# Information Security Lead Role

## Purpose

This role is key in helping to safeguard the Banks assets and information by providing consultancy advice and practical assistance on information security risk and control matters, promoting the commercial advantages of managing information security risks efficiently / effectively and leading the implementation of security uplift initiatives. You will have security oversight across the bank providing guidance on security architecture, vendor compliance, vulnerability management, related regulatory changes, industry trends & emerging threats and staff training.

You will be responsible for working with the CISO to implement appropriate information security controls to satisfy the Bank needs in accordance with security policy & standards, risk management, risk appetite, best practices and regulatory expectations. This includes integration into the Banks broader policies and processes around incident response and the development of contingency plans for events which could impede business and/or harm the Banks reputation.

## Role dimensions

- **Reports to:** Head of Information Security and Technology Risk (CISO)
- **Department:** Technology
- **Location:** New Plymouth, Auckland or Wellington
- **Direct Reports:** No

## Person specifications

- 5+ years of experience in information security and risk management role.
- Professional Certifications such as CISSP, CISM, CISA, CRISC etc.
- Experience working in the financial services industry desired.
- Good understanding of the information security processes, concepts and best practices.
- Knowledge of information security frameworks or standards such as NIST CSF, ISO 27000 series, ITIL as well as controls management.
- Experience working with RBNZ & FMA guidelines, AML/CFT requirements, and New Zealand's Privacy Act 2020.

## Role specific areas of responsibility

- **Leadership, Collaboration & Culture** – Be a leader and advocate for information security amongst your team, your peers, the Bank and key stakeholders. Collaborate with technology, audit, risk, legal, procurement and the wider business to ensure a cyber resilient culture is core to everything we do at the Bank. Working with your peers you will drive an embedded culture of cyber resilience where everyone has the training and awareness to carry out their role to maintain cyber resilience.
- **Information Security Consulting, Policies & Reporting** – Help ensure that information security controls are embedded across the Bank. This includes advocating and consulting across the Bank on matters relating to information security and includes engaging with change initiatives to provide information security direction throughout the change lifecycle. Assist the CISO to ensure the right policies, standards and guidelines are updated and maintained to provide guidance to the Bank and partners. Provide appropriate and timely reporting on information security posture to senior stakeholders.
- **Information Security Risk Management & Threat Awareness** – In collaboration with the Technology risk and the Banks risk functions, ensure appropriate information security risks and controls are captured and managed appropriately. This includes proactively identifying new risks across the Bank and adjusting / developing new controls, being across new emerging cyber threats and being engaged with industry regulators and partners.
- **Strategy, Architecture & Roadmap** – Develop in conjunction with the CISO the Banks information security strategy. This should incorporate security architectural definitions and practices to embed good information security practices and controls across the Bank.
- **Security Programme Delivery & Improvements** – Lead and provide input into a programme of continuous improvement across information security which clearly identifies and tracks improvements in accordance with an agreed controls framework. Any investments in the business, technology or information security area should clearly identify the return on investment in controls lifecycle maintenance or improvement.
- **Security Assurance** – Contribute to an assurance framework that collaborates with internal teams for self and continuous assessment, and any external assessments including regulators and independent testing. The assurance framework should clearly define the controls, their current effectiveness and identify their overall design and operating effectiveness to meet agreed and regulatory compliance outcomes. This should be fundamental to supporting any remediation, improvement or risk mitigation activity.
- **Third Parties –** Ensure third parties adhere to TSB's requirements and policies. Work with the procurement team in relation to onboarding and regular assessments of third parties.
- **Industry Engagement –** Maintain relationships with the wider New Zealand security community, in order to provide perspectives on information security approaches being adopted in response to changes in the threat landscape.

***Note:*** *From time to time there may be additional activity not contained within this position description that the appointee is to complete in the interests of the appointment and their own personal development. The position description is a living document and the Bank reserves the right to amend from time to time as required.*