TANIUM

WHITEPAPER

Enhancing Cybersecurity Governance: Leveraging Data-Driven Insights Across the Three Lines Model

CONTENTS

Introduction

In the high-stakes world of corporate risk management, cyber threats are as complex as they are relentless. Amidst this complex web of cyber threats, the Three Lines Model offers a beacon of clarity and structured defense, positioning it as a critical ally in cybersecurity risk management.

For over two decades, the Three Lines Model — a risk management framework delineating roles and responsibilities across operational management, risk and compliance functions, and internal audit — has been the cornerstone of risk governance, proving its worth beyond the financial sector that first adopted it.

The Three Lines Model's strength lies in its simplicity: a well-defined risk appetite, clear accountability, and a synergy of risk management and compliance systems.

This white paper is an invitation to reimagine the Three Lines Model's application in an area that remains largely unchartered: cybersecurity risk management. The Three Lines Model is a powerful tool for leveraging trusted, shared data to:

- Make smarter decisions about risk
- Articulate and identify cybersecurity, risk, compliance and governance responsibilities more effectively
- Support risk management, compliance systems and reporting.

Read on to explore how the Three Lines Model enhances cybersecurity governance while fostering an agile, responsive risk management culture capable of addressing dynamic cyber threats.

What is the Three lines Model?

As defined by the Institute of Internal Auditors, the Three Lines Model "*helps organisations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management*."[1]

Known as the Three Lines of Defense Model until 2020, the benefits of adopting a Three Lines Model include:

- Customisable: The Three Lines Model thrives on principles, not rigid rules. It can be moulded to an organisation's goals and changing business landscape.
- Value creation, not just protection: The Three Lines Model shifts the narrative from risk avoidance to strategic enablement, so risk management can be integrated into growth plans.
- Provides clarity in complexity: Defined roles and responsibilities cut through ambiguity. They provide an understanding of how each line of defence fortifies an organisation against threats.
- Aligned for impact: The Three Lines Model moves towards common goals, ensuring decisions align with stakeholder interests.

The Three Lines Model requires maturity and sophistication to fully harness its power. It's a powerful foundation for setting strategic goals and navigating risk and compliance with confidence.

Cybersecurity: A unique operational risk

Within the context of the Three Lines Model, a risk appetite statement articulates the amount and type of risk an organisation is willing to accept to achieve its strategic objectives and business plan. It serves to balance bold moves with prudent oversight.

A comprehensive risk appetite statement delves into the spectrum of risks that could impact an organisation. These include:

- Financial risks: liquidity, credit and market risks.
- Operational risks: legal, regulatory, compliance, conduct, technology, data and change management dangers.

While cybersecurity risk falls within the scope of operational risk, it is unique because it has cross-cutting implications. A cybersecurity event can directly trigger or amplify operational or financial risk events.

The 2017 NotPetya cyberattack2 serves as a stark example. It crippled Ukrainian companies before escalating and inflicting billions in damages globally. The attack disrupted operations for multinational corporations such as Maersk and Merck, leading to substantial operational and financial fallout. This incident highlights the necessity of integrating security risk management within the Three Lines Model to prevent, respond to, and recover from similar attacks.

Anchoring cybersecurity risk in reality

Individual business units should ideally have risk appetite statements that align with the organisation's risk appetite statement. They should also as be equipped with qualitative and quantitative key risk indicators for measuring risk. Organisations have typically struggled to develop credible sets of key risk indicators as they relate to the cybersecurity realm — this is particularly so in the context of quantitative metrics.

Key risk indicators serve as the pulse check of an organisation. They indicate alignment with the risk appetite and flag the trajectory of risk — be it stabilising, improving or deteriorating. And yet many organisations are operating without a compass. They lack the necessary data to craft a reliable set of key risk indicators.

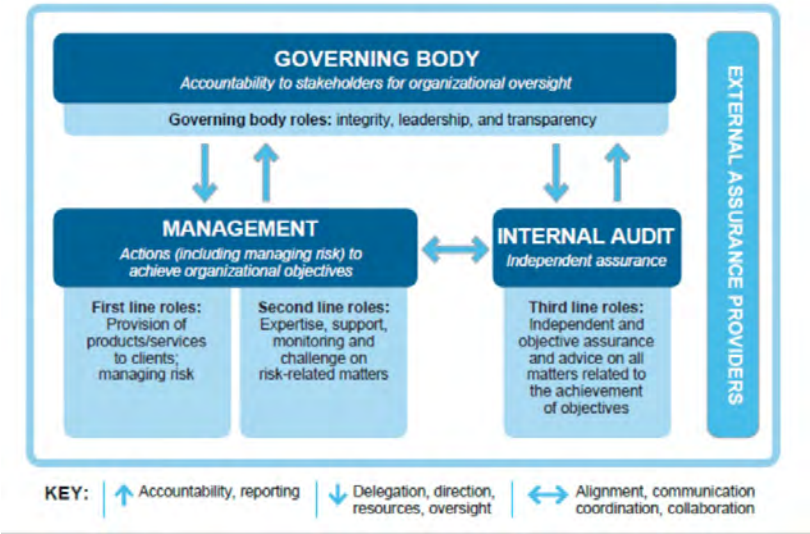
The most critical deficiency lies in the scarcity of predictive data — those faint yet telling signals that herald a looming cyber threat. When these signals are missed, the result is an illusion of security, vulnerable to shattering under the pressure of an unforeseen breach. These breaches are often preceded by detectable signs, which, if identified and interpreted through a well-tuned lens of risk data analytics, could prevent a full-blown cyber crisis.

Addressing this gap requires a dedicated commitment to improving how an organisation records, collects and curates actionable risk data. Robust key risk indicator data, combined with a Three Lines Model-inspired risk appetite statement, support organisations to navigate cyber challenges with confidence.

Adapting the Three Lines Model for cybersecurity accountability

The Three Lines Model is a flexible and adaptive framework for addressing the dynamic business landscape. By tailoring this model to an organisation's specific needs, it establishes a clear, structured approach to accountability in management.

Figure 1 – The Institute of Internal Auditors' Three Lines Model



Source: "The IIA's Three Lines Model — An update of the Three Lines of Defense", The Institute of Internal Auditors, July 2020.

As shown in Figure 1, the Three Lines Model sets out three distinct levels of accountability:

First line: Business and support units

- Own and actively manage risks within the board's risk appetite.
- Establish robust operational structures and processes, ensuring compliance and control.
- Adhere to legal, regulatory, and corporate social responsibility standards.

Second line: Risk and compliance functions

- Develop and uphold the enterprise risk management framework, aligning with board directives.
- Evaluate and challenge the First Line's risk management practices, offering advice and guidance.
- Independently report on risk management performance to the executive leadership and board.

Third line: Internal audit

- Maintain a direct, independent reporting line to the board.
- Assess and communicate the efficacy of risk management by the First and Second Lines

Clarity in cybersecurity risk ownership

Clarity in risk ownership within the Three Lines Model's first line is imperative, yet often elusive. For instance, shared risks may lack a clear custodian, leading to ambiguity over ownership and funding for mitigation efforts. The clarity of ownership is particularly vexing for technology and cybersecurity risks, where ambiguity can lead to governance breakdowns. (For an example of this, see the below case study.)

Ownership should generally reside with the owner of the business activity or system in question. This makes sense, as it aligns risk with its associated business context. Yet, even in organisations with defined risk ownership guidelines, avoidance of accountability can occur. Individuals may overstep their remit, assuming responsibility for risks beyond their purview.

The Chief Information Security Officer plays a key role in resolving these challenges. Their role should be advisory, akin to a medical doctor's relationship with a patient. Like medical professionals, Chief Information Security Officers should not assume the burden of decision-making. This rightly belongs to the business owners.

However, confusion arises when roles and responsibilities are not precisely delineated, leading Chief Information Security Officers to inadvertently shoulder decision-making responsibilities. This is compounded when project managers assume accountability for delivery risk[3] (which may legitimately be within their scope of authority), as well as delivered risk[4] (which should never be within their scope of authority). This can cause risks to slip into live environments unchecked and lead to costly remediations and delays.

The Three Lines Model, with its clear demarcation of roles, ensures precise cybersecurity risk ownership. In turn, it enables Chief Information Security Officers to guide and business owners to decide. The result is fortified governance and accountability.

Data challenges in risk governance

Risk management is about making decisions in the absence of perfect or complete knowledge. However, a critical risk decision can rarely be made without any knowledge at all. **The better the quality, completeness and timeliness of the data on which a risk decision is made, the better the outcome.**

At the same time, organisations often grapple with data deficiencies — too little, too much, improperly captured, or inaccessibly stored. Advancements in AI and machine learning are beginning to enhance risk insight, enabling more informed decisions.

Moreover, delaying difficult decisions invariably restricts options and precludes optimal outcomes. Effective risk decision-making can be distilled into a simple maxim: the right person, with the right information, at the right time.

Integrating the Three Lines Model into cybersecurity risk governance shines a spotlight on the growing importance of data. Timely, relevant and most importantly, trustworthy data is not only important to the operators and protectors of the enterprise's IT systems but also to the business owners in the first line as well as the risk and audit teams in the second and third lines respectively. Only with access to high-quality data can stakeholders across all three lines form the necessary insights to perform their roles within the Three Lines Model.

Addressing skills gaps

With 93 per cent of organisations in a recent Forbes survey reporting a gap in IT skills,5 there's no denying organisations are struggling to attract and retain technical talent. This poses a threat to cybersecurity preparedness, while also hindering the second and third lines from fulfilling their roles.

These lines rely heavily on expertise to identify, assess, and mitigate digital risks. Without sufficient skills in areas such as threat intelligence and analysis, incidence response and regulatory compliance knowledge, these lines may struggle to adequately oversee and audit measures.

To counter this, forward-thinking organisations are cultivating talent across all lines, investing in training, and fostering career mobility. AI and machine learning advancements promise further enhancement of these capabilities.

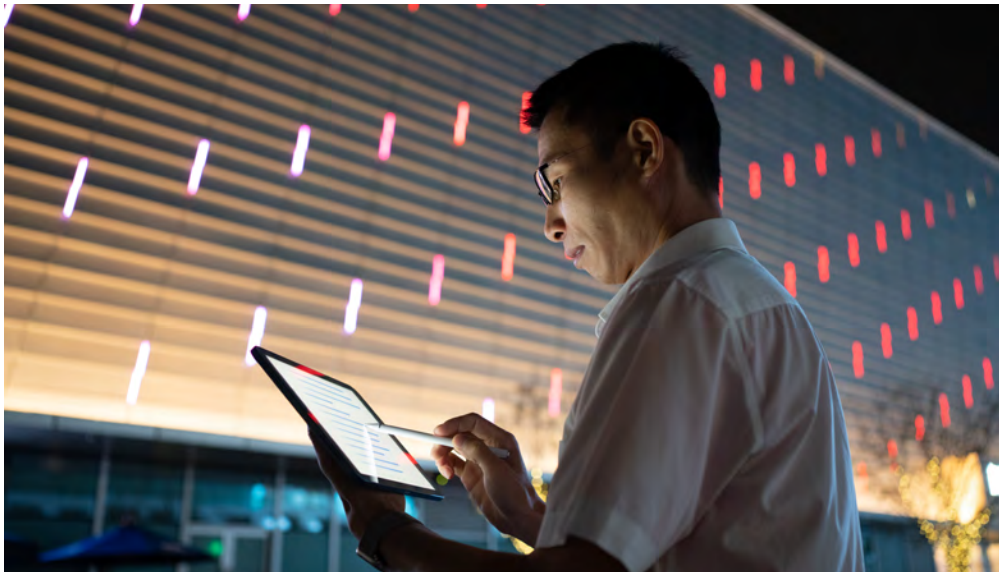
Strengthening risk management and compliance through system integration

The Three Lines Model requires seamless integration between each line's systems and functions to enhance risk management and compliance. In fact, its cohesive approach to risk management and compliance (typically steered by the second line) can help avoid the perils of system isolation and partial insights — both of which affect an organisation's cybersecurity posture.

Why integrated systems matter in a Three Lines Model

Success in cybersecurity governance hinges on the first line's engagement: their input enriches the system, enhancing its relevance and utility in reflecting the true risk environment. This engagement becomes the linchpin for system integration, ensuring insights provided by the risk and compliance platforms are accurate and actionable.

When systems are disconnected — such as when the second line's systems operate in isolation from the first line's business and technology systems — shared data and insights can be lacking. This separation can also cause information asymmetry, compromising the data quality used by the second and third lines. It can also potentially affect the completeness, accuracy and relevance of risk assessments.



Without integrated systems, second and third lines may struggle to gain a comprehensive view of risks, especially in the realms of technology and IT. This siloed perspective may hinder their ability to effectively critique or endorse the first line's strategic proposals for addressing these risks. Second and third lines may resort to sampling or deep dives to understand the organisation's risk profile, which don't necessarily capture the broader risk context. The first line may then implement quick fixes rather than comprehensive solutions, neglecting more critical risks that require attention.

A Three Lines Model approach for integrating systems

All three lines must recognise the significance of integrating risk management and compliance systems into the core operational systems of the first line.

The second and third lines must rigorously test and constructively challenge the first line's strategies, but the effectiveness of their review and support is contingent upon the quality of the data they receive.

It is also essential to consider the informational needs of all lines in the development and maintenance of the first line's systems, ensuring that risk management and compliance are embedded from the outset.

To the IT leaders steering their organisations through a sea of cyber uncertainties, the call to action is clear: Advocate for and invest in harmonising systems across all lines of defence. Embrace a 'risk and compliance by design' philosophy, ensuring that the architecture of your first-line systems incorporates the needs of the second and third lines.

This foresight will create a robust, shared data ecosystem that empowers each line to operate with the full context, elevating your organisation's risk posture and decision-making.

Where to from here?

Whether your organisation has implemented a Three Lines Model for risk management governance, or you are part of any of the three lines defined within this model, the crux of effective cybersecurity governance lies in the power of trusted, verifiable data and integrated systems. The journey towards robust cybersecurity governance is multi-faceted:

- **The significance of risk appetite:** A well-defined risk appetite is crucial for balancing strategy with oversight. Risks must align with an organisation's strategic objectives and business plan.
- **Data-driven insights as a cornerstone:** The need for reliable, predictive data to foresee and manage emerging cyber threats cannot be overstated. This calls for a commitment to enhancing data collection and analysis processes.
- **Integration and collaboration across the three lines:** A unified approach, where all three lines actively engage and contribute to a cohesive risk management strategy, is critical. This integration ensures risk and compliance systems reflect real-time, on-the-ground realities, especially in the dynamic field of threats.
- **Overcoming information asymmetry:** Bridging gaps between lines to prevent information asymmetry is key. Seamless communication and data sharing across all lines ensure risk management is proactive, comprehensive and timely.

The true strength of governance lies not in isolated efforts or siloed strategies but in the collective, data-driven insights and actions across all levels of an organisation.

Every organisation can transform technology and cyber data into shared, actionable risk management insights. Tanium's expertise and solutions offer a pathway to not just understand but actively manage and mitigate technology risks and threats, aligning with the principles and structure of the Three Lines Model.

Case study: Optimising risk management with the Three Lines Model

In an initiative to strengthen its cybersecurity, a major Australian organisation implemented a vulnerability and patch management scanning system across its IT network. Initially, the data was reported by platform type, like desktops and servers, which catered well to the maintenance teams responsible for these platforms. However, this approach lacked a crucial element: alignment with the Three Lines Model for effective cyber risk management – especially in the context of risk ownership.

The turning point occurred when it was recognised that the reporting format did not meet the needs of the business owners — the rightful first-line risk owners in the Three Lines Model. These owners required insights specific to their segments of the IT network, crucial for assessing compliance with the organisation's risk appetite. The existing reporting format obscured their visibility of their cyber risk and hindered their ability to prioritise measures alongside other business activities while maintaining stability in their operational domains.

To realign with the principles of the Three Lines Model, the reporting system was restructured to offer dual perspectives: one by platform for technical maintenance (first-line service provider) and another by business unit for operational management (first-line business risk owner). This strategic adjustment significantly enhanced the effectiveness of the program. It empowered the business owners with the clarity to make informed decisions and prioritise within their risk management strategies.

This adaptation also improved data quality and relevance, benefiting both the second and third lines by providing more comprehensive oversight and enabling more informed executive and board-level decision-making. It exemplified the Three Lines Model in action, with each line contributing to a holistic, effective approach to managing cyber risks within the organisation.

Embark on your governance journey with Tanium

Tanium can redefine your approach to risk management and turn challenges into opportunities for secure, sustainable growth. Contact Us to find out more or learn more about Tanium's Platform here

Contact Us