

Job Title	Senior Cyber Security Architect
Department	Cyber Resilience Team
Reports to	Cyber Resilience Manager
Grade	Technical Tier 3
Purpose & Overview	The Senior Cyber Security Architect role in Wales & West Utilities (WWU)'s Cyber Resilience Team is responsible for designing and implementing robust cyber security solutions to safeguard WWU's information assets. This role involves developing strategic security architectures, in line with WWU's Cyber Security Strategy, to ensure the integration of security controls and collaborating with various teams to enhance overall cyber resilience. This is a critical role in aligning security strategies with business objectives in order to mitigate the evolving cyber threat landscape and will focus on overseeing and managing the Cyber Security Architecture and Engineering Function.
Key Responsibilities	- Develop and maintain a comprehensive security architecture that aligns with WWU business objectives, its compliance requirements and industry best practice. - Design and implement security solutions for networks, systems, applications and cloud environments as appropriate. - Conduct thorough risk assessments to identify potential security threats and vulnerabilities. - Collaborate with the GRC team to develop strategies for mitigating and managing identified risks. - Evaluate, select and integrate security controls into WWU's IT infrastructure. - Ensure that security controls are effectively implemented and monitored to protect against cyber threats. - Working closely with the relevant IT teams, integrate security measures into the software development lifecycle (SDLC) and existing IT processes that impact cyber security. - Collaborate with enterprise system architects, IT administrators and 3rd party suppliers as appropriate, to ensure security considerations are incorporated into system designs. - Develop and enhance technical incident response plans, ensuring they are aligned with WWU's security architecture. - Collaborate with the incident response team to test and refine incident response procedures. - Stay abreast of cyber security legislation, NIS Regulations and relevant industry standards, making sure security architectures and practices comply with relevant regulatory requirements and industry best practice. - Contribute to WWU's security awareness and training programme to encourage security best practice within WWU. - Evaluate emerging technologies and assess whether their deployment can enhance WWU's security risk profile and posture. - Provide recommendations on adopting new technologies while ensuring fundamental security considerations are addressed.

	- Create and maintain appropriate documentation related to security architecture, including diagrams, policies and procedures. - Ensure that documentation is accessible and understandable for relevant stakeholders.
Technical Skills	- Significant experience with increasing levels of responsibility, ideally some of which has been spent in a CNI security environment. - Experience of working in a complex technical security architecture environment.
Qualifications	<u>Essential:</u> - Bachelor's or Master's degree in Cybersecurity, Information Technology, Computer Science or related field and/or in-depth experience in a comparable position in another organisation. - Extensive experience in cybersecurity roles with a focus on architecture and design. - In-depth knowledge of cybersecurity frameworks, standards, and best practices. - Strong understanding of networking, systems, applications, and cloud technologies. - Excellent analytical and problem-solving skills. <u>Desired:</u> - CISSP - Security Architectural qualifications, such as: - SABSA SCF, SCP, or SCM, - CISSP-ISSAP, - GDSA - General (non-Security) Architectural and IT Governance Qualifications, EG, within TOGAF, COBIT, etc.
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.