riskonnect

5 (Plus 1) Cyber Risk Management Strategies for Today’s Interconnected IT and Third-Party Ecosystem

Discover How GRC Leaders can Innovate, Compete, and Stay Resilient.

AI and digital technology are accelerating the speed and scale of cyber threats. Hackers are leveraging AI to launch more sophisticated attacks. Yet organizations must adopt AI, cloud, and other emerging technologies to compete, innovate, and streamline processes. The only way to move fast without encountering unnecessary risk is by uniting IT and third-party risk management through an integrated cyber risk program that provides deep insights into risk exposure.

As third-party related issues and breaches grow more frequent and costly, their overall impact on business operations and brand trust has become impossible to ignore. According to the Verizon 2025 Data Breach Investigations Report, 30% of data breaches involved a third party, up 15% from the previous year. Although the modern technology offered by third-party vendors provides businesses with a wealth of capabilities to streamline and automate processes, each vendor becomes a new attack vector and exposes businesses to new risks. These vulnerabilities do not stop at the vendor's network. Once connected, a third party's weaknesses can compromise internal IT systems, disrupt mission-critical services, and expose sensitive data.

Vendor technology issues often lead to operational failures, system downtime, compliance violations, data breaches, and reputational damage. To demonstrate resilience to the board, CISOs realize they can no longer manage third-party risk in isolation. Instead, they must manage it proactively, integrating it into their broader cybersecurity, IT risk management, GRC, and organizational resilience strategy to increase speed of innovation and reduce risk exposure.

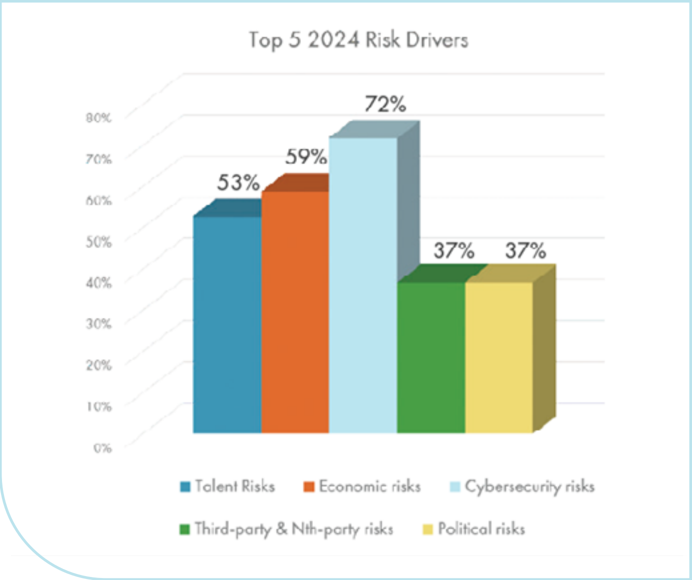
Third-party vendors are an integral part of an organization's ecosystem, and any failure can cause widespread consequences. As vendors become part of the extended enterprise, firms expect them to uphold the same standards in business continuity planning, regulatory compliance, certifications, incident response, and risk management. Therefore, it is easy to see why organizations increasingly view third-party risk management not as an isolated discipline but as an extension of their existing processes to protect themselves.

Third-party risk management is a strategic advantage when done well, empowering organizations to embrace new technology and smarter working methods. Innovative CISOs integrate IT and third-party risk management to enable rapid adoption of AI, cloud solutions, and third-party integrations. Rather than blocking innovation to avoid risk, strong cyber risk management practices allow leaders to confidently engage promising new partners, with the proper onboarding, expectations, and controls in place.

Third-Party Risk is an Enterprise-Wide Concern

Given the widespread use of third-party technologies, organizations should prioritize the security, compliance, and operational risks they introduce. However, only 8% of global risk management decision-makers selected third-party risk in their top 5 enterprise risk management concerns in the latest Forrester report, The State of Third-Party Risk Management, 2024.

At first glance, this appears to indicate low prioritization. However, many of the top risk areas cited, including data privacy, information security, emerging technology, regulatory compliance, business continuity, operational risk, and supply chain risk, are inherently linked to third-party relationships. The same applies to IT risks. When connected to an at-risk vendor, an internal system vulnerability becomes more dangerous, and vendor incidents can cascade into IT failures. Riskonnect's 2024 New Generation of Risk Report found that 72% of companies considered cybersecurity a top risk driver, while 37% cited third-party and Nth party risks as top priorities. Therefore, rather than viewing third-party and cyber risk as standalone categories, the survey results suggest that third-party and IT risk must be embedded in the broader enterprise risk program and managed holistically.



Regulations Require Greater Third-Party Risk Oversight

Reliance on third parties and the adoption of cloud, AI, and other digital systems continue to rise, and regulations are accelerating in line with this trend. Many widely adopted regulations—ISO 27001, NIST, NIS2, COBIT, HIPAA, DORA, SEC, the GDPR, and APRA CPS 230—include requirements for managing service provider risk. In addition to vendor oversight, these frameworks require rigorous oversight and continuous monitoring of internal IT assets, data systems, and configurations. Integrating IT risk controls with third-party oversight ensures consistent, complete compliance. It enables businesses to secure their infrastructure with the required security and privacy controls and demonstrate to regulators, auditors, and customers that their vendor network aligns with regulatory requirements.

CISO Accountability for Vendor-Related Incidents is Rising

CISOs are increasingly accountable for cyber breaches, operational failures, and compliance lapses relating to vendors and the IT environment that their vendors can access. This responsibility demands integrated governance and aligned controls across internal and third-party risk domains to provide CISOs with a consolidated view of risk and eliminate data silos. This heightened accountability has prompted CISOs to bolster vendor monitoring, enforce stricter onboarding standards, and expand oversight across the extended enterprise to safeguard the company, protect their professional reputation, and avoid financial penalties and board scrutiny.

5 (Plus 1) Strategies for CISOs to Manage IT and Third-Party Risk to Embrace New Technology with Confidence

1. Tie IT and Vendor Risk to Business Continuity and Incident Response Plans

Proactive CISOs understand that a breach, outage, or failure by a critical vendor can grind operations to a halt. Rather than treating vendor risk as a separate concern, you should integrate it directly into business continuity planning (BCP) and incident response playbooks. This approach helps ensure the organization can continue operating during vendor disruptions like IT issues, cyberattacks, compliance failures, or operational breakdowns. It protects the organization, avoiding costly business disruptions and downtime and preserving brand trust. Highlighting these benefits resonates at the board level, enabling CISOs to demonstrate why third-party risk is a core component of overall cyber resilience.

To integrate these processes successfully, your third-party risk management program must:

- Identify which third parties underpin core systems, processes, and regulatory obligations.
- Map vendor services to business-critical functions and the internal IT systems they connect to.

This mapping enables you to understand the potential impact if a critical vendor fails and allows you to focus on the vendors that matter most in your business continuity plans.

In addition, organizations should also:

- Plan scenario and vulnerability testing exercises that include internal IT system failures and third-party failures to ensure preparedness extends to critical third-party vendors.
- Establish backup vendors and contingency plans.
- Ensure vendor assessments cover business continuity, incident response, and recovery time objectives, and confirm vendors will meet SLAs and KPIs.
- Use AI-driven detection and automation to trigger containment steps across connected vendor integrations and internal assets during incidents.

As the number of third-party vendors you work with increases, so does the likelihood of vendor-related incidents and disruptions. To ensure timely and effective resolution, organizations must establish a clearly defined incident reporting process that captures third-party-related incidents, threats, and instances of underperformance. These plans should include escalation protocols, communication plans, and remediation procedures.

2. Use Risk Data and Vendor Due Diligence as a Catalyst for Digital Growth

Whether it is AI, new markets, or digital rollouts, proactive CISOs treat third-party risk as an input to innovation rather than an obstacle. In the Forrester report cited earlier, data shows that respondents who made the connection between increased levels of enterprise risk and increased reliance on third parties frequently describe risk management as an accelerator of innovation.

Strong third-party risk management enables CISOs to conduct due diligence quickly, allowing them to approve high-impact vendor partnerships without compromising security or compliance. Assess each vendor's security posture and consider whether your internal IT infrastructure can securely support the integration, so your systems don't become the weak link. This assurance is critical when adopting cutting-edge platforms or AI-powered tools. Use AI-assisted checks to flag access control gaps, misconfigurations, and dependency risks before vendors are onboarded.

To make fast, assured decisions, effective TPRM programs focus on a few critical actions:

- Performing rapid risk assessments tailored to the vendor's role and risk profile
- Leveraging AI and risk intelligence to flag issues relating to financial stability, compliance, or cybersecurity
- Ensuring clear expectations around SLAs, KPIs, and incident response

This strategic approach ensures that innovative vendors—especially smaller or more agile providers—can be onboarded without delay while maintaining resilience and compliance.

By embedding vendor due diligence steps and controls early in the selection process, CISOs can approve new vendors without compromising the organization's risk appetite. Third-party risk management should enable digital growth, empowering innovation teams to move faster with confidence.

3. Make Cyber and Vendor Risk a Board Priority

CISOs should elevate third-party risk to the boardroom by framing it in terms of operational resilience, reputational risk, regulatory exposure, and financial consequences. CISOs who articulate vendor risk by highlighting business impact and long-term resilience get buy-in faster and earn executive approval. There is also a risk in standing still. Boards must understand that avoiding new technology can create as much exposure as adopting it. This translation of risk data into meaningful metrics is essential for getting signoff for new strategic vendors and gaining executive support for stronger third-party risk management programs, ongoing investment, and cross-functional engagement.

When done well, third-party risk management becomes a powerful leadership tool that helps CISOs accelerate vendor onboarding and get approvals to implement new technology, enabling their organizations to stay ahead of the curve in an increasingly competitive market. To build a case for investment in integrated cyber risk management, present a combined view of vendor vulnerabilities and internal IT weaknesses, especially where they intersect. Use AI summaries to detect risk trends and present potential business impact to the board. CISOs who regularly raise vendor risk in board meetings and present meaningful metrics are more likely to secure risk resources and influence vendor selection decisions, helping their companies adopt new digital solutions that advance the organization's business model.

Board-level visibility of third and fourth-party risks limits surprises when incidents occur. Successful third-party risk management programs ensure leadership teams are already aligned on response protocols, escalation procedures, and the potential impact of a failed vendor, minimizing panic when vendor-related incidents do occur.

4. Connect Tools and Risk Data Across Teams

Less mature organizations often store third-party risk data across disparate systems and data sources. Different teams and departments and onboarding vendors without any central point of oversight, and the vetting process lacks consistency. In other cases, procurement has contracts, IT owns access management, compliance tracks certifications, and risk teams manage assessments. In a fragmented environment, teams often miss due diligence steps, overlook critical warning signs, and deliver disjointed response efforts. Disconnected data and tools limit visibility, impairing timely risk detection. This lack of oversight makes prioritizing mitigation or reporting accurately to the board harder for CISOs and weakens their ability to lead strategically.

Proactive CISOs recognize that a disjointed approach lacks consistency and oversight, and they use third-party oversight to break down walls. They centralize vendor data alongside IT asset inventories, vulnerability scans, and configuration management data in shared platforms or dashboards. They also implement consistent processes for onboarding, conducting risk assessments, benchmarking, performance scoring, and due diligence checks to avoid missing risk signals. Adopting a shared data model ensures risk scoring reflects real dependencies across vendors and IT systems. This unified approach provides a fair evaluation of vendors through cross-functional governance structures that automate data sharing between systems. It gives risk leaders a holistic view of vendor risk and dependencies, empowering them to prioritize mitigating the most critical risks while keeping the board informed.

Standardizing your risk framework, assessment templates, due diligence processes, onboarding, and offboarding makes vendors more comparable. This enables organizations to detect poorly performing, high-risk vendors with ease. Access to interconnected third-party risk management data empowers the board to make faster, more informed decisions when choosing new vendors and technology partners.

Industry leaders agree, according to OCEG, "CISOs are no longer just technical experts. They are boardroom voices guiding business strategy, and the GRC function is evolving right along with them". CISOs must work with GRC teams to use integrated risk data to present clear options and trade-offs to protect the organization from cyber and third-party risk.

5. Shift From Sporadic Risk Assessments to Continuous Monitoring

The strongest risk management programs incorporate real-time, continuous monitoring of third-party vendors and internal IT systems. Intelligent CISOs route vendor alerts and IT telemetry into one dashboard, and they use AI correlation to spot risk earlier so they can act before it escalates. A recent OCEG article stated that "Real-time risk intelligence is now expected. Whether it's continuous control monitoring, real-time vendor scoring, or predictive alerts about regulatory changes, organizations are expected to know that their risk controls are effective".

Initial assessments during onboarding and annual reviews are no longer sufficient to stay ahead of third-party risks. SecurityScorecard's 2023 breach research states that at least 29% of all breaches involved third-party attack vectors. Vendor risk evolves fast, and CISOs need near real-time visibility and continuous monitoring to stay ahead of emerging threats.

CISOs at the forefront use real-time data to track changes in vendor performance and consider their performance and impact on critical services. They subscribe to third-party risk intelligence providers to understand if suppliers are hitting the headlines because of financial instability, compliance violations, and ethical mishaps. They also perform regular risk assessments and conduct questionnaires monthly or quarterly to detect changes in circumstances that could pose a risk. Vendor-reliant processes can also be factored into regular business continuity plan updates and scenario and vulnerability testing, ensuring adequate contingency planning.

This continuous monitoring allows organizations to be more agile and proactive instead of waiting for a yearly review or a crisis before re-evaluating a vendor! With ongoing monitoring, regular assessments, and due diligence, CISOs can identify early warning signals and take preventive action. This integrated best-practice approach also supports more accurate risk scoring based on how each vendor connects to critical services, rather than treating all vendors equally. This ongoing stream of data relating to vendors and their performance enables businesses to make dynamic, responsive decisions on their choice of vendors and act quickly to avert vendor-related crises.

5 (Plus 1) Game-Changer: Leverage AI to Unite Cyber and Vendor Risk

AI is accelerating rapidly, and today's CISOs must look beyond the hype to harness AI's real, practical value. Whether you are managing third-party risk or monitoring internal IT systems and controls, AI can detect potential risks, failed controls, vulnerabilities, misconfigurations, and anomalous activity faster than manual reviews. By embedding AI into their processes, CISOs can eliminate time-consuming, repetitive tasks, spot risk signals earlier, and respond to emerging threats with greater agility. AI is critical in third-party risk management, where manually assessing hundreds - or even thousands - of vendors is no longer sustainable.

AI can streamline onboarding, automate due diligence checks, flag anomalies in vendor behavior, and even predict future risk based on historical patterns and external data. It enables CISOs to scale their oversight without increasing headcount and to move from reactive risk assessments to proactive risk detection.

OCEG says, "Generative and agentic AI can already auto-populate risk assessments, detect control redundancies, scan regulations, and even summarize weekly risk reports into executive insights. But while AI promises big gains in productivity, it also introduces new risks: hallucinations, bias, data privacy violations, and unclear ownership."

Because AI brings big opportunities and serious risks, CISOs should lead the conversation, not watch from the sidelines. Those who embrace AI responsibly, with strong governance and controls, will position their organizations to mitigate cyber and third-party risk more effectively and gain a competitive edge. AI is not just another tool, but a strategic advantage for those who use it wisely. Organizations should operationalize AI in areas like due diligence checks, continuous risk monitoring, incident response, and board reporting to produce insights highlighting issues across vendors and IT systems in real time.

Fuel Innovation and Resilience with Third-Party Risk Management

In today's connected environment, IT and third-party risks are two sides of the same coin. Proactive CISOs recognize that third-party vendors broaden the attack surface and manage them with the same rigor as internal processes. By embedding third-party risk management and AI into core areas like business continuity, digital transformation, executive decision-making, and daily risk management activities, CISOs turn vendor risk management into a vital source of intelligence that enables their organizations to adopt modern technology at pace.

The most forward-thinking CISOs are no longer content with reactive or disjointed approaches. They are shifting toward integrated, strategic supplier risk management programs that reduce risk and unlock opportunities to innovate and grow. The continuous monitoring and vetting in today's third-party risk management programs and the increased use of AI provide vital data to support decision-making, enabling a pre-emptive approach that addresses vendor risk before it becomes problematic.

Managing third-party and IT risk holistically drives resilience, agility, and long-term competitive advantage. Bringing vendor and IT risk together in one program lets leaders adopt AI-based technology and new partners at speed while protecting resilience, compliance, and trust. CISOs must move from a mindset of risk avoidance to one of confident, risk-informed innovation by using third-party risk data to identify issues and dependencies in their vendor ecosystem. Integrating IT and vendor risk ensures organizations can adopt new technology and service providers without compromising IT security or exceeding their risk appetite.

Discover how to successfully integrate IT and third-party risk management into one holistic platform with Riskonnect

Ready to see it in action?

REQUEST A DEMO

About 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 partner with Riskonnect 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-Pacific. To learn more, visit riskonnect.com.

CONNECT NOW →

Integrated Risk Management Solutions:

INSURABLE RISK

- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

BUSINESS CONTINUITY & RESILIENCE

- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

GOVERNANCE, RISK & COMPLIANCE

- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- IT Risk Management
- AI Governance
- Business Strategy