Job Title	Industrial Control Systems Security Manager
Department	Cyber Resilience Team
Reports to	Cyber Risk Management Manager
Grade	Technical Tier 3
Purpose & Overview	- The Industrial Control Systems Security Manager in Wales & West Utilities (WWU)'s Cyber Resilience Team will focus on overseeing and managing the cyber security assurance program for industrial control systems. - This position involves developing and implementing strategies to ensure the availability, integrity and confidentiality of critical operational technology (OT) assets. - This roleplays a crucial role inleading a team of experts, conducting technical risk analysis and evaluation and implementing measures to enhance the overall cyber resilience of industrial processes. - The role defines strategies for OT resilience and security that ensures compliance with industry standards and regulatory requirements, while contributing significantly to the safety, reliability and cyber resilience of WWU's critical industrial processes. - Strong leadership skills, technical expertise and a commitment to continuous improvement are essential for this key role.
Key Responsibilities	- Develop and implement the cyber assurance strategy for WWU's industrial control systems, aligning it with WWU's cyber security strategy and wider business goals. - Collaborate with key stakeholders to ensure the strategy meets operational and regulatory requirements. - Oversee and conduct risk assessments specific to ICS environments to identify and prioritise potential security vulnerabilities. - Develop and implement risk mitigation strategies, considering the safety and reliability of industrial processes. - Manage the overall ICS cyber assurance program, including assisting with the development of policies, procedures and assurance frameworks. - Ensure that assurance activities align with industry standards, regulatory requirements and WWU's business goals. - Lead a team of ICS cyber security professionals, providing guidance, mentorship and support as required. - Foster a culture of continuous learning and professional development. - Assist with the development and maintenance of incident response plans specific to ICS environments. - Assist with incident response efforts during cyber security incidents, collaborating with IT and OT teams to minimise disruption and investigate root causes. - Oversee the implementation and management of security controls for ICS, including firewalls, intrusion detection and prevention systems and endpoint protection. - Collaborate internally and externally (with the IT Team), as required, to ensure the effective deployment of security measures.

	– Ensure compliance with relevant regulations, standards and guidelines specific to ICS cyber security, such as NIST Cyber Security Framework and IEC 62443. – Oversee assurance testing activities, including vulnerability assessments, penetration testing and compliance audits. – Collaborate with external auditors to validate the effectiveness of security controls. – Ensure compliance with security awareness and training programs for personnel working with ICS components. – Promote a culture of security awareness and best practice within the OT environment. – Implement lessons learned from incidents, audits and assurance activities, to enhance overall cyber resilience. – Collaborate with OT and IT teams to ensure a unified approach to cyber security across WWU. – Facilitate communication and cooperation between traditionally siloed OT and IT environments. – Maintain comprehensive documentation of cyber assurance measures, configurations and incident response procedures. – Generate regular reports for senior leaders as required.
Technical Skills	– Broad experience in a similar technical role, ideally some of which has been spent in a CNI or stringently controlled environment. – A good understanding of ISA/IEC 62443 standards and technical frameworks such as ICS410. – A deep knowledge base of technical solutions; protocols, hardware, software, and applications. – Knowledge of network architecture, firewalls, DMZ, and segmentation strategies to protect ICS networks. – Proficiency in securing operating systems, databases, and applications specific to industrial control systems. – Ability to develop and execute incident response plans tailored to the unique challenges of ICS environments. – Understanding the complexities of applying patches in an ICS environment, lifecycle management, considering system stability, uptime and IGEM requirements. – Conducting regular security audits to ensure compliance with internal policies and external regulations. – Familiarity with programming languages commonly used in ICS and the ability to automate security tasks. – Knowledge of physical security measures to protect ICS hardware and infrastructure. – Understanding of ICS-specific communication protocols like Modbus and DNP3.
Qualifications	– Essential: – Extensive experience in multi-faceted engineering and cyber roles with a focus on industrial control systems and OT environments. – In-depth knowledge of ICS security principles, standards and protocols. – Strong communication and interpersonal skills for effective collaboration with cross-functional teams. – **ISA I**EC62443 Fundamentals Specialist – GICSP – Desirable: – Bachelor's or Master's degree in Cyber or Engineering related field – ISA IEC62443 Cyber Security Expert

Formatted: Font: Bold

	– Other relevant cyber security or engineering certifications
Additional Information	– Vetting required – We require candidates to hold SC Clearance for this role. WWU will sponsor candidates who do not already hold SC Clearance through the process. Please note, however, that failure to attain or maintain SC Clearance during your tenure within this role, will be grounds for termination. Typically, this requires that candidates are either UK Nationals, or, have been resident in the UK for a minimum of five years and hold indefinite Right to Remain. Further details of what SC Clearance entails can be found at: https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels