Position description

Position title	Supplier Security Assurance Analyst
Group / Branch	Finance & Technology/Enterprise Security & Resilience
Reports to (Title)	Cyber Resilience Strategy Manager
Competency level	Individual Contributor

Job Purpose

Supplier Security Assurance Analyst is responsible to provide specialist advice on supplier risks and assurance that SEW suppliers and third parties adhere to security requirements, policies and standards. This role will work closely with Procurement, Legal, Contract and Business Owners to assess and monitor security practices of suppliers and manage relevant risks and exposures to protect SEW information, systems and services.

Key Accountabilities

- Lead security risk assessments for new and existing suppliers across the life cycle applying a risk-based approach
- Evaluate the supplier business dependencies and adequacy of their security practices and controls against SEW security requirements, policies and standards
- Maintain the supplier security posture ensuring ongoing monitoring and re-assessments, tracking remediation actions for closure where necessary
- Clear, consistent documentation and reporting of the identified supplier risks and control gaps and provide appropriate risk treatment recommendations
- Review and embed SEW security controls and requirements within the supplier contracts and agreements and support Procurement and Legal teams
- Enhance the third-party risk management program and resolve material risks in a timely manner
- Develop security policies, standards and procedures from the supplier security assurance activities
- Develop initiatives to build resilience from supplier activities and support security operations for third-party breaches/incidents

- Able to obtain security clearance as needed

Knowledge, Skills & Experience

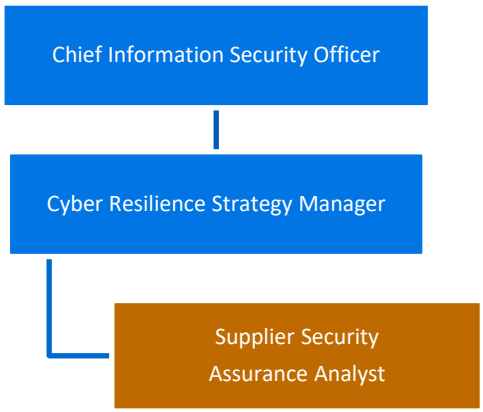
- 5+ years of experience in information risk or third-party risk, assurance role or equivalent
- Demonstrated experience in third party risk management using platforms such as UpGuard, SecurityScoreCard, BitSight or similar
- Strong understanding of cyber security fundamentals, principles and frameworks such as NIST CSF, ISO 27001, VPDSS, ASD ISM, CIS etc.
- Understanding of common security controls and practices across OT, Cloud, SaaS and Managed Services in an enterprise environment
- Ability to interpret assurance artefacts and negotiate security requirements with suppliers
- Strong analytical, communication and stakeholder engagement skills
- Familiarity in critical infrastructure or regulated environments is desirable

Education and Formal Certifications:

- Bachelor's degree in computer science, Cybersecurity, Information Security, or a related field (or equivalent experience)
- Certifications such as CISSP, CTPRP, CTPRA, CRISC or ISO 27001 highly desirable

Dimensions

Organisational Chart



Number of people managed: N/A

Size of budget managed: N/A

Value of Assets managed:

Describe the level/type of responsibility the role has over the organization's assets, both physical and non-physical

Ensuring a sustainable, resilient organisation:

Authorities outlined in **Instrument of Delegations** None

Compliance management responsibilities outlined in the **compliance and obligations register** None

Security for Critical Infrastructure identified role: No