Position description

Position title	Vulnerability Assessor
Group / Branch	Finance & Technology/Business Technology Services
Reports to (Title)	Security Architecture and Engineering
Competency level	Individual Contributor

Job Purpose

Vulnerability Assessor is responsible to identify, analyse, prioritise and report security vulnerabilities across IT infrastructure, applications, and cloud environments. Vulnerability Assessor will work with the security, technology and business teams to ensure timely remediation of security risks and vulnerabilities, improving overall security posture.

Key Accountabilities

- Conduct vulnerability scans and assessments across on-prem networks, cloud and OT environments.
- Perform manual validation and analysis of vulnerabilities to reduce false positives.
- Collaborate with Enterprise IT, Operational Technology and development teams to prioritise and remediate vulnerabilities.
- Assess third-party software and services for security weaknesses and address vulnerabilities
- Develop and maintain vulnerability management policies, processes, and metrics.
- Research and provide informational updates on emerging threats, vulnerabilities, and mitigation strategies.
- Assist with penetration testing and red teaming efforts when necessary.
- Generate detailed reports and executive summaries outlining risk levels and remediation strategies.
- Support security operations and liaise with the internal and external stakeholders to remediate reported vulnerabilities
- Able to obtain security clearance as needed

Knowledge, Skills & Experience

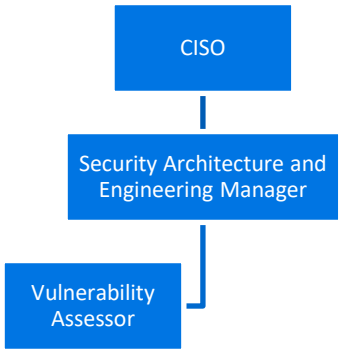
- 3+ years of experience in vulnerability assessment, penetration testing, or security analysis.
- Proficiency with scanning tools (Nessus, Qualys, Rapid7, CrowdStrike, Defender, Dragos etc.).
- Understanding of common security vulnerabilities (OWASP Top 10, CVSS scoring, etc.).
- Experience with cloud security and container security assessments.
- Knowledge of security frameworks (NIST, CIS, MITRE ATT&CK).
- Ability to interpret security findings and communicate risks to technical and non-technical stakeholders.
- Experience with penetration testing methodologies and tools (Burp Suite, Metasploit, etc.)
- Experience with scripting (Python, PowerShell, Bash) for security automation

Education and Formal Certifications:

- Bachelor's degree in computer science, Cybersecurity, or a related field (or equivalent experience).
- Industry certifications such as OSCP, CEH, GPEN, or CISSP

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