Security Consultant Role Mandate

Purpose

This role is key in helping to safeguard the Banks assets and information by identifying, analyzing and helping to mitigate cyber risk across the organization through the completion of security risk and control assessments, implementing treatments that mitigate security concerns and participating in the operation of security functions across the Bank. You will have the opportunity to grow and develop your security skills across various technical and non-technical security domains while providing safe security outcomes for the Bank, its customers and its stakeholders.

You will be responsible for contributing to security governance and assurance activity by providing evidence of effective security operations, identification of security threats, delivering risk analysis and treatment recommendation, working with stakeholders and the wider security team and learning and developing your skills in delivering best practice security advise to stakeholders.

Role dimensions

- **Reports to:** Information Security Lead
- **Department:** Technology
- **Location:** New Plymouth, Auckland or Wellington
- **Direct Reports:** No
- **Financial Authority:** No

Person specifications

- 2-4+ years of experience in information security or technology risk role.
- Graduate or foundational professional certifications such as SSCP or Security+.
- Experience working in the financial services industry desired.
- An understanding of the information security processes, concepts and frameworks.
- Experience delivering and operating technology and security solutions.

Role specific areas of responsibility

- **Information Security Risk and Threat Identification** – Responsible for completing risk security assessments to ensure security risks and threats to the Banks assets are identified, the likelihoods and potential impacts are understood, treatments identified and monitored through supporting governance and assurance activity to completion, while contributing to the overall security posture of the Bank.
- **Information Security Treatments** – In collaboration with the Banks wider Security and Technology functions, responsible for providing advice on ways to address security risks through treatments, monitoring security treatments to ensure they mitigate or remediate operational risk, and contributing (through analysis / expertise) to strategic enterprise security initiatives to improve the Banks protective and detective security capabilities.
- **Data Security Operations** – Contribute to the operational effectiveness of data protection controls through identification and resolution of potential events, remediation of identified issues, and the continuous development of our data security operations.
- **Identity and User Access Operations** – In collaboration with the Banks wider Security functions, contribute to the improvement of enterprise identity and user access controls.
- **Security Assurance** – Help ensure that the Bank is able to meet its internal and external security obligations by contributing to cyber assurance activities such as information gathering for audits, regulatory reviews and independent assessments.
- **Security Skills and Industry Engagement –** Grow and maintain your cyber security skills through workshops, industry events and building internal relationships with stakeholders and engaging externally with the wider New Zealand technology and security community.

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.*