

MITR/TECH | Governance, Risk & Compliance

Be Prepared! Get Ready to Answer Your Board's Upcoming Questions About Your IT Risk Technology

Equip yourself with the knowledge and tools needed to confidently address your stakeholders' inquiries and stay one step ahead in the ever-changing realm of IT risk oversight.

EMPOWER. AUTOMATE. ELEVATE.



Table of contents

- 3** Introduction
- 4** IT risk management 101
- 6** The regulatory landscape
- 8** Mitigating IT risk: where to begin
- 9** How to leverage GRC technology: 3 key missions for stakeholder transparency
- 11** Conclusion

Introduction

In the dynamic landscape of business and GRC technology, 2023 - 2025 marks a pivotal period for companies of all sizes. The renewed focus on managing IT risk has become not just a priority but a business-critical imperative. This shift is underscored by increased regulatory activity, like the [U.S. Securities and Exchange Commission's \(SEC\) proposed amendments](#), which compels organizations to provide comprehensive reporting on cybersecurity incidents and disclose their strategies for identifying and managing cybersecurity risks.

Your board is poised to become more involved than ever in understanding and overseeing your IT risk technology – and they're going to start asking more questions. Equip yourself with the insights, answers, and resources you need to maintain trust and visibility with your stakeholders as you navigate the evolving IT risk landscape.







IT risk management 101

IT risk encompasses any potential adverse impacts to an organization's information technology systems, processes, or data. This includes threats such as cyberattacks, system failures, data breaches, technological vulnerabilities, etc.

By defining and exploring the various types of IT risks, organizations can gain a better, more comprehensive understanding of the potential challenges facing their operational resilience. Recognizing the importance of IT risk management is crucial for the overall health and sustainability of a business.

Effective IT risk management acts as a safeguard, protecting critical assets and ensuring the continuity of operations. It goes beyond mere compliance, becoming a strategic imperative for organizations seeking to navigate the complexities of a rapidly evolving technological environment.

Key components of IT risk management involve a deep dive into fundamental elements such as:

-  **The starting point:** a holistic view of the organization's entire IT infrastructure and extended service providers (third parties).
-  **The challenge:** devices, networks, users, and the intricate web of interconnected risks that they represent.
-  **Information security compliance:** a core part of IT risk management. Regardless of the certification (ISO 27001, NIST, SOC2 Type 1...), demonstrating best practices in this space has never been more crucial.
-  **IT risk quantification:** detecting, monitoring, mitigating, and preventing risks across your entire business ecosystem and beyond. Quantification is key; otherwise, how can you truly understand the real magnitude of a threat?




Two-thirds of executives consider cybercrime their most significant threat in the coming year.¹

These components form the foundation for a proactive and adaptive approach, allowing organizations to not only address existing risks but also anticipate and mitigate emerging threats.

Key challenges in IT risk management

As companies delve into the complexities of IT risk management, they encounter a myriad of challenges that demand strategic attention and thoughtful solutions. Navigating these obstacles is integral to building a robust defense against potential threats. Below are some key challenges that organizations often face in the realm of IT risk management.

- 1. Limited cyber capabilities:** CSOs see the need to advance further through investment in cyber capabilities and people process technologies.
- 2. Heightened threats:** enterprises are under-prepared to respond to rising threats.
- 3. Regulatory reporting:** the pressure continues to mount as regulatory requirements for better visibility increase
- 4. Resilience:** with the uptick of ransomware and cyber attacks, the capacity to withstand or recover quickly is imperative.



45% of security and IT executives expect a further rise in ransomware attacks.²



A tip from the experts: according to PWC's survey,³ executives are prioritizing 5 best practices to mitigate attacks:

1. Enabling remote/hybrid work
2. Accelerating cloud adoption
3. Increasing data volumes
4. Converging OT and IT
5. Digitizing of how services are delivered to clients

²PWC, 2023

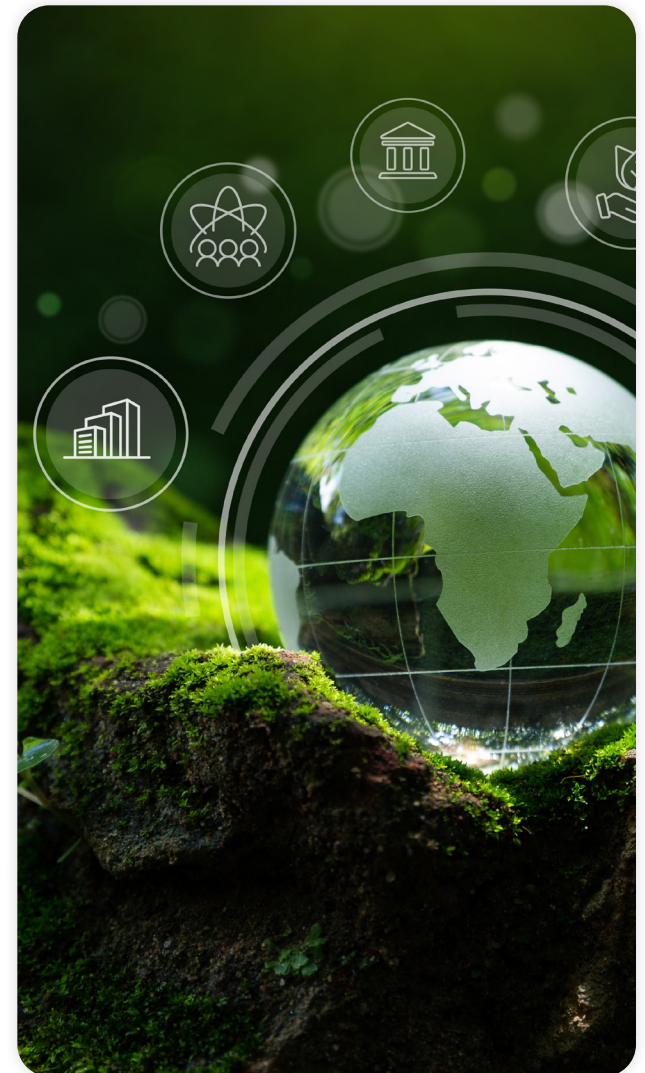
³PWC, 2023

The regulatory landscape

When we look at how the world has changed with the power of technology, more and more businesses are making great use of the cloud and third parties. While helpful in optimizing business operations, it is important to recognize that **cybercriminals are also getting more savvy in finding new ways to exploit these technologies, which has increased the number of cyberattacks**. As a result, a lot of effort is going into creating effective disclosure and transparency practices for anyone affected: investors, executives, board members, and the infosec team.

Navigating regulatory requirements is a critical aspect of effective IT risk management, considering the ever-evolving landscape of compliance standards. Organizations must stay informed and adapt to changes in regulations that directly influence their IT risk strategies.

Read on for an example of one such update.



The SEC's cyber disclosure rule

Delving into specific guidelines, particularly those proposed by authoritative bodies like the U.S. Securities and Exchange Commission (SEC), provides a detailed understanding of the expectations and obligations placed on today's businesses.

In 2023, the SEC adopted rules requiring public companies to report material incidents **within four business days** after determining that an event has occurred.⁴ It also requires registrants to disclose material information regarding their cybersecurity risk management, strategy, and governance on an annual basis.

The SEC's new rules on cyber risk reporting include topics like:

- Material cybersecurity incidents
- Periodic updates about previously reported incidents
- Registrant's policies and procedures to identify and manage cybersecurity risks
- Registrant's board of directors' oversight of cybersecurity risks

- Management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures
- Annual reporting, or certain proxy disclosure, about the board of directors' cybersecurity expertise

IT risk management compliance goes beyond the SEC, encompassing various regulations and standards that impact IT risk management practices globally. Understanding the global perspective is imperative, as international regulations contribute significantly to shaping an organization's IT risk management strategy. Organizations worldwide are already crafting best practices (whether they are public companies or not) around third party risk management.

A comprehensive IT risk management approach ensures that businesses meet local compliance requirements **and** adhere to broader international standards, fostering a robust and adaptable framework that aligns with the complexities of the global business environment.

⁴PWC, 2023

⁵Mitratech, 2022

Mitigating IT risk: where to begin

To address this new paradigm of IT risk in today's technology-driven landscape, you'll need to build a strong IT risk management framework. Here's a quick look at what that entails:

IT infrastructure: a complete register of the organization's technology assets is essential. This marks the starting point for any cybersecurity framework.

Protection measures: develop specific measures to put in place in different scenarios as part of an operational resilience framework.

Regulatory compliance: follow not only specific regulatory requirements on cyber risk management that impact your organization but also certifications of value and weight in this space (like ISO 27001).

Third-party risk management: at this point, there should be a [third-party risk management program](#) within every organization.⁶ It is important to keep in mind that working with any third party comes with an inherent risk that must be analyzed.

Risk-aware culture: lastly, training and awareness. Technology, processes, and people come hand-in-hand – train your teams to make well-informed decisions by creating a risk-aware culture within the organization.

These foundational steps provide a solid starting point for companies to initiate and navigate the path toward mitigating IT risks and ensuring long-term resilience.

IT Infrastructure



Protection Measures



Regulatory Compliance



Third-Party Risk Management



Risk-Aware Culture

⁶Mitratech, 2023

How to leverage GRC technology: 3 key missions for stakeholder transparency

Technology can be a powerful business partner, capable of empowering organizations with risk management capabilities like:

- Real-time monitoring and full environmental visibility
- IT risk quantification
- Powerful data analytics
- Automation and ease of use
- Framework alignment and asset modeling
- Scalability and business continuity



There are three key “transparency missions” your organization should be aiming to accomplish when approached by board members or stakeholders. Here’s a closer look at each — along with insights on how an integrated GRC platform (like [Mitratesh's Alyne](#)) can help.



Mission: Reporting for everyone

Let visuals tell the risk and compliance story for you.

Simplify information.

Create consistent, real-time views of your risk and compliance posture in easy-to-consume ways for those who only want the 30,000-ft perspective. Provide the drill-down ability for anyone who requires further analysis.



Mission: Adaptability to rapid regulatory changes

Smart technology helps you stay compliant and efficient.

Use machine learning to automatically match laws, standards, policies, and controls.

Increasing regulatory requirements create rising operational burdens. GRC platforms like Alyne⁷ harness the power of machine learning to automatically interpret your policies and operational documents into your own internal controls through intelligent control matching. Use sentiment analysis to monitor all communication to find those items where risk appears and immediate attention is required.



Mission: Taking “metrics” to the next level

Add quantification techniques to gain a true understanding of risk and compliance.

Enhance your risk insights.

Leverage quantitative techniques across your risk and compliance programs to gain actionable insights. Quantification techniques — including the adoption of FAIR methodologies and performing Monte Carlo simulations — can confirm risk assumptions and provide strong evidence to support key business decisions made by your board members.

⁷Mitratesh's Alyne

Conclusion

The convergence of regulatory changes, technological advancements, and heightened stakeholder awareness necessitates a proactive approach to IT risk management. By understanding the SEC's proposed amendments, anticipating board inquiries, and implementing powerful communication tools, your organization can not only navigate the current landscape but also thrive in the evolving world of IT risk technology.

Equip yourself with the knowledge and tools needed to confidently address your board's inquiries and stay ahead in the ever-changing realm of cybersecurity oversight. But most importantly, look for specific value drivers to find the right solution for your organization. Remember, GRC doesn't have to be hard! Learn more about Alyne and how it can ease your process by [requesting a demo](#) today.

Ready to empower your people, automate your processes, and elevate your results with Mitratesch's integrated Governance, Risk and Compliance (GRC) solutions?

Get in Touch ▶



About Mitratesch

Mitratesch is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across their organization.

With Mitratesch's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

Mitratesch serves over 10,000 organizations worldwide, spanning more than 160 countries.

For more info, visit: www.mitratesch.com

MITRATESCH

CONTACT US

info@mitratesch.com

www.mitratesch.com

Mitratesch US

+1 (512) 382.7322

Mitratesch EMEA

+44 (0) 1628.600.900

Mitratesch AUS

+61 (0) 3.9521.7077