Produced by the Cyber-resilience // Singapore Council

# // BUSINESS-TECHNOLOGY DIGITAL RISK MANAGEMENT PLAYBOOK

Published by: Spark

A.I. | Cyber-Resilience | Cloud Architecture | Digital Engineering | Sustainability Development | Board Leadership

WAHSPARK.COM

# Executive Summary

In today's rapidly evolving digital landscape, enterprises face an unprecedented array of digital risks that threaten their strategic objectives and operational resilience. Digital risk management has become a critical component for modern enterprises, requiring a cohesive integration of business and technology strategies to effectively mitigate threats and capitalize on opportunities.

Digital risk management encompasses the identification, assessment, and prioritization of risks arising from digital technologies and processes. It involves implementing strategies to manage these risks in alignment with the organisation's overall objectives. As enterprises increasingly rely on digital technologies, the scope of digital risks has expanded, encompassing cybersecurity threats, data privacy concerns, and technology disruptions.

The integration of business and technology is essential for effective risk management. This alignment ensures that risk management strategies are not only technically sound but also aligned with business goals. By bridging the gap between IT and business functions, organisations can foster a holistic approach to risk management, enhancing their ability to respond to threats and leverage technological advancements for competitive advantage.

Traditional compliance-based approaches to risk management are often insufficient in today's dynamic threat landscape. The rapid pace of technological change and the expanding attack surface introduce new vulnerabilities that compliance frameworks may not adequately address. organisations face challenges in keeping up with evolving regulations and ensuring that compliance efforts translate into effective risk mitigation.

In response to these challenges, organisations are increasingly adopting a risk-based approach to cyber-defence. This approach prioritizes risks based on their potential impact on business objectives, enabling organisations to allocate resources more effectively. By focusing on risk rather than compliance alone, enterprises can develop more agile and adaptive risk management strategies that are better suited to the complexities of the digital age.

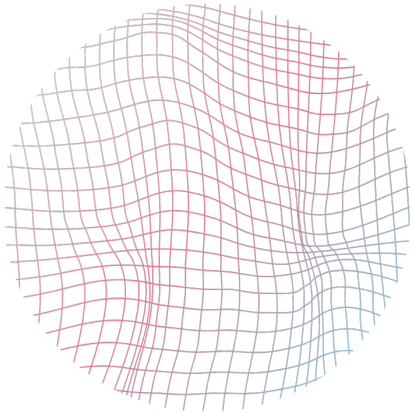
To successfully extend risk management decision models to business functions, cyber and IT teams must develop core competencies in several areas:

**Risk Quantification:** Utilizing frameworks like FAIR to quantify cyber risks in financial terms, facilitating better communication and decision-making.

**Collaborative Risk Management:** Engaging with business units to develop a common understanding of risks and foster a culture of shared responsibility.

**Empirical Risk Sharing Models:** Creating models that allow for empirical assessment and sharing of risks across the organisation, ensuring that all stakeholders are aligned in their risk management efforts.

This playbook aims to provide a comprehensive guide for enterprises to modernize their cyber-risk management strategies, leveraging practitioner-tested frameworks and fostering collaboration between business and technology teams. By adopting these strategies, organisations can enhance their resilience against digital threats and drive sustainable growth in the digital era.



01

# Building Trust-Based Communication: Transitioning from a Compliance-Based Model to a Dynamic, Risk-Based Approach

In the contemporary digital landscape, organisations face an ever-evolving array of cybersecurity threats. The traditional compliance-based model, which primarily focuses on adhering to predefined standards, often falls short in addressing the dynamic nature of these threats. Transitioning to a risk-based approach requires building trust-based communication channels that enhance cybersecurity integration across the organisation.

The drivers for robust risk management today are defined by two broad themes:

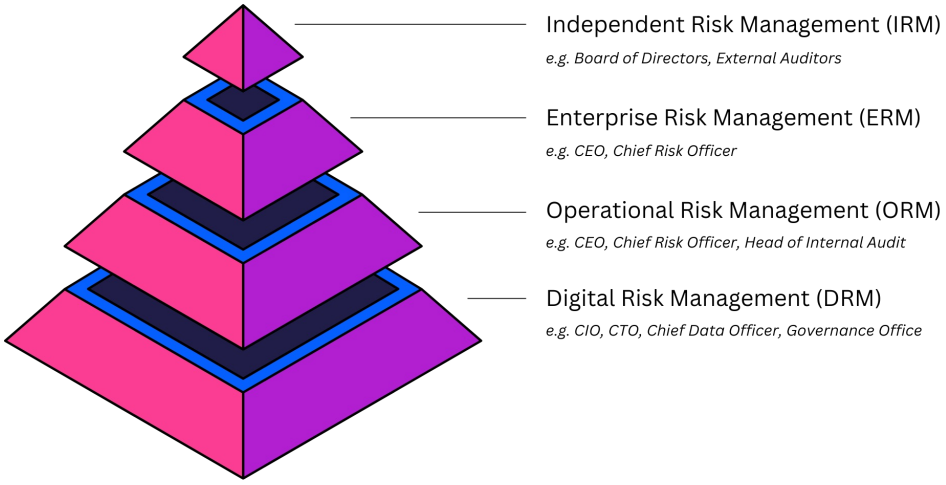
1. The **legal right** for an organisation to operate

This theme is much more pronounced in heavily regulated industries such as banking, pharmaceutical and medical industries as well as in power and utilities. Companies are required to adhere more strictly to regulations in order to obtain and retain their license to operate, leading to more rigorous risk management processes within the organisation.

2. The **ability** for an organisation to operate

Organisations also have to build resilience against internal and external disruptions, such as service downtime, data loss or theft, physical disruptions such as natural disasters or health crises, and system outages. As organisations become more connected, the digital elements of daily business operations have become mission-critical. Hence disruptions in digital services both from external threats like cyber-attacks, or internal errors such as a software patch gone wrong, are critical risk factors that organisations must seriously address today.

***The role of digital risk management within a typical corporate structure of risk management structures***



Where do digital leaders stand in the pecking order of risk managers in a typical organisation? For enterprises with a formal corporate board, the layers of risk managers in practice could look more like an onion. Right at the top, board directors, with the help of external auditors assess the risk independently from business operations. Enterprise risk management documents and translates the risk posture of the board into policies that reflect the risk parameters the organisation should operate within. The Chief Risk Officer tends to oversee a broad spectrum of risk vectors, including compliance and legal risks, financial risks, strategic risks and operational risks. Digital risks, or traditionally known in formal frameworks as information security risks, would typically come under the purview of the operational risk domain. Operational risks include risks arising from internal processes, systems, or external events that can disrupt daily operations, including supply chain disruptions or IT system failures.

**Seeing Eye to Eye with the Board**

What are corporate boards thinking about today in addressing growing digital risks, as part of the broader risk management strategy?

According to the EY Global Board Risk Survey 2021, nearly 8 in 10 board directors believe that better risk management will be crucial in enabling their organisations to protect and build value in the next five years. Even then, many board members lack confidence in their organisation's capabilities in managing risks. Just 18% of the survey respondents believe that their organisation's disaster response and contingency planning are highly effective, while only 13% believe that their organisation is highly effective in embedding risk and compliance activities.

While boards and management may regularly be monitoring and addressing traditional risks, such as regulatory changes, a drop in demand and increased borrowing costs, but they need to pay greater attention to atypical and emerging risks. Only 39% in the abovementioned survey say that their company can manage such risks effectively, which may include threats relating to new technology or climate risks.

Boards are emphasising the integration of digital risk management into overall corporate governance and decision-making processes. The rapidly changing threat landscape requires boards to adopt agile risk management practices. This includes the ability to quickly identify and respond to emerging risks, rather than relying solely on static, compliance-based approaches.

Boards have also prioritised establishing a common language for risk management is crucial for effective communication across the organisation. This involves creating a structured risk taxonomy and ensuring that all stakeholders, from front-line employees to executives, understand their roles in managing risks.

**Key drivers shaping today's dynamic digital risk landscape:**

1. **Rapid Advancements in Digital Technologies:** The proliferation of technologies such as clou, Internet of Things (IoT), and artificial intelligence (AI) has expanded the digital footprint of organisations. This expansion increases the potential attack surface, introducing new vulnerabilities that cybercriminals can exploit.

2. **Sophisticated Cyber Threats:** Cyber threats have become more sophisticated, with attackers employing advanced techniques such as ransomware, phishing, and zero-day exploits. These threats evolve rapidly, requiring organisations to adopt more agile and proactive risk management strategies.

3. **Regulatory Changes:** The regulatory landscape is continually evolving, with new data protection laws and cybersecurity regulations being introduced globally. organisations must adapt quickly to comply with these regulations, which can vary significantly across jurisdictions.

4. **Unprecedented Connectivity:** The rise of remote work and global supply chains has increased interconnectivity between organisations. This connectivity can lead to increased exposure to third-party risks, necessitating more comprehensive risk management approaches.

**Widening Gaps in today's compliance-based risk-management approaches**

1. **Lack of Agility to combat new threats and patch new vulnerabilities:** Compliance-based approaches often rely on predefined standards and checklists, which can be rigid and slow to adapt to new threats. In a dynamic environment, this lack of agility can leave organisations vulnerable to emerging risks that fall outside the scope of existing compliance frameworks.

2. **Regulation-Driven, Reactive Nature of compliance standards:** Traditional compliance approaches are typically reactive, focusing on meeting regulatory requirements rather than proactively identifying and mitigating risks. This can result in organisations being unprepared for unexpected threats.

3. **Time Gap and Limited Scope:** Compliance-based models may not cover all potential risks, particularly those related to new technologies and business models. This limited scope can lead to gaps in risk coverage, leaving organisations exposed to unanticipated vulnerabilities.

4. **Ineffective Communication:** Compliance approaches often focus on technical compliance rather than effective communication of risks to stakeholders. This can result in a lack of understanding and support for risk management initiatives across the organisation.

**How can organisations stay ahead of today's dynamic digital risk landscape?**

1. **Develop Open Communication Channels Between IT and Business Units:** Establishing open communication channels is crucial for aligning IT and business objectives. This involves creating regular forums for dialogue, such as cross-functional meetings and workshops, where IT and business leaders can discuss cybersecurity challenges and strategies. Utilizing collaborative platforms and setting up a joint risk assessment task-force, involving members of business units, IT and cybersecurity leads, to facilitate real-time information sharing can bridge the gap between technical and non-technical stakeholders, ensuring that cybersecurity measures are aligned with business goals.

2. **Foster a Culture of Transparency and Trust Within the Organisation:** Building a culture of transparency involves promoting open discussions about risks and encouraging employees to voice concerns without fear of retribution. This can be achieved by sharing success stories and lessons learned from past cybersecurity initiatives, demonstrating the value of proactive risk management. Trust is then further reinforced by involving employees at all levels in risk management processes, ensuring they understand their roles and responsibilities in maintaining cybersecurity.

   Using gamification techniques and reward mechanisms for employees who've identified and reported suspicious activity, has been found to be effective in decentralising cyber-defence efforts beyond the cyber team, by empowering every employee to stay vigilant against potential cyber-attacks. Gamified cybersecurity training has been shown to boost employee engagement by 60% and make 90% of employees feel more productive and involved1. In another study, 83% of participants felt more motivated with gamified training, and 87% reported increased productivity and engagement.

3. **Establish Clear Quantitative and Qualitative Measures to Identify and Assess Risks:** Frameworks like FAIR (Factor Analysis of Information Risk) provides a quantitative approach to risk assessment, translating cyber risks into financial terms that are understandable for business stakeholders. This facilitates informed decision-making and prioritizes risk management efforts.

**How is Risk measured in the FAIR Framework?**

Fundamental components to facilitate accurate risk identification and quantification. While there are several other risk computation variables in data inputs offered by the Open Risk Taxonomy, however, we will use a simplified version provided by the FAIR Framework for purposes of illustrating risk computations in business and financial terms.

In practice, risk managers may encounter challenges in data collection, from conflicting scan reports to poor data quality from historical logs. Hence, a delicate balance of operational data inputs and expert calibration, will improve the accuracy of risk scoring over-time.


The FAIR framework has defined specific inputs, to help risk managers derive a dollar value from known risk factors and chart a suitable course of action for risk-treatment. While not all are listed here, we've extracted the basic variable definitions for the purposes of a simple illustration.

**Table of Highlighted Risk Quantification Inputs**
*This table only highlights key input definitions for illustration purposes, please refer to the Open FAIR Framework documentation to review the full list of definitions.*

| | |
|---|---|
| **Loss Event Frequency (LEF)** | LEF is the probable frequency, within a given timeframe, that loss will materialize from a threat agent's action. It is a measure of how often loss is likely to happen |
| **Threat Event Frequency (TEF)** | TEF is the probable frequency, within a given timeframe, that threat agents will act in a manner that may result in loss. |
| **Vulnerability** | Vulnerability in is defined as the probability that a threat agent's actions will result in loss. It is expressed as a percentage and can be estimated directly or derived from Threat Capability (TCap) and Difficulty (Diff).<br>• Threat Capability (TCap): The capability of a threat agent, measured on a percentile scale representing the range of capabilities within a threat community.<br>• Difficulty (Diff): The level of effort required to overcome controls or defences. |
| **Secondary Risk** | Secondary Risk represents the primary stakeholder's loss exposure due to potential secondary stakeholder reactions to the primary event. I |
| **Loss Magnitude (LM)** | LM is the probable magnitude of primary and secondary loss resulting from an event. It is divided into two components:<br>• Primary Loss Magnitude (PLM): Direct loss to the primary stakeholder resulting from an event.<br>• Secondary Loss Magnitude (SLM): Loss associated with secondary stakeholder reactions to the primary event. |

To put these risk calculations into context, here is a sample (and oversimplied) fictitious case to help you visualise the risk computations needed to produce sensible dollar-risk-values for risk prioritisation purposes.

**Background:**
TechSecure Inc. is a technology company that stores sensitive customer data, including personal and financial information. The company is evaluating the risk of a cyber attack that could lead to a data breach.

**Loss Event Frequency (LEF)**
LEF is the probable frequency that a loss will occur due to a threat agent's action. For TechSecure Inc., this involves assessing how often a cyber-attack might result in a data breach.

- **Threat Event Frequency (TEF):** TechSecure estimates that cyber criminals attempt to breach their systems approximately 10 times per year. This is based on historical data and industry trends.
- **Vulnerability:** The probability that a cyber attack will succeed is estimated at 20%, considering the current security measures in place, such as firewalls and intrusion detection systems.

Using these factors, TechSecure calculates the LEF as follows:
LEF = TEF × Vulnerability = 10 × 0.2 = 2
This means TechSecure expects approximately 2 successful data breaches per year.

Loss Magnitude (LM) is the probable magnitude of loss resulting from a loss event. It includes both primary and secondary losses.

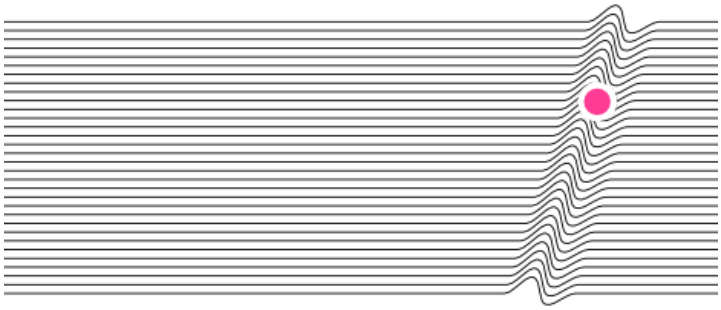
- **Primary Loss Magnitude (PLM):** Direct costs include incident response, legal fees, and customer notification. TechSecure estimates these costs at $500,000 per breach.
- **Secondary Loss Magnitude (SLM):** Indirect costs such as reputational damage, loss of customers, and regulatory fines. These are estimated at $1,000,000 per breach.

**Calculating Risk**

The overall risk to TechSecure Inc. is calculated by combining LEF and LM. With an LEF of 2 breaches per year and a total LM of $1,500,000 per breach (PLM + SLM), the annualized risk exposure is:

Annualized Risk = LEF × LM = 2 × $1,500,000 = $3,000,000
This indicates TechSecure Inc. faces an annual risk exposure of $3,000,000 due to potential data breaches.

To read more about the FAIR framework, visit: www.opengroup.org/open-fair



## 4. Comparing Design of Popular Risk Management Frameworks

The NIST (National Institute of Standards and Technology) and ISO (International organisation for Standardization) frameworks offer comprehensive guidelines for qualitative risk assessment, helping organisations to systematically identify and evaluate potential threats.

| Framework | **FAIR**<br>*Factor Analysis of Information Risk* | **NIST CSF**<br>*NIST Cybersecurity Framework* | **ISO 31000:2018 Standard** |
|---|---|---|---|
| **Purpose:** | Focused on providing a quantitative model for understanding, analyzing, and quantifying information risk in financial terms. | Provides a policy framework of computer security guidance for how private sector organisations in the US can assess and improve their ability to prevent, detect, and respond to cyber attacks. | The purpose of ISO 31000 is to provide guidelines on managing risk faced by organisations. It aims to integrate risk management into all aspects of an organisation, ensuring that it is a fundamental part of governance, strategy, and decision-making processes. |
| **Structure:** | Breaks down risk into quantifiable components, such as Threat Event Frequency and Vulnerability, to provide a clear, measurable understanding of risk. | Organized into five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk. | Structured around principles, and a process for managing risk. It emphasizes integration, structured and comprehensive approaches, customization, inclusivity, dynamism, and continual improvement. |
| **Approach:** | More quantitative, providing a method for translating cyber risks into financial terms, which aids in prioritizing risks and making informed decisions about resource allocation. | More qualitative, focusing on best practices and guidelines to help organisations build a comprehensive cybersecurity program. It emphasizes flexibility and is designed to be adaptable to various types of organisations and industries. | Adopts a qualitative approach to risk management, focusing on principles and guidelines that can be adapted to any organisation and context. It emphasizes the importance of a comprehensive and integrated risk management process that includes risk identification, analysis, evaluation, treatment, monitoring, and review. |

Each framework offers unique strengths, and their integration can provide a robust foundation for dynamic risk-based cybersecurity management. By leveraging the quantitative insights of FAIR, the comprehensive guidelines of NIST, and the structured approach of ISO, organisations can build a cohesive risk management strategy that enhances cybersecurity integration and aligns with business goals.

Transitioning to a dynamic risk-based approach requires building trust-based communication channels that foster collaboration between IT and business units. By adopting practitioner-tested frameworks and fostering a culture of transparency, organisations can enhance their cybersecurity posture and effectively manage the complexities of the modern threat landscape.

# 02

# Operationalising a Shared Responsibility Model in IT-Business Risk Management

To lead risk-sharing initiatives and build organisational competencies to effectively deal with digital risks today, involves creating a collaborative framework where both IT and business units share ownership of risk management. The objective is to encourage shared responsibility through joint risk management ownership.

The primary objective is to foster a culture of shared responsibility in risk management across IT and business units. This involves:

- Encouraging joint ownership of risk management processes.
- Enhancing communication and collaboration between IT and business units.
- Ensuring all stakeholders understand their roles in managing risks.

**1. Define Roles, Responsibilities and a Common Risk Taxonomy Across Departments**

- **Importance:** Clearly defining roles and responsibilities is crucial to avoid confusion and ensure accountability. According to a study by Oracle and KPMG, confusion about responsibilities in shared models can lead to misconfigurations, resulting in data loss and other security issues.
- **Implementation:** The 3 lines of defence model proves to be effective in delineating policy, governance, oversight and operational duties to implement effective risk controls.
- **Taxonomy Reference:** The Open Risk Taxonomy, developed by the Open Group, provides a comprehensive, quantitative and qualitative risk assessment model that effectively contextualises digital risks in business terms.

| | 1st line of defence<br>**IT Operations & Dev Teams** | 2nd line of defence<br>**Policy & Governance Teams** | 3rd line of defence<br>**Internal & External Audit** |
|---|---|---|---|
| **Description** | It is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving their objectives in technology domains (Application and Infrastructure operations), | It provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line, conducts monitoring, | It is provided by internal audit. sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines of are operating effectively and advise how they could be improved. |
| **Controls/Policy Examples** | Firewalls, encryption, and access controls to mitigate risks like data breaches, system outages, and unauthorized access | GDPR, Data protection policies, Information security risk treatment and controls | |

As outlined by the Open Group, the objective of the Risk Taxonomy (O-RT) Standard is to provide a single logical and rational taxonomical framework for anyone who needs to understand and/or analyse information security risk.

What O-RT define as assets, in context, it can apply to an application, a database, a live business process, or a production environment.

To assess the potential magnitude of loss from asset loss, the Open Group has identified 3 broad categories:

- **Criticality** – characteristics of an Asset that have to do with the impact on an organisation's productivity; for example, the impact a corrupted database would have on the organisation's ability to generate revenue
- **Cost** – the intrinsic value of the Asset; e.g., the cost associated with replacing it if it has been made unavailable (e.g., stolen, destroyed); for example, the cost of replacing a stolen laptop or rebuilding a bombed-out building
- **Sensitivity** – the harm that can occur from unintended disclosure

Sensitivity is further broken down into four sub-categories:

- **Embarrassment/Reputation** – the information provides evidence of incompetent, criminal, or unethical management and refers to reputation damage resulting from the nature of the information itself, as opposed to reputation damage that may result when a Loss Event takes place
- **Competitive Advantage** – the information provides competitive advantage (e.g., key strategies, trade secrets) and, of the sensitivity categories, this is the only one where the sensitivity represents value; in all other cases, sensitivity represents liability
- **Legal/Regulatory** – the organisation is bound by law or contract to protect the information
- **General** – sensitive information that does not fall into any of the above categories but would result in some form of loss if disclosed

O-RT has also outlined key actions that Cyber-attackers can take, to gain access to, steal, or disrupt the operations of business assets. Which, once mapped, will provide a guide for cyber investments to protect assets in context of the broader threat landscape.

Threat Agents can take one or more of the following actions against an Asset. The :

- **Access** – unauthorized access of Asset(s)
- **Misuse** – unauthorized use of Asset(s)
- **Disclose** – illicit disclosure of sensitive information
- **Modify** – unauthorized changes to Asset(s)
- **Deny Access** – prevention or denial of authorized access

What makes it challenging for cybersecurity leaders to confidently quantify and define risk with the business, is that the criticality, sensitivity and cost of assets are changing dynamically. Defending against cyber-attackers has grown in complexity, especially with new tactics such as social engineering and stealthy injection used as part of sophisticated advanced persistent campaigns. Due to the stealthy way that attackers operate, seemingly benign and low-risk assets, are used to gain access to higher value assets, and these malicious injections could last in IT systems in years, even infecting critical back-ups.

Mapping the attack surface and assigning risk scores to assets will have to be done in a threat-informed approach, where cyber teams consider past (and more actively used) TTPs, pay attention to attack signatures, and assign threat-weighted scores to be applied in asset-risk scores. While this can be extremely arbitrary when translated into probabilities computations, cyber companies have started developing and deploying A.I. models to keep up with today's growing number and sophistication of cyber-threats.

Where cyber and IT teams would encounter challenges, is in contextualising, and most times, quantifying accurately, the potential impact created by successful breaches in business-critical assets. O-RT has categorised these variables as Asset Loss Factors.

**2. Implement Joint Risk Management Teams**

i. **Challenge**: Overcoming organisational silos between cyber, IT and corporate business units in harmonising risk taxonomies and business processes

ii. **Composition**: Form cross-functional teams comprising members from IT, security, and business units. This approach ensures diverse perspectives and expertise in risk management.

iii. **Benefits**: According to PwC, having a dedicated risk management team that regularly updates the board increases confidence in identifying new types of risks by 57%.

**3. Lead Effective Cross-Functional Meetings**

i. **Purpose**: Regular meetings facilitate communication and alignment on risk management priorities and strategies.

ii. **Best Practices**: Use structured agendas, encourage open dialogue, and ensure that all voices are heard. Meetings should focus on identifying risks, discussing mitigation strategies, and reviewing progress

iii. **Leverage Technology and Tools**: Utilize risk management applications to automate and streamline processes. Technology can enhance the consistency and effectiveness of risk management initiatives. More on this topic will be covered in the next segment.

iv. **Foster a Risk-Aware Culture**: Encourage a culture where risk management is viewed as a shared responsibility. Training and regular communication are key to embedding this culture throughout the organisation

**4. Selecting appropriate risk treatment options – understanding your levers in context**

Selecting the most appropriate risk treatment options is recommended to be done in deliberation of financial costs involved, human resources and time committed, vis-a-vis measurable intended outcomes from risk mitigation activities

As recommended by ISO 31000, Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

- Taking or increasing the risk in order to pursue an opportunity;

- Removing the risk source;

- Changing the likelihood;

- Changing the consequences;

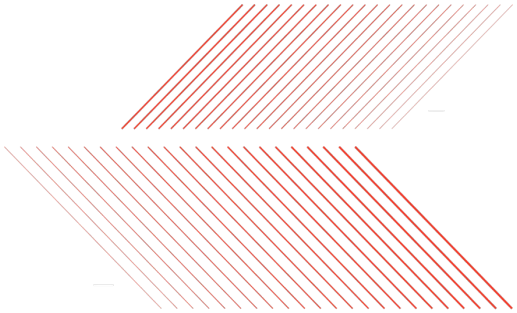
- Sharing the risk (e.g. through contracts, buying insurance);

- Retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and should take into account all of the organisation's obligations, voluntary commitments and stakeholder views.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Lastly, risk treatment can also introduce new risks that need to be managed.



# 03

# Critical Components & Challenges in **Integrated Digital Risk Management Operations**

**Challenges abound in Implementing the 6 Critical Steps to Comprehensive Digital Risk Management**

Comprehensive Digital Risk Management includes 6 critical components, digital leaders today face a myriad of challenges when operationalising tech risk management controls and policies.

1. **Third Party Technology Vendor Management:** Establish clear contracts with vendors that include specific security requirements and performance metrics to ensure accountability. As part of annual service-level reviews, regular due diligence checks and continuous monitoring of third-party vendors are needed to assess their risk posture and compliance with security standards.

*Potential Challenges*

- **Lack of Visibility**: organisations often struggle with gaining a clear understanding of third-party vendors' policies, procedures, and controls, which can lead to increased risk exposure.
- **Vendor Due Diligence:** Conducting thorough due diligence and risk tiering can be resource-intensive and complex, especially when dealing with a large number of vendors.
- **Continuous Monitoring:** Implementing effective continuous monitoring controls to detect and respond to emerging threats from vendors can be challenging as well, considering enterprises may have legacy versions of proprietary software, or use open source code and software tools.

2. **Technology Issue Remediation:** Implement structured root cause analysis and allocate sufficient resources for comprehensive testing and timely remediation of technology issues.

*Potential Challenges*

- **Incomplete Testing and Remediation**: Often, the need for complete testing and remediation is overlooked out of convenience and speed-to-market delivery concerns, leading to unresolved vulnerabilities and potential liabilities.
- **Resource Constraints:** Limited resources can hinder timely and effective remediation of technology issues, particularly in smaller organisations.

3. **Technology & Security Exceptions Management:** Develop a clear framework for exception handling, including approval criteria and regular reviews to assess risk impact of new and existing tech risk exceptions.

*Potential Challenges*

- **Risk Accountability:** There can be a lack of clarity regarding who is responsible for managing and mitigating risks associated with exceptions, leading to accountability issues and a pile-up of risk-exceptions backlog that could give rise to critical unaccounted vulnerabilities.
- **Compliance Challenges:** Navigating complex regulatory requirements and ensuring compliance during exceptions management can be daunting.

4. **Vulnerability Management:** Use continuous scanning and risk-based prioritization to quickly identify and address critical vulnerabilities with effective patch management.

*Potential Challenges*

- **Inadequate Risk Assessment:** Many organisations struggle with conducting thorough risk assessments, leading to incorrect prioritization and unaddressed critical vulnerabilities.
- **Patch Management Difficulties:** Timely deployment of patches is often challenging, resulting in prolonged exposure to known vulnerabilities.

5. **IT Asset Management:** Maintain an accurate inventory of IT assets and implement lifecycle management to ensure timely updates and reduce security risks.

*Potential Challenges*

- **Lifecycle Management:** Managing the entire lifecycle of IT assets, from acquisition to disposal, to minimize risks related to outdated or unsupported technology.
- **Ongoing Shadow IT:** Non IT teams may be creating unmanaged assets that IT departments lack visibility on, leading to security vulnerabilities and compliance issues due to unauthorized software and hardware use
- **Asset categorisation:** Companies may have accumulated a significant backlog of decommission assets or immaterial assets that pose little risks to the organisation that cannot be identified and isolated.

6. **Tech Policy Management:** Develop comprehensive IT policies with stakeholder engagement, ensuring consistent enforcement and alignment with business objectives and compliance requirements.

*Potential Challenges*

- **Policy Implementation:** Ensuring consistent implementation of security policies across the organisation can prove challenging, especially with the rise of remote work, Bring-Your-Own-Device and risky employee behaviours such as pasting post-it notes of passwords on their devices or at their desks.
- **Change Management:** Adapting policies to keep pace with rapid technological changes and emerging threats requires continuous effort and resources.

# 04

# **Modernising the Digital Risk Management** Toolkit with A.I., for the New A.I. World

In the new AI-driven world, modernizing the Digital Risk Management Toolkit with Artificial Intelligence (AI) is essential for cybersecurity leaders and risk managers. As organisations increasingly adopt AI technologies, they encounter new attack surfaces and heightened digital and IT risks. Leveraging AI in cybersecurity offers significant advantages in managing these challenges.

**Mapping the ever-evolving risk landscape with dat—driven intelligence**

AI empowers organisations to process vast amounts of data swiftly, providing critical insights into potential threats and vulnerabilities. By automating threat detection and response, AI reduces reliance on human intervention, enabling faster and more precise risk identification. This automation is crucial for handling the complexity and volume of data in modern digital environments.

To effectively manage unknown risk factors, risk frameworks must be **adaptive and dynamic**. This involves integrating AI to continuously monitor and assess the risk landscape, allowing for rapid adjustments to risk management strategies. AI's predictive capabilities can help foresee potential threats, enabling proactive measures rather than reactive response.

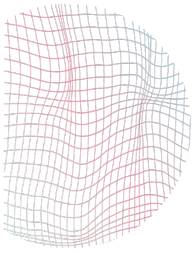
| Compliance-based **Static Risk Management** | | **A.I.-Enabled Dynamic Risk Management** |
|---|---|---|
| **Periodic Assessments** Risk assessments are conducted at set intervals, which may not capture emerging threats in a timely manner. This can leave organisations vulnerable to rapidly evolving cyber threats. | ▶ | **Real-Time Data Processing** AI systems can analyse vast datasets in real-time, providing immediate insights into potential risks. This capability allows for the swift identification of threats and vulnerabilities, enabling proactive measures to mitigate risks. |
| **Manual Processes** Static frameworks often depend on manual processes for threat detection and response, which can be slower and more prone to human error compared to automated systems. | ▶ | **Predictive Analytics** AI algorithms can predict potential risks by identifying patterns and trends in historical data. This predictive capability helps organisations anticipate and prepare for future threats, enhancing their resilience against cyberattacks. |
| **Limited Predictive Capabilities** Without the use of AI, static frameworks lack the predictive analytics needed to anticipate future threats, relying instead on historical data and trends. | ▶ | **Automated Response** AI can automate threat detection and response processes, reducing the reliance on human intervention. This automation accelerates incident response times, minimizing the impact of cyber threats. |
| **Inflexibility** Static frameworks are less capable of adapting to new technologies and threat landscapes, which can hinder an organisation's ability to manage emerging risks effectively. | ▶ | **Continuous Learning and Adaptation** AI systems can learn from new data and evolving threat landscapes, continuously updating their risk management strategies. This adaptability ensures that organisations remain prepared for both known and unknown risks. |

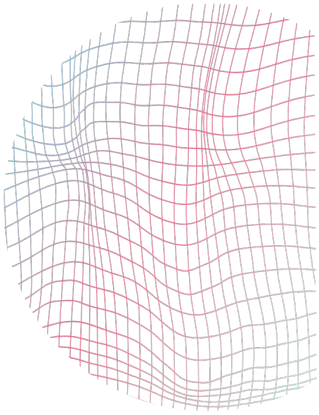
# Concluding Remarks

he Digital Risk Management Playbook underscores the urgent need for a transformative approach to risk management in the digital era. As digital technologies rapidly evolve, they expand the attack surface, introducing sophisticated cyber threats and regulatory complexities. Traditional compliance-based models, often reactive and rigid, are inadequate in addressing these dynamic challenges. The playbook advocates for a shift towards a risk-based approach, emphasizing agility, proactive risk identification, and the integration of business and technology strategies.

Key findings highlight the importance of fostering collaborative risk management across IT and business units, utilizing frameworks like FAIR for quantifying risks in financial terms, and building a culture of transparency and shared responsibility. The role of digital risk management is increasingly pivotal within corporate structures, requiring boards to adopt agile practices and establish a common risk language.

Looking forward, organizations must embrace AI-driven solutions to enhance real-time threat detection and response capabilities. By leveraging AI's predictive analytics, enterprises can anticipate and mitigate future risks, ensuring resilience and sustainable growth. This evolution in risk management is not merely a strategic necessity but a fundamental shift towards safeguarding organizational value in an interconnected world.





Spark

## Get in Touch

Laura Flores
Content Strategy
**laura@wahspark,com**

David Chin
CEO, SPARK
**david@wahspark,com**


wahspark.com