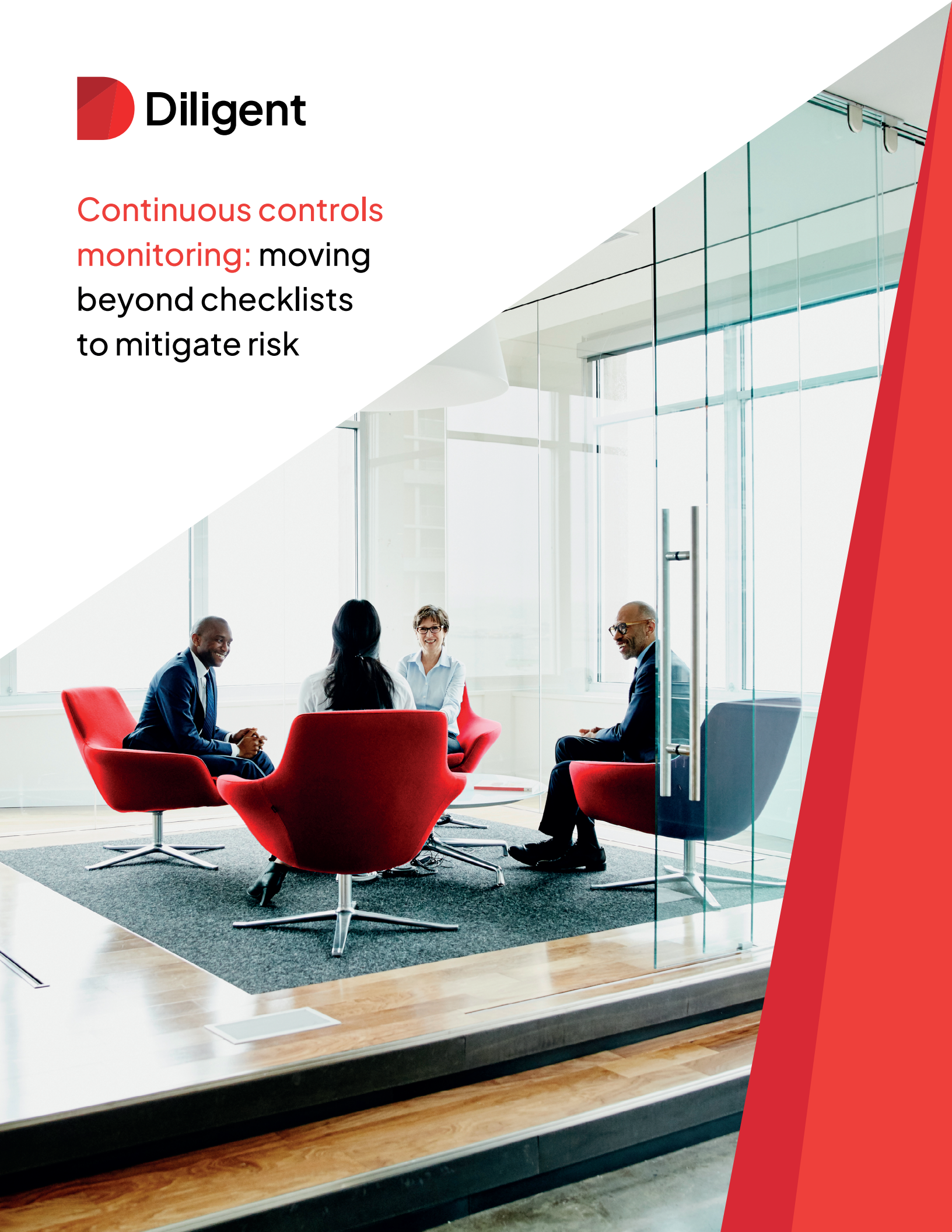
Diligent

Continuous controls monitoring: moving beyond checklists to mitigate risk



High-profile data breaches have been making headlines across the Asia-Pacific region. In New Zealand, a third-party data breach affecting several government organisations compromised thousands of autopsy reports and other data. In Australia, recent major breaches of a health insurer and telecom company resulted in a combined 19.5 million stolen customer records. A further 14 million highly sensitive customer records were stolen in March when a consumer finance provided was the latest to fall victim to a cyberattack. A Bloomberg estimate put the total company cost for just one of these attacks between A$700 – A$960 million.

For dining app company Eatigo International, insufficient digital security measures resulted in a data breach that affected 2.76 million individuals, a fine from Singapore's Personal Data Protection Commission and a recommendation from the regulators to build a comprehensive data inventory that classifies risk levels for the personal data it collects. The consequences of insufficient IT compliance can be high.

In light of these increasingly frequent incidents, one concept has become top of mind for IT and information security professionals: continuous controls monitoring.

Several converging factors drive this trend. As high-profile cyberattacks and data breaches continue to make headlines, the compliance landscape itself has become increasingly complicated.

In Europe, organisations face evolving regulations related to data access, cloud providers and artificial intelligence. In the Asia-Pacific region, authorities from Singapore to Australia are refining their approaches to mandatory breach notifications, privacy regulations and cyber resilience. And in the Americas, organisations have new rules to consider from the U.S. Securities and Exchange Commission on cybersecurity risk management, strategy, governance and incident disclosure.

The cost of getting compliance wrong is high – businesses can face fines, potential legal action, reputational damage and more. Meanwhile, the benefits of a robust IT compliance program are many.

With continuous monitoring of critical controls, an organisation can establish a strong compliance posture against a growing number of global IT and information security standards, and quickly pivot for new and evolving requirements.

Controls, compliance and the need for continuous monitoring

Robust IT compliance gives organisations visibility into regulations, operations and how the two align, strengthening leaders' ability to make informed decisions. It also helps organisations seize opportunity by wrangling the many certifications required for bids, contracts and other new business prospects.

Risk, audit and IT teams are able to do more (and more quickly) when they're equipped with automated workflows and a common controls framework (CCF). Meanwhile, accurate records and a view of resources mapped against risk and ROI keep teams accountable.

As organisations have become more and more reliant on digital systems and technologies for their operations, controls have emerged that are critical to regulatory compliance, security, risk management and business continuity. These controls can flag issues from user access to segregation of duties, and require rigorous testing to ensure they are working as they should.

IT controls help risk, audit and information security teams determine how well the organisation's compliance program is working. For example:

- ✓ What's the approval process for deploying new code into production, and how well is it being followed?
- ✓ What about the communication and enforcement of password policies?
- ✓ Are critical vulnerabilities being addressed in a timely manner?
- ✓ Can IT staff see when data backup failures fall below a certain threshold?
- ✓ Are IT staff able to regularly access log files for things like firewall configurations?

With both tech stacks and regulatory requirements continuing to grow, it's become increasingly difficult to maintain oversight over these controls. Periodic testing and a 'checklist' approach are no longer enough to stay ahead of constantly evolving threats or ensure the organisation's controls are keeping up. At the same time, IT and information security teams need new systems and tools to expand testing coverage as their technology footprint expands.

This is where continuous controls monitoring comes in. When powered by automation, these systems streamline the many processes related to controls testing. This accelerates the identification of vulnerabilities and gaps, and enables IT and information security teams to do more with less, freeing them up for more value-added work. Finally, the digitised, centralised and integrated aspects of continuous compliance monitoring enable compliance and risk management responsibilities to be mapped and tracked for increased accountability throughout.

With this approach, IT and information security teams can actively manage cyber risk, third-party risk, regulatory risk and more across the organisation. This in turn strengthens the organisation's relationships and reputation with regulators, investors, partners, customers and other key stakeholders.

6 steps to

setting up a continuous controls monitoring system

01

Identify relevant laws, regulations, certifications and standards

Just as a building needs a solid foundation to stand securely, a successful controls monitoring system must be built upon the right rules and requirements.

To ensure alignment, IT and information security teams should identify and become familiar with the applicable frameworks and standards for their organisation, as well as their underlying requirements.

Common examples include ISO 27001, the international standard for managing information security risks such as cyberattacks and data leaks; SOC 2 for organisations storing customer data; and PCI-DSS, governing payments and credit cards.

This information will guide the creation of a content repository that puts regulations and required data in one place, allowing compliance teams to search by type, region, important dates and more.

This step enables organisations to align IT controls and testing to the most recent, relevant compliance requirements.

APAC compliance updates: Are your controls ready?

The Asia-Pacific region is rapidly responding by modernising data and security regulation. In Singapore, regulators have been sharpening their focus on specific industries, from the Cybersecurity Labelling Scheme for Medical Devices to updated expectations by the Monetary Authority of Singapore ('MAS') on how licensed insurers notify the public about data breaches.

In Australia, organisations who've just got used to the 13 Information Privacy Principles – which govern how organisations respond to breaches and inquiries about personal data – will need to add a revised Cybersecurity Strategy and a reformed Privacy Act to their radar. The latter increases the maximum civil penalty for serious or repeated interference, and expands the act's extraterritorial application and the investigation and enforcement powers of the Office of the Australian Information Commissioner. In addition, the Attorney-General's Department recently released its Privacy Act Review Report, which includes an additional 116 recommended changes (many significant), that, if adopted, will fundamentally change how Australia deals with data.

02

Assess risks, costs and impact

Once IT compliance teams have identified the relevant frameworks and requirements that monitoring system will need to accommodate, it's time to determine control priorities, and build the business case and buy-in for a monitoring solution. This involves quantifying the risks, costs and impact of incidents slipping through the cracks.

Poor controls and oversight related to IT compliance can be a very expensive mistake in today's world. According to IBM's 2022 Cost of a Data Breach report, compliance failures increased the average cost of a data breach by 68.28%.

As we touched on earlier in this guide, regulatory fines are just the beginning of how IT non-compliance can impact an organisation's bottom line.

Lapsed, lagging or a lack of security certifications leave money on the table when potential clients mandate these assurances within contracts or tenders. IT compliance standards exist to give companies and consumers confidence that their data is safe; incidents that slip through the cracks hinder trust and put an organisation's reputation at risk.

03

Map out requirements, risks and existing resources

The steps we've covered so far feed into compliance mapping – the process of connecting regulatory requirements to risk management, control and the compliance processes that already exist across the organisation.

Often considered among the most critical aspects of a compliance management system, compliance mapping involves:

- ✓ Assessing non-compliance risks for each requirement
- ✓ Defining processes for how each requirement is met
- ✓ Defining controls that make sure the compliance process is effective in reducing non-compliance risks
- ✓ Mapping controls to specific analytics and tests that confirm effectiveness

04

Put innovations like automation to work

With gaps and requirements identified, it's time to explore monitoring in detail. The organisation will need processes and tools to determine each control's compliance status – including coverage, potential issues and assurance levels.

Continuous monitoring enables this to occur in real-time and on a continuous basis. And technology makes continuous controls monitoring possible, particularly with tools that feature automated workflows and testing.

Organisations lose out by not fully tapping technologies like automation and AI for controls monitoring and compliance management. Automation enables testing efforts to go beyond mere samples of activity data, yielding a fuller picture of whether compliance controls and processes are working as they should. An AI engine can accelerate control mapping for multiple security requirements, further saving time and improving accuracy.

With a common controls framework (CCF), teams can build controls once for use across multiple frameworks, requirements and certifications.

05

Enable robust reporting

Continuous controls monitoring is only effective if the right information gets to the right people at the right time, in a way that's easy to digest.

Without a clear view of compliance risks – and the effectiveness of IT controls for flagging and mitigating these risks – chances are high that something significant will slip under the radar and go unaddressed.

Robust reporting capabilities are an essential part of a continuous controls monitoring system. Risk, audit, compliance and IT/information security teams need an efficient and easy way to provide status updates, quickly identify and address gaps in IT controls, and use the results of this monitoring to assess risks and trends.

When evaluating solutions, look for customisable templates, ready-to-use visualisations and executive dashboards.

06

Make the system even smarter with advanced analytics

Continuous controls monitoring systems collect vast amounts of data. Advanced analytics help IT/information security, risk, audit and compliance teams put this information to work for even greater insight and effectiveness.

Are tests running slower or faster than organisational or industry benchmarks? Are duplicate processes impeding efficiency? Advanced analytics cut through the terabytes of data to answer questions like these.

Particularly when integrated with data from other systems, like an organisation's ERP, advanced analytics empower IT compliance teams to improve controls monitoring and turn anomalies and exceptions into actionable insight.

Find the right tools

Not all software options offer specialised risk and control monitoring for the complexities of today, or the flexibility and scalability for the requirements of tomorrow.

Learn how Diligent's IT Compliance solutions are built with these considerations in mind to help organisations grow securely and confidently into the future.

Schedule a Demo

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Empowering more than 1 million users and 700,000 board members with a holistic view of their organisation's GRC practices so they can make better decisions, faster. No matter the challenge. Learn more at diligent.com.

For more information or to request a demo:

info@diligent.com | diligent.com/en-au

© 2023 Diligent Corporation.