Senior Risk Partner – Digital & Cyber
Legal & Assurance

Role snapshot

Reports To	People leader	Direct reports
GM Risk & Resilience	No	NA
Role Band	**Business Unit**	**Department**
7	Legal & Assurance	Risk & Resilience
Location	**Delegated authority – OPEX**	**Delegated authority – CAPEX**
Auckland	To be confirmed	To be confirmed

Purpose

Provide independent second-line risk leadership and oversight across Digital & Data, Technology and Cyber Security, ensuring technology, cyber, information, AI and third-party risks are effectively identified, assessed, monitored and managed within Vector's enterprise risk management framework and approved risk appetite.

The Senior Risk Partner – Digital & Cyber partners with business leaders, Digital & Data, Technology and Cyber Security teams to strengthen risk maturity, improve decision-making and support the sustainable delivery of business outcomes. The role ensures material risks are visible, understood and appropriately managed while providing constructive challenge, oversight and assurance regarding risk exposure, control effectiveness and risk treatment activities.

The role contributes to organisational resilience by embedding practical risk management practices, translating enterprise risk appetite into operational decision-making and ensuring technology-related risks remain aligned with Vector's strategic objectives and governance expectations.

Capabilities, experience & skills

Skills	Capabilities	Experience
Strong skillset in cyber security, digital technology, AI, data and operational risk.	Strong business acumen with the ability to understand, support and challenge operational priorities, specifically digital and cyber security practices.	At least 5 years senior level experience in technology and cyber security.
Formal risk management experience is not essential. What matters most is a proven ability to engage with Digital, Data and Cyber teams to navigate digital and security risks and competing priorities.	Ability to translate complex technical risks into business impacts and decisions.	Experience supporting senior leaders, executives and governance bodies.
Excellent written and verbal communication skills, with the ability to clearly articulate and	Strong stakeholder engagement and influencing capability.	Experience working within or alongside risk frameworks and methodologies.

discuss complex digital insights and risks to a wide range of stakeholders.	Ability to provide independent challenge while maintaining trusted relationships.	Experience operating within regulated, critical infrastructure or complex corporate environments
	Strategic thinking and sound judgement.	
	Strong communication and facilitation skills.	

Key accountabilities & outcomes

Governance and Risk Leadership

- Embed strong risk management practices across Digital and Cyber Security functions.
- Promote alignment between risk practices and strategic, customer, and operational priorities, ensuring decisions reflect Vector's risk appetite.
- Facilitate timely and accurate communication of risks, insights, and opportunities that may influence service delivery or organisational objectives.
- Maintain and refine risk-related policies, standards, and procedures, ensuring they remain current and fit for purpose.
- Apply relevant industry standards and frameworks where they add value to strengthening Vector's risk maturity.

Digital & Cyber Risk Partnering

- Act as a trusted partner to Digital, Data and Cyber teams, integrating risk thinking across strategy and operations.
- Support teams to identify, assess, and manage risks in line with Vector's risk appetite.
- Assess emerging risks associated with new technologies, AI, digital platforms and evolving operating models.
- Support teams to make well-balanced, technically informed decisions, ensuring customer and stakeholder outcomes, data integrity, security, and reliability remain front of mind.
- Ensure risk management is integrated into strategic and operational activities and that gaps in mitigation or monitoring are identified and addressed.

Risk Assurance

- Design and deliver a targeted risk assurance programme to test the effectiveness of key controls and risk mitigation strategies.
- Conduct second line assurance reviews in collaboration with Digital and Cyber teams, providing practical recommendations for improvement.
- Monitor and report on the performance of key controls, highlighting areas requiring attention.
- Maintain a clear record of assurance findings and ensure follow-up actions are tracked to completion.

Risk Reporting and Analytics

- Lead the development of Digital and Cyber risk reporting to senior leadership, ensuring visibility of key operational and strategic risks.
- Maintain and enhance risk systems and key risk indicators to support consistent and accurate risk data capture and analysis.
- Use data and insights to identify emerging risks, trends, and opportunities for improvement.
- Ensure reporting aligns with the enterprise risk management framework such that it supports oversight by the Executive and Board.

Team Effectiveness

- Participate in team and group projects.

- Promote and foster a highly engaged and positive risk culture in the organisation.

Key relationships

Internal

- GM Risk & Resilience
- General Counsel & Company Secretary
- GM Cyber Security
- GM Technology
- GM Data & Analytics
- GM Delivery & Change
- Business Owners
- Delivery Partners
- Architecture leaders
- Risk & Resilience team
- Executive Leadership Team

External

- External auditors
- Risk and assurance providers
- Cyber and technology suppliers
- Regulatory and industry bodies
- Strategic delivery partners

Living our behaviours

Change Makers | Customer. Customer. Customer. | Walk in Others' Shoes | We, Not Me | Consider It. Done.

Health, safety and wellbeing

Everyone has a personal and company-wide responsibility for health, safety and wellbeing, including compliance with relevant standards, policies and procedures and prompt escalation of hazards, near misses, injuries and incidents. During emergency or business-critical events, the role may be required to support response activities outside normal responsibilities or standard hours, with appropriate support and guidance.

Emergency & critical event support

Due to the nature of Vector's business and its critical role within the community, there may be emergencies and/or business and community critical events (such as power outages through storms or natural disaster events). This may require you to be available to perform duties outside of your normal day-to-day responsibilities and become part of a companywide response team. The employee and the manager will discuss these requirements, recognise the employee's personal circumstances and agreeing to the working hours.

During these events, Vector will continue to provide the necessary support and systems to operate in the safest and healthiest way possible. Vector empowers its managers and individual employees to monitor their health more closely, notice changes in themselves and others, and encourages open communication to seek any required support.