Job description

Title	Enterprise Information Security Manager
Number	
Group	Chief Operating Financial Office
Division	Digital Services
Reports to	Chief Information Security Officer
Direct reports	Security Risk and Assurance Officer
Date	October 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 Defence 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

The primary purpose of this role is to lead Council's information security governance, risk, compliance and assurance (GRC) function. The role is accountable for the security policy framework, the management of information security risk, compliance with legislative, regulatory and contractual obligations including PCI DSS, and independent assurance that security controls are designed and operating effectively. Translate security strategy into a governed, measurable and auditable programme, ensuring the Executive Leadership Team, Audit and Risk Committee and Elected Members have clear and timely visibility of Council's security posture, risk and compliance.

Key outcomes

Lead a high-performing security GRC and assurance team	• A high-performing, engaged and capable security GRC team delivers against Council priorities. • Governance, risk, compliance and assurance activities are effectively prioritised and resourced. • Team capability, resilience and succession are strengthened to meet evolving security and regulatory demands.

	• External assurance providers deliver quality outcomes and value for money. • A culture of collaboration, continuous improvement and high performance is embedded across the team and Digital Services
Security governance and policy	• Council maintains an effective and fit-for-purpose information security policy and governance framework. • Security roles, responsibilities, decision-making and escalation pathways are clearly defined and understood. • Security practices align with recognised standards and support organisational objectives. • Security maturity is measured, reported and continuously improved. • Security policies are consistently applied and embedded across Council.
Information security risk management	• Information security risks are identified, assessed, treated and monitored within Council's risk appetite. • Security risks have clear ownership, treatment plans and ongoing oversight. • Security risk advice supports informed decision-making across projects, systems and services. • Significant risks are appropriately escalated and formally accepted where required. • Third-party security risks are effectively managed and mitigated.
Compliance and PCI DSS	• Council meets applicable information security legislative, regulatory and contractual obligations. • PCI DSS compliance is maintained and independently evidenced. • Emerging compliance obligations are proactively identified and addressed. • Security, privacy and information management requirements are managed in an integrated and effective manner.
Security assurance and audit	• A risk-based assurance programme provides confidence that security controls are effectively designed and operating. • Audit and assurance findings are addressed in a timely manner and drive measurable improvement. • Security assurance is embedded within solution delivery and change processes. • Systems and services receive appropriate security certification and accreditation. • Assurance practices are continuously improved to increase effectiveness and efficiency.
Incident readiness and resilience assurance /Security awareness culture	• Council's incident response, business continuity and disaster recovery capabilities are regularly tested and effective. • Lessons from incidents and investigations strengthen Council's security posture. • Security incidents are supported by consistent risk, compliance and stakeholder management. • Staff demonstrate security-aware behaviours and understand their security responsibilities.

	• Security awareness activities contribute to reduced organisational risk and improved resilience.
Reporting and relationships	• Leadership receives timely, accurate and actionable reporting on security posture, risk, compliance and assurance. • Security performance and risk indicators support informed governance and investment decisions. • Technical security matters are translated into clear business impacts and priorities. • Trusted relationships across Council and external stakeholders support effective security outcomes. • Collaborative partnerships strengthen Council's security capability, resilience and adoption of good practice. • Relationships are leveraged to achieve organisational objectives and support team success.

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 in cyber security, information technology, computer science, risk or related discipline. • 8 plus years experience in information security including 3 years in governance, risk, compliance or assurance. • Recognised industry certification such as CISSP, CISM, CRISC or CISA • Strong working knowledge of NZISM, the Protective Security Requirements, ISO/IEC 27001, the NIST Cybersecurity Framework, PCI DSS and the Privacy Act 2020, and experience applying them in a complex organisation. • Experience leading a team, managing external auditors, assessors and specialists • Excellent report writing, influencing and communication skills, with the ability to translate technical risk to non technical audience. • Experience within local government, central government or a similarly complex, highly regulated operating environment.

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