

Job Title	Asset Security Manager
Reports To	Cyber Risk Management Manager
Grade	Grade 6

Purpose	Define and deliver the strategy for the accurate identification, recording and classification of vulnerabilities in WWU's IT and OT assets estate, together with the vulnerability management and remediation regime required to ensure asset vulnerabilities remain within business risk appetite.
Key Accountabilities	<ul style="list-style-type: none"> • Define and manage the technology asset register for the cyber team, utilising existing data sources where available and defining new sources where they are not already in place. • Ensure the ongoing accuracy and completeness of the register, including the correct classification of systems, key technical attributes, asset purpose, criticality, business and system owners and relationships with other assets. • Define and implement the vulnerability identification, prioritisation and management processes required to ensure WWU has an accurate view of the vulnerabilities in its asset estate and follows an agreed methodology for prioritising and remediating vulnerabilities. • Work closely with colleagues performing related penetration testing and risk assessment activities, providing accurate and timely technical information regarding assets and the status of vulnerabilities. • Prepare and deliver regular, high-quality management reporting regarding WWU's asset estate and its security posture.
Technical Know-How & Skills	<ul style="list-style-type: none"> • Deep understanding of asset discovery and management principles, methodologies and tooling with proven experience in an IT asset management role • Deep understanding of vulnerability management principles, methodologies and tooling with proven experience in a vulnerability management role • Strong understanding of operational technology concepts and differences between IT and OT environments • Strong understanding of attacker TTPs • Strong written and verbal communication skills in English • Strong understanding of security risk assessment and risk management concepts and approaches • Strong commitment to personal development and self-learning with ability to work on own initiative • Ability to work with less technical colleagues and be able to convey technical information in a way that all can understand • Experience of managing a team of technical staff • Experience with operational technology in the utilities sector or other industrial CNI environments will be highly advantageous

Qualifications	<ul style="list-style-type: none"> • Networking and infrastructure certifications e.g. Cisco, Microsoft, Linux, Azure (desirable) • Relevant tool-specific certifications e.g. Nessus, Lansweeper etc. (desirable) • CISSP (desirable) • GICSP (desirable) • GIAC (desirable)
Job Dimensions	<p>People Management: The role holder will be required to manage a small team of asset vulnerability analysts who will assist the Asset Security Manager in achieving the objectives of the role.</p> <p>Vendor Management: The role-holder will manage WWU preferred suppliers who will provide additional resource and capabilities where required to ensure the objectives of the role are fully met.</p> <p>Budget Management: No budget management requirements. Knowledge of Opex, Capex and general procurement processes useful.</p>