EBOOK

Technology Risk Management

DETECTION TO PROTECTION

riskonnect

Technology fuels nearly every aspect of business today. Accomplishing even the simplest tasks – for customers, employees, suppliers – usually requires technology.

The payoff has been enormous. Trading in paper for software has boosted efficiency, eliminated waste, and saved lots and lots of money. And generative AI is already delivering on its promise to supercharge that efficiency and layer on intelligence.

In this world, system availability is non-negotiable. Organizations simply cannot function without technology. And the responsibility for keeping all those systems – the very business itself – humming along falls squarely on the shoulders of CISOs, CIOs, CTOs, and other technology professionals.

That's a heavy burden to bear.

Every new piece of technology opens the organization up to more risk. The old way of inventorying risk, identifying anomalies, and patching vulnerabilities component by component is not enough anymore. There are too many technology assets, too many systems, too many business services, too many users, too many teams, too many controls, too many servers, too many devices, and too many regulations.

Meantime, cybercriminals are using all the same tech advances to launch ever-cleverer attacks aimed at taking down your systems, stealing your data, and generally wreaking havoc on the business. And your own people could inflict enormous damage, whether they mean to or not.

Risk detection is still important. But you need more to protect your business.

Boards and C-suites are taking notice and demanding that tech leaders accurately anticipate and manage risks and provide insight on the effectiveness of processes and controls. The business depends on it.

IT risk is no longer a technical cybersecurity issue – it's a business issue.

Technology risk management goes beyond IT risk detection and security to protection that encompasses resilience, business continuity, compliance, third-party risk management, and data privacy.

This ebook will help you move from simple risk detection to comprehensive protection by expanding your vision, capabilities, and influence.

TABLE OF CONTENTS

WHAT'S DRIVING THE CHANGE

Technology is at the heart of nearly every business, which makes organizations increasingly vulnerable to disruption from both external and internal forces. Can your systems, processes, assets, and people withstand the pressure?

EXTERNAL FORCES

New technologies. AI tools, big data, cloud technology, and automation are flooding the market, offering tantalizing possibilities to boost productivity. But every new technology introduces new risk.

More rules and regulations. Strict data privacy rules, mandatory cyber incident reporting requirements, and operational resilience requirements are increasing the compliance burden, as well as the consequences for failure. Regulators are now turning their sights on enforcing responsible AI use, led by the EU AI Act.

Booming cybercrime. Cyberattacks – ransomware, malware, phishing, etc. – are up sharply as criminals apply technology like generative AI to stay a step ahead of cybersecurity protocols and hack into your systems. More than three-quarters of organizations reported at least one ransomware attack in the past year – and more than a quarter of those were attacked at least four times.

Soaring costs. Cybercrime costs companies approximately $10.5 trillion annually. The global average cost of a data breach is currently estimated at $4.45 million. Ransomware demands average $2 million, plus another $2.75 million in clean-up costs. Average costs, however, don't paint the full picture. Change Healthcare, for instance, expects to rack up more than $2 billion in costs associated with its cyberattack.

GENERATIVE AI: A BOON OR A BUST?

AI brings in new threats like potential bias, hallucinations, and uncannily realistic phishing attacks. But it also promises to strengthen defenses. Generative AI tools can boost the capacity of IT teams overwhelmed by the ever-increasing number and complexity of cyberattacks. AI can also help with:

- Threat detection and analysis
- Incident reporting
- Adaptive controls
- Regulatory change

INTERNAL FORCES

Ubiquitous technology. The increasing reliance on technology to serve customers, engage workforces, optimize operations, and store data makes system availability essential. And PII, proprietary competitive strategy, and other stored sensitive data make for a tempting target for cybercriminals.

Inside threats. Employees, partners, contractors, and suppliers with system access can compromise security, whether unintentionally or maliciously. Internal threats can range from accidental data exposure from improper handling to deliberate data theft and extortion. Also, the pressure to implement new tech faster than the competition may lead some to cut corners on security governance – or sidestep the IT function altogether.

Demands for reassurance. Boards and the C-suite want proof that high-risk events, critical technology, security controls, and physical assets are being accurately assessed and appropriately managed. They are now looking at technology as a value creator instead of a cost center.

No boundaries. Security threats aren't confined within the four walls of the organization. Organizations rely on a multitude of partners, vendors, and other third-party suppliers to conduct business. Every one of those entities exposes you to security risks. And it's not just your immediate partners. Those four, five, or six degrees away can pose just as big of a threat.

Welcome to the New Era of the CISO

The role of chief information security officer began with the mission of protecting the confidentiality, integrity, and availability of the organization's information assets in a digital world. CISOs implemented security measures like firewalls, intrusion detection systems, and data encryption to ward off potential problems. The role eventually grew to include compliance with data privacy and other regulations.

Today's CISO still must do all of that – plus so much more.

As strategy, growth, and revenue increasingly depend on technology, CISOs are now confronted with an expanding list of expectations to protect the organization's prized technology assets and future aspirations from cyberthreats – and help it recover quickly from any disruptions that do occur.

The new CISO is expected to have a deep understanding of the organization's resilience for the full array of digital risks, not just security. They must develop and implement a comprehensive strategy to address cybersecurity, IT risk, resilience, business continuity, compliance, third-party risk, and more.

They also must create a consistent, compelling narrative, set priorities, and identify what concrete changes are necessary to IT, cyber, and AI risk practices. They must grasp what the board and C-suite expect and know how to succinctly explain complex regulations. And they need to understand how to translate technical information into a compelling story for leaders and frontline users across the organization.

This transformation is essential for organizations taking on the challenges of the digital age. While change of this magnitude is never easy, it also represents a new era of influence and reach for CISOs. They now hold the keys that will allow the organization to fearlessly unlock the power of new technology and innovation.

WHAT IS TECHNOLOGY RISK MANAGEMENT?

Technology risk management identifies, anticipates, and addresses the risks of technology failure to ensure smooth and uninterrupted operations. It goes beyond IT risk management and brings together the strategies, processes, systems, finances, and people to manage risks from cyberattacks, ransomware demands, data breaches, service outages, equipment breakdowns, human error, and more.

Protecting the company's digital assets against cyberthreats has long focused on intrusion detection systems, security information and event management systems, vulnerability scanners, and other tools. While those are still essential for identifying immediate threats, they are now just one piece of the broader IT risk management puzzle.

Technology risk is a moving target. Cyberthreats are growing in number and complexity as bad actors use increasingly sophisticated techniques. Even the most advanced cybersecurity measures cannot eliminate your risk.

If not properly managed, technology risks have the potential to seriously damage the business and its future viability. You need proactive, comprehensive, and structured risk management that coordinates across multiple stakeholders and departments.

Effective technology risk management will:

- Increase agility by establishing governance, standards, and practices.
- Reduce costs associated with a technology disruption.
- Eliminate time delays in the event of a cyber incident.
- Keep the organization compliant with changing regulations.

Technology risk is a moving target.

YOUR TECHNOLOGY RISK MANAGEMENT PLAYBOOK

Guarding against numerous, complex, and sophisticated cyberthreats takes more than cataloging threats and implementing cybersecurity measures for each tool. A formalized, comprehensive, holistic view of risk will help you bring on new technology and encourage innovation, while ensuring risks are identified and managed.

Here are seven steps to follow:

1. **Identify your technology assets and vendors**. Inventory all networks, devices, infrastructure, software, data, processes, and people – developers, users, tech staff – that operate that technology.

2. **Assess your risks.** Evaluate your digital infrastructure, systems, and processes, vulnerabilities and existing controls to determine the likelihood and potential impact of risks from both internal and external sources.

3. **Decide what risks to avoid completely.** Some risks are not worth the potential damage. Modify plans or processes to circumvent these risks.

4. **Decide what risks to mitigate.** Develop and implement strategies to reduce the likelihood and potential impact of risks through technical controls, robust policies, and proper procedures.

5. **Decide what risks to transfer.** This option shifts responsibility for the impact to another party, usually through insurance or outsourcing.

6. **Decide what risks to accept.** Some risk is necessary to embrace disruptive technology. Accept those risks when the cost of mitigation outweighs the benefits.

7. **Monitor results.** Reassess your risks and response plans and adjust your plans as necessary.

Myth: IT risk management is all I need.

Truth: Unless you have a comprehensive technology risk management strategy, you are vulnerable to risks that may not be immediately apparent but can have significant long-term effects.

Focusing solely on risk detection can lead to a false sense of security. Effective technology risk management ensures that risks are not only identified but assessed and managed in a structured and proactive manner that aligns with your organization's risk appetite and regulatory requirements.

To broaden your approach:

Conduct a risk management audit. Assess your existing risk management practices to identify gaps and areas for improvement.

Implement a comprehensive risk management framework. Consider adopting frameworks such as NIST RFM, ISO 31000, or COSO ERM to guide your risk management activities.

Prioritize regulatory compliance. Regularly review and update your practices to ensure compliance with relevant regulations and standards.

AUDIT

FRAMEWORK

COMPLIANCE

THE FOUR BIGGEST CHALLENGES FACING INFORMATION SECURITY PROFESSIONALS

SECURITY REVIEW

Companies that must maintain security certifications like SOC 1, SOC 2, and ISO 27001 are constantly under audit. And it can be an uphill battle if data must be pulled together from multiple systems and stakeholders – or if the culture doesn't prioritize or follow established security protocols.

COMPLIANCE

New regulations around data security, privacy, and breach notifications are always popping up around the world. It's difficult to maintain compliance without a comprehensive and adaptable system that streamlines the compliance process with automation and predictive analytics.

THIRD PARTIES

Keeping up with an ever-expanding list of suppliers and vendors is a huge challenge. And it's particularly difficult when important details like what information each supplier can access must be collected from numerous places by a team with limited bandwidth.

BOARD REPORTING

Information security professionals and board members speak in different languages. Technology risk is complex and technical, which doesn't always resonate with those in the upper echelon looking at the business from 30,000 feet. And translating tech-speak like cyber landscape, attack surface, or zero trust into the high-level business terms the board prefers may not come naturally to a CISO.

WHAT TO LOOK FOR IN TECHNOLOGY RISK MANAGEMENT SOFTWARE

You can't protect what you don't know about. Technology risk management software should eliminate blind spots and help you tamp down trouble before it materializes. And since no one has the capacity to spend a lot of time on set-up, it must be easy to use right out of the box.

Here's what to ask about software you are considering:

Does it do more than simply detect vulnerabilities? Detection is important, but what do you do if something happens? Look for software that provides a comprehensive process for managing assets, risks, threats, and vulnerabilities and clear remediation within the context of your business objectives and financial considerations.

Does it have automatic integrations? Security programs can be extremely complex and involve a surprising amount of manual work. Look for software that simplifies control monitoring, automates data collection and analysis, and provides a unified view of your security landscape.

How fast is the time to value? IT security professionals don't have the luxury of a prolonged implementation period. Look for software with minimal set-up time that can quickly plug into your existing security tools.

Will it help prioritize resources? Translating risks, threats, and vulnerabilities into financial terms to prioritize efforts can be tricky if you can only see one piece at a time. Look for software that quantifies financial risks and provides a comprehensive view of potential impacts, so you can prioritize high-risk areas and reduce the likelihood of costly incidents.

Does it provide a big-picture view of IT assets and risks? It's difficult to be proactive if most of your time is spent putting out fires. Look for software that provides an all-in-one view of key asset information like owner, business unit, and data classification, along with real-time insights, continuous monitoring of incidents, and automated recovery reporting to manage threats proactively.

Will it prove the value of your security investments? Controls are expensive, and the cost – in time and money – can be difficult to justify to a nontechnical audience. Look for software that can map assets to risks and controls, as well as regulatory standards and requirements, so you know where you get the biggest bang for your buck – and can provide hard evidence on the ROI.

GET READY FOR WHAT'S NEXT

Technology risks – IT, cyber, and AI – are often at the top of the risk register. And for good reason. These are the risks that have the potential to take the company down. Instantly.

There are no higher stakes than that. What worked in the past – detecting vulnerabilities to attacks and mishaps – is not enough to protect the organization in an environment changing as quickly as this one. Adding to the tension are all the powers of artificial intelligence, working both for and against you.

Managing technology risks today requires insight not just on IT risks and controls, but also on third-party risks, compliance, resilience, business continuity, and more. Are you getting quality information to manage those risks? Do you know how those risks link to business strategy? Can you prove it?

A technology risk management solution will help you move from simple risk detection to comprehensive protection. You'll not only know where your risks are, you'll know what they mean and what to do about them.

The board and C-suite will have concrete proof that money is well-spent, and the company is well-protected. The technology security team will finally have time to think about how to thwart new threats. And the company will be positioned to accelerate growth knowing that it can take on new technologies with confidence.

The more you can detect, the better you can protect. Surprises may still happen, but they won't happen as often or be as costly. Those bad actors looking to exploit a gap in your defenses will have to head on over to your competitors.

#DONTRISKIT

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.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

CONNECT NOW →

riskonnect.

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

Risk Management Information System

Claims Administration

Billing

Policy Administration

Third-Party Risk Management

Enterprise Risk Management

Environmental, Social, Governance

Business Continuity & Resilience

Internal Controls Management

Compliance

Internal Audit

Policy Management

Project Risk Management

Technology Risk Management

Active Risk Manager

Business Strategy

Health & Safety

Healthcare