Job description

Title	Chief Information Security Officer
Number	
Group	Corporate Operating and Financial Office
Division	Digital Services
Reports to	Chief Digital Officer
Direct reports	Enterprise Security Manager (not yet created), Enterprise Architect
Date	23/9/2026

Job holder commitment

The job holder accepts as a fundamental requirement of their employment that they must demonstrate a personal commitment to:-

- modelling organisational values at all times
- a safe and healthy work environment
- assisting Council to fulfil its Civil Defense responsibilities

At TCC we uphold the principles of Te Tiriti o Waitangi by engaging in an effective and meaningful partnership with tangata whenua. We are committed to developing our knowledge and understanding of te reo Māori, tikanga Māori, Matauranga Māori and our partnership with tangata whenua.

Job purpose

Provide strategic leadership, governance and assurance for information security, cyber security, artificial intelligence governance and enterprise architecture across the organisation. Lead organisational capability and advise executive leadership on security, technology risk and resilience.

Key outcomes

High Performance Leadership Team	• Live the principles of a high-performance and collaborative leadership team for Digital Services. • Model these principles and behaviours for the wider organisation. • Co-lead and promote projects and processes relating to secrity across Digital Services.

People leadership and capability development	• Contribute as a member of the Digital Services leadership team modelling organisational values and collaborative leadership behaviours. • Lead cross-functional initiatives that strengthen organisational outcomes. • Provide leadership and direction to build high-performing, collaborative teams and capability across areas of responsibility. • Build organisational capability and understanding of information security, cyber risk, AI governance and emerging technology. • Support and enable leaders and teams to understand their responsibilities and confidently embed secure and responsible practices into their work.
Enterprise security strategy, governance and assurance	• Set and lead the enterprise information and cyber security strategy. • Establish governance frameworks, policies and standards. • Provide assurance and strategic advice to executive leadership and governance bodies. • Embed security-by-design principles across organisational initiatives.
Cyber risk, compliance and resilience	• Oversee enterprise cyber risk, compliance and assurance programmes. • Ensure compliance with applicable obligations and standards. • Lead organisational cyber resilience, incident response and recovery capability. • Develop and talk to approapirate levels of cyber intelligence and information and Audit & Risk Committee
AI and emerging technology governance	• Lead risk management and assurance components for AI and emerging technologies. • Ensure responsible, secure and ethical adoption of AI. • Provide executive assurance on opportunities, risks and value realisation.
Enterprise Architecture Sponsorship	• Act as executive sponsor for Enterprise Architecture, • Align business strategy, technology investment and organisational change
Strategic stakeholder engagement	• Maintain influential relationships with regulators, government agencies, industry bodies and partners. • Represent the organisation on cyber security and emerging technology matters.

The job description is not an exhaustive list of requirements, the job holder will be required to perform tasks assigned to them that are not explicitly described in this document.

Person specifications

Essential
• Degree-level tertiary qualification, preferably with a postgraduate qualification in a relevant discipline (e.g. cyber security, computer science, risk). • 10+ years cyber/information security leadership experience (preferably at CISO level) • Recognised industry certification(s) such as CISSP, CISM, CRISC or equivalent • • Strong working knowledge of relevant frameworks and legislation, e.g. NZISM/Protective Security Requirements, ISO 27001, NIST, PCI DSS and the Privacy Act 2020.nt or executive level • Demonstrated experience leading cyber incident response and engaging confidently with executive leadership, Boards/Elected Members and regulators during significant events. • Proven experience in a senior digital or technology security leadership role, including budget, vendor and multi-disciplinary team accountability. • Sound understanding of AI security governance and emerging technology risk, and its practical application in a complex organisation.

Here to make Tauranga better

WHANAKE TE TAI

Our values

Pono / Integrity

We do what we say we will do

Manaakitanga / Respect

We listen to all views and show we care

Whāia te tika / Service

We do the right thing for our community and each other

Whanaungatanga / Collaboration

We work together and create connections