WHITE PAPER

TECHNOLOGY RISK MANAGEMENT

A Proactive Framework for the Digital Age

PRESENTED BY

ITGRCForum
EMPOWERING THE GRC COMMUNITY

SPONSORED BY

riskonnect

TABLE OF CONTENTS

The Growing Frequency of IT Incidents 3

The True Cost of IT Incidents 4

Regulation is Driving Change 5

What do Regulators Expect? 5

Identify and Assess Risk 6

Mapping Operational Dependencies 6

Assessing Residual Risk 7

Mitigate and Monitor Risk 7

Continuous Risk Monitoring 8

Stress Testing 8

Detect and Respond 8

Incident Response 9

Business Continuity Planning 9

The Role of Industry Frameworks 9

Achieving Proactive TRM with Technology 10

Consolidate Your Risk 10

Quantify Your Risk 11

Monitor and Respond to Your Risk 11

The Role of TRM in Enterprise Risk Management (ERM) 12

Riskonnect | About the Authors 13

Technology now sits at the heart of modern business strategy, driving efficiency, innovation, and competitive advantage.[1] Organizations increasingly rely on a vast network of critical IT systems, both internally managed and externally sourced, to enhance operations and deliver value. Artificial intelligence (AI) is accelerating this transformation, with 72% of companies already adopting AI and 65% reporting regular use of generative AI.[2] The role of AI is set to grow further—92% of firms plan to increase their AI spending over the next three years.[3]

However, as businesses expand their digital footprint, they also expose themselves to greater risks. The convergence of cyber threats, operational vulnerabilities, AI-driven dependencies, and third-party risks has created a broader category: technology risk. These risks are not hypothetical—and their impact is increasing at an alarming rate.

The Growing Frequency of IT Incidents

- 87% of Fortune 1000 companies experienced a significant cyber incident at a third party in the past 12 months.[4]
- Between November 2022 and October 2023, over 30,000 cybercrime incidents were detected globally.[5]
  - Public Administration: 12,217 attacks
  - Finance: 3,348 attacks
  - Professional Services: 2,599 attacks
  - Manufacturing: 2,305 attacks
- The UK Cyber Security Breaches Survey 2024 found that larger organizations face a higher frequency of attacks (74% of large enterprises reported security breaches, compared to a 50% average across all businesses) due to the value of their data and the complexity of their IT ecosystems.[6]

Recent disruptions—including CrowdStrike and SWIFT outages in July 2024 and the Barclays outage in early 2025—highlight how technology incidents have become an ongoing reality. A 2025 PagerDuty survey found that 88% of executives expect another large-scale outage within the next year.[7] The question is no longer *whether* an incident will occur, but how prepared organizations are *when* it does.

These challenges require a broader approach to technology risk management (TRM)—one that extends beyond cybersecurity and data protection to encompass hardware failures, software malfunctions, network disruptions, and operational threats. Because technology underpins everything from physical assets to customer relationships, risk management can no longer be siloed; it must be cross-functional, proactive, and embedded directly within the business strategy.

This white paper explores why firms must adopt a more proactive and integrated technology risk management framework—driven by the financial and regulatory costs of incidents—and how technology can enhance visibility, enabling better risk management and stronger resilience outcomes.

[1] Cursor AI recently became the fastest-growing company in history, achieving an ARR of $100m in less than 12 months, with less than 20 employees.

[2] https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[3] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

[4] https://www.rsaconference.com/library/blog/rsac-esaf-cisos-transforming-third-party-risk

[5] https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/

[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#chapter-4-prevalence-and-impact-of-breaches-or-attacks

[7] https://www.pagerduty.com/resources/learn/execs-expecting-it-outages-2025/

The True Cost of IT Incidents

The impacts of IT incidents are profound; disrupting operations, eroding trust and causing financial damage that extends far beyond the initial breach:

- **Financial Losses**: The average cost of a data breach reached $4.88 million in 2024, reflecting a 20% increase since 2020.[8] These costs stem from regulatory fines, legal fees, and remediation efforts.

- **Stock Price Decline:** Publicly traded companies suffer an average 7.5% drop in share price following a cyber incident, as investors react to financial uncertainty and reputational damage.[9]

- **Customer Trust & Retention:** 55% of U.S. consumers report they would be less likely to continue business with a company that has experienced a breach, underscoring the long-term brand damage.[10]

- **Operational Downtime:** The 2024 cyberattack on Change Healthcare, which cost the broader UnitedHealth Group a total of $1.1 billion, disrupted payments across the U.S. healthcare system for weeks.[11]

These impacts serve as a reminder that technology risk is not an IT problem—it is an enterprise risk that requires executive oversight, structured risk management and cross-functional resilience strategies. Managing these risks demands a more sophisticated, integrated approach that accounts for the way technology risks interact and amplify one another.

[8] https://www.ibm.com/reports/data-breach

[9] https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

[10] https://www.cnbc.com/2022/05/21/americas-small-businesses-arent-ready-for-a-cyberattack.html

[11] https://securityaffairs.com/173467/data-breach/change-healthcare-data-breach-190m-people.html

Regulation is Driving Change

Regulators worldwide are tightening requirements across organizations for TRM, pushing them to take a more structured and proactive approach to safeguarding critical systems, data, and services. The growing reliance on technology has introduced new risks that regulators are addressing through expanded oversight and stricter reporting mandates.

The impact of these rules is multifaceted. Not only do they introduce more stringent requirements, but they also significantly broaden the scope compared to preexisting legislation, bringing more firms into the regulator's purview. Several major regulations[12] are redefining TRM parameters across industries:

- **DORA:** Applies to 22,000+ financial institutions and Information and Communication Technologies (ICT) providers in the EU, mandating a comprehensive operational resilience framework, including risk management, incident reporting, and third-party oversight.[13]
- **NIS2:** Expands regulatory coverage to an estimated 100,000–150,000 organizations across 18 critical sectors—including finance, energy, and healthcare—and introduces stricter cybersecurity obligations, including incident response, supply chain security, and board-level accountability for cyber risk governance.[14]
- **EU AI Act:** Affects all companies developing, deploying, or distributing AI in the EU and introduces risk-based AI governance, requiring transparency, security controls, and stricter oversight for high-risk AI systems.[15]
- **SEC Cyber Disclosures:** Applies to 4,000+ publicly traded U.S. companies and requires prompt disclosure of material cyber incidents and detailed cybersecurity risk management reporting in regulatory filings.[16]

What Do Regulators Expect?

Despite differences in scope and enforcement, regulators worldwide are aligned on key principles: enhancing transparency, strengthening governance, and ensuring organizations can prevent, withstand and recover from disruptions. These expectations span operational and technology risks—including the growing regulatory scrutiny on AI.

[12] *Note: this list is illustrative, not exhaustive. Other similar regulations and guidance exists elsewhere in the form of the FCA operational Resilience Act, APRA CPS230, and Singapore's Guiding Principles on Business Continuity*

[13] https://www.pwc.com.cy/en/audit-assurance/digital-operational-resilience-act.html

[14] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[15] https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[16] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules.html

Identify and Assess Risk

Firms must have a *"sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience."*[17]

Risk is to be assessed at both the product and service levels, focusing on services classified as *important* or *critical*—those whose disruption could result in severe consumer harm or systemic risk. DORA defines a critical or important function as one whose disruption, failure, or defective performance would materially affect a financial entity's ability to operate effectively. This includes impairing financial performance, service continuity, or compliance with regulatory obligations.

Regulators expect firms to have defined and documented all of their products and services, ahead of thorough risk assessments.

Mapping Operational Dependencies

Under DORA, firms are required to systematically map their operational dependencies, encompassing the people, processes, and technology ensuring a clear link between critical service delivery and the underlying infrastructure that supports it. The rise of technology- and AI-driven operating models means an increasing share of these dependencies are technological. This includes core IT infrastructure, cloud services and AI-enabled decision systems.

Under the EU AI Act, firms deploying AI models must explicitly link AI systems to the business services they support and classify them accordingly:

Risk Level	Examples	Requirements
Unacceptable Risk	Social scoring, subliminal manipulation, real-time biometric surveillance	Prohibited—No risk assessment required as these AI applications cannot be used in the EU.
High Risk	AI in credit scoring, fraud detection, hiring, biometric ID verification	Strictest regulatory requirements, including pre-deployment risk assessments, ongoing monitoring, and documentation.
Limited Risk	AI chatbots, automated customer support, recommendation engines	Transparency obligations, requiring clear user disclosures but no strict risk assessment.
Minimal Risk	AI for entertainment, gaming, productivity enhancement	No obligations, but firms may conduct voluntary assessments.

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Assessing Residual Risk

Regulators demand a risk-based approach to mitigation, meaning firms must prioritize control enhancements based on the materiality of risk rather than applying blanket measures. In-scope firms need to assess their residual risk exposure using an impact and likelihood assessment.

Both DORA and NIS2 emphasize a risk-based approach. However, when it comes to explicitly calculating residual risk, DORA is the more detailed of the two in outlining expectations. Article 6 requires firms to conduct periodic risk assessments, taking into account:

- The effectiveness of existing preventive, detective, and corrective controls
- The potential impact and likelihood of ICT-related incidents
- The residual risk that remains after controls are applied

Impact

Firms must identify vulnerabilities that could lead to systemic failures, regulatory breaches and consumer harm, including:

- Single points of failure within critical infrastructure.
- Over-reliance on a single third-party service provider.
- Technology and AI systems handling sensitive data.

Likelihood

Firms must assess the likelihood of risk materializing, ensuring their analysis accounts for both internal controls and external threat landscapes. Key considerations include:

- Effectiveness of preventive controls, such as cybersecurity frameworks, access management, and encryption
- Resilience of IT infrastructure, software, and outsourced services to withstand cyberattacks, outages, and operational disruptions
- External threat intelligence and emerging risks, including geopolitical, supply chain, and AI-driven vulnerabilities
- Incident detection, response, and recovery capabilities, ensuring alignment with regulatory expectations for operational resilience

Mitigate and Monitor Risk

All regulations related to TRM place ultimate accountability on senior management for the firm's risk framework. Structured, well-documented mitigation strategies serve to protect the firm and its management from severe consequences. Proactive mitigation strategies are supported by robust control measures:

- Preventive controls – designed to stop issues before they occur, such as access restrictions (NIS2), periodic risk monitoring (DORA), and AI model validation frameworks (EU AI Act).
- Corrective controls – mechanisms to remediate identified risks, including incident response plans (NIS2 and DORA) and model retraining processes (EU AI Act).

AI systems must meet standard operational resilience requirements while complying with additional governance obligations under the EU AI Act, particularly for high-risk applications. The extent of these requirements depends on a firm's role as a developer or deployer:

- **Developers** must manage risks across the AI lifecycle, conducting rigorous testing to mitigate foreseeable harm to safety, security, and fundamental rights. They must also implement robust data governance, ensuring training and validation datasets are representative, error-free, and managed to prevent bias. Additionally, comprehensive technical documentation should outline system design, data usage, cybersecurity measures, and risk controls, with post-market monitoring ensuring ongoing risk mitigation.
- **Deployers** must establish governance controls to ensure AI is used as intended, with human oversight mechanisms for intervention when necessary. They must also manage data inputs responsibly, ensuring they are relevant, representative, and appropriate for the system's intended use.

Continuous Risk Monitoring

Mitigation is only effective when paired with ongoing risk monitoring. Businesses need to monitor risk telemetry—ideally in real-time—as threats, vulnerabilities and data exposure are constantly evolving. Firms must establish mechanisms to monitor:

- **Operational risk indicators,** such as system uptime and failure rates
- **Cyber threat intelligence,** including external threat vectors, emerging vulnerabilities, and system intrusion attempts
- **AI performance metrics,** such as drift detection and assessments of bias and hallucinations, to ensure model outputs remain reliable over time

Stress Testing

Under DORA, financial entities are required to conduct real-world scenario testing—not just theoretical assessments. The focus shifts from whether a disruption could happen to how well the firm can function when it does. Instead of assuming defenses will hold, firms must simulate large-scale cyberattacks, AI system failures, or cloud outages and test their response under crisis conditions.

The shift from passive evaluation to active stress testing forces organizations to confront weak points in their business continuity, incident response, and resilience strategies. A stress test that exposes vulnerabilities should be viewed as an opportunity to address gaps before an actual disruption turns into a crisis.

Detect and Respond

Regulators expect firms to maintain robust frameworks for detecting, responding to, and recovering from incidents. These frameworks must not only ensure operational resilience but also align with strict reporting timelines, transparency obligations, and continuous improvement mandates.

Effective incident management consists of two key components:

- **Incident Response** – Detecting, containing, mitigating, and disclosing security incidents in a timely and structured manner
- **Business Continuity Planning** – Maintaining critical business functions and ensuring rapid recovery after a disruption

Incident Response

Firms must establish structured Incident Response Plans (IRPs) to minimize damage and notify affected parties. Regulators enforce proactivity through rapid and comprehensive reporting requirements:

- **NIS2 (Article 23):**
    - **Within 24 hours** – Initial notification to Computer Security Incident Response Teams (CSIRTs) and affected parties
    - **Within 72 hours** – Submission of a detailed incident report outlining impact, root cause, and immediate mitigation efforts
    - **Within one month** – Delivery of a comprehensive post-incident analysis, including long-term corrective actions
- **EU AI Act:** Deployers of high-risk AI systems must promptly disclose serious risks to providers, distributors, users, and regulators.
- **SEC Cyber Disclosures:** Public companies must report material cybersecurity incidents in an 8-K filing within four business days.

Proactive measures must be implemented to meet these requirements. This includes automated response mechanisms and efficient forensic investigation capabilities.

Business Continuity Planning

Regulators require firms to ensure operational resilience by maintaining business continuity in the face of cyber incidents, IT failures, and third-party disruptions. Business Continuity Planning (BCP) must include failover strategies, redundancy measures, and recovery processes, aligning with strict regulatory expectations. DORA's Article 11, for instance, provides direct guidance:

- Financial entities must develop and maintain comprehensive ICT business continuity plans to ensure availability, integrity, and recovery of critical functions.
- Plans must account for cyber incidents, third-party failures, and operational disruptions.

To meet these standards, firms must take a number of proactive steps, including the implementation of automated failover mechanisms, cloud-based disaster recovery solutions, ongoing resilience testing and third-party risk assessments.

The Role of Industry Frameworks

While regulatory mandates are increasing, some industries and jurisdictions still lack prescriptive cybersecurity requirements. In such cases, firms can look to establish best practices from regulated sectors or align with widely recognized industry frameworks, such as the NIST Cybersecurity Framework (CSF).

The NIST CSF is the preferred choice for many organizations due to its comprehensive, flexible, and risk-based approach. It provides a structured methodology, covering the full spectrum of cybersecurity through its six core functions:

- **Identify** – Map critical assets, data flows, and vulnerabilities.
- **Protect** – Implement security safeguards across internal systems and third-party dependencies.
- **Detect** – Monitor systems for suspicious activities using behavioral analytics.
- **Respond** – Contain, report, and mitigate cyber incidents efficiently.

- **Recover** – Restore operations while learning from incidents to improve resilience.
- **Govern** – Establish policies, roles, and accountability structures to ensure cybersecurity is embedded into organizational decision-making.

As regulations continue to evolve, firms that proactively align with advanced frameworks like NIST CSF will be better positioned to meet future compliance requirements while strengthening their current technology risk posture.

Important Note: While the NIST Cybersecurity Framework aligns closely with many regulatory requirements, it should not be seen as a one-size-fits-all solution. Organizations must remain vigilant, as compliance with NIST does not automatically guarantee regulatory compliance. Certain jurisdiction-specific mandates, particularly around reporting obligations, may require additional measures beyond the framework's scope.

Achieving Proactive TRM with Technology

Modern businesses operate in an environment where compliance is no longer enough—firms must actively anticipate, mitigate, and adapt to evolving technology risks. As regulators intensify oversight, technology landscapes grow more complex, and cyber threats scale exponentially, a reactive or checkbox-style approach to TRM is unsustainable.

A truly proactive approach to TRM is essential for:

- **Regulatory Resilience** – Meeting not only today's compliance mandates but also preparing for tomorrow's evolving expectations
- **Operational Efficiency** – Reducing the cost and complexity of risk management by replacing manual, fragmented processes with automated, scalable solutions
- **Reputational Protection** – Preventing breaches and failures that could erode customer trust, investor confidence, and market position

The sheer volume and velocity of technology exposure make manual approaches to proactive TRM infeasible. Legacy systems, disconnected data sources, and outdated methodologies leave businesses exposed not just to compliance failures, but to existential threats. True resilience demands a proactive, technology-enabled risk management strategy.

Here are three ways that technology can elevate your TRM approach:

Consolidate Your Risk

Traditional TRM approaches often suffer from fragmentation, where risks, assets and controls are tracked in isolation and manually mapped. This disconnect makes it difficult to see how different components interact and where vulnerabilities might emerge. Without a connected view, organizations risk blind spots, reactive decision-making and inconsistent risk management across teams.

A more effective strategy consolidates risk intelligence by dynamically mapping each component—assets → risks → controls → threats → services. By linking elements within a single, dynamic and visual repository, organizations gain a truly comprehensive view of their risk posture. Instead of managing cybersecurity, IT, and operational risks separately, firms can see how threats propagate across their environment, how vulnerabilities affect critical services, and whether controls are effectively mitigating risk.

This consolidated view fosters a shared understanding of risk by establishing a single source of truth.

Quantify Your Risk

Traditional TRM approaches were often reactive, assessing financial losses only after an incident had occurred. This left businesses without a clear, forward-looking understanding of the true financial impact of risk—and without the ability to prioritize mitigation efforts effectively.

A proactive approach changes this. Modern TRM strategies create visibility before an incident happens, and with the right specialist tools, firms can now quantify risk in financial terms rather than relying on generic scoring models. This enables data-driven, business-aligned decision-making that strengthens both compliance and resilience.

By integrating financial exposure into risk assessments, businesses can:

- Prioritize remediation efforts based on financial impact, ensuring resources are allocated to the most business-critical risks.
- Justify risk mitigation investments with clear financial reasoning, making it easier to secure budgets and drive proactive risk management.
- Translate technical risks into business terms, improving communication between risk teams, budget holders, and senior decision-makers.

Proactive risk quantification transforms risk management into a strategic enabler, aligning security investments with business priorities.

Monitor and Respond to Your Risk

Traditional approaches to risk monitoring have often been reactive, detecting and responding to threats only after they have escalated. This delay increases the likelihood of financial losses, regulatory breaches, and reputational damage.

A proactive approach is essential. Real-time monitoring and automated response mechanisms reduce risk exposure by identifying threats before they escalate, allowing organizations to act swiftly and decisively. By integrating advanced analytics, and automated workflows, firms can transform risk management from a reactive cost center into a strategic advantage:

- **Detect and contain threats faster** – Integrating real-time data feeds ensures continuous assessment of the evolving threat landscape, allowing firms to flag risks before they turn into incidents.
- **Streamline compliance and reporting** – Automated workflows ensure incidents are escalated to the right teams, triggering predefined response protocols and simplifying regulatory reporting.
- **Enhance cross-functional collaboration** – Siloed teams slow down containment efforts. A centralized TRM solution brings together InfoSec, IT, and data privacy teams to ensure full visibility and coordinated responses.
- **Prioritize incidents based on business impact** – Modern incident management tools track risks from detection to resolution, enabling firms to respond based on asset vulnerability, data sensitivity, and service criticality—minimizing disruption.

In high-stakes moments that would typically lead to chaos, panic, and human error, firms with a proactive, technology-enabled TRM framework can rely on automation, operational alignment, and seamless collaboration to respond swiftly and effectively—even with the speed and scale of modern threats.

The Role of TRM in Enterprise Risk Management (ERM)

Technology is a core enterprise risk that must be managed as part of an organization's broader risk strategy. As firms become increasingly dependent on AI, automation, cloud infrastructure, and digital services, technology-related risks now directly impact business continuity, financial stability, regulatory compliance, and competitive positioning.

Yet, many organizations still treat TRM as a separate discipline, distinct from ERM. This siloed approach is no longer viable. Technology risk is enterprise risk, and ERM frameworks must evolve to reflect that reality.

A modern ERM framework must account for technology risks as a fundamental component, not a peripheral concern. Without this integration, firms risk underestimating the business-wide impact of technology failures, cyber threats, and third-party digital dependencies.

Consider a cloud platform: It may simultaneously host sensitive customer data for compliance teams, process financial transactions for accounting, and power predictive analytics for marketing. If its security is compromised, the consequences extend beyond IT—they affect regulatory standing, financial performance, customer trust, and brand reputation. Evaluating such risks in isolation overlooks their enterprise-wide implications.

To ensure resilience, firms must:

- **Recognize technology as a core enterprise risk,** integrating TRM within the ERM framework.
- **Ensure technology risks are contextualized,** not compartmentalized, and cross-functional dependencies must be mapped, not ignored.
- **Balance technical expertise with business alignment,** ensuring risk decisions reflect broader strategic objectives.

The days of treating technology risk as a back-office IT issue are over. In a digital-first world, TRM must take its rightful place as a foundational element of ERM, ensuring that technology-related risks are managed with the same rigor as financial, operational, and strategic risks.

RISKONNECT

Riskonnect delivers an integrated, technology-driven approach to TRM, bringing all essential capabilities under one roof.

With Riskonnect, organizations gain a single source of truth for managing technology and operational risks, eliminating silos and ensuring risks are contextualized, prioritized, and proactively managed. By consolidating risk intelligence, quantifying financial exposure, and enabling real-time monitoring with automated response, Riskonnect empowers firms to make data-driven decisions, investing with confidence rather than intuition.

The risks are evolving—your approach should, too.

Find out more about Technology Risk Management at riskonnect.com

RISKONNECT INTEGRATED RISK MANAGEMENT SOLUTIONS

RISK MANAGEMENT INFORMATION SYSTEM

CLAIMS MANAGEMENT

BILLING

POLICY ADMINISTRATION

HEALTH & SAFETY

THIRD-PARTY RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

INTERNAL AUDIT

INTERNAL CONTROLS MANAGEMENT

POLICY MANAGEMENT

BUSINESS STRATEGY

COMPLIANCE

PROJECT RISK MANAGEMENT

TECHNOLOGY RISK MANAGEMENT

BUSINESS CONTINUITY & RESILIENCE

ENVIRONMENTAL, SOCIAL & GOVERNANCE

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

ABOUT THE AUTHORS

riskonnect

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia. To learn more, visit riskonnect.com.

PARKER & LAWRENCE
GROWTH ADVISORY

Parker & Lawrence Growth Advisory is a specialist research firm partnering with technology vendors in AI, risk and compliance to uncover industry insights, shape narratives and drive commercial success.