Job Title	Cyber Continuity Management Specialist
Department	Cyber Resilience Team
Reports to	Cyber Incident Response Manager
Grade	Technical Tier 1
Purpose & Overview	– The Cyber Continuity Management Specialist (Business Continuity) in Wales & West Utilities (WWU)'s Cyber Resilience Team is responsible for developing and implementing strategies to ensure the continuity of cyber operations in the face of disruptions, incidents or emergencies. This role involves assessing risks, developing cyber continuity plans and collaborating with cross-functional teams to maintain the WWU's cyber resilience. – The role will be fully accountable and responsible for designing and architecting systems and processes ensuring continuity of cyber security functions in the event of a major incident – The Cyber Continuity Management Specialist plays a critical role in minimising the impact of cyber incidents on business operations and supporting WWU's ability to recover effectively. – Reporting to the Cyber Incident Response Manager, this is a key role developing and implementing effective cyber continuity plans, conducting testing and fostering a culture of awareness. The role significantly contributes to WWU's overall cyber resilience. – Strong analytical and communication skills are essential for this role.
Key Responsibilities	– Develop and maintain cyber continuity plans to ensure the availability and resilience of WWU's critical cyber assets and functions. – Design the technical and business and technical architecture for cyber continuity, including infrastructure, applications, communications and business processes – Responsible for assessing and auditing the control effectiveness of recovery and continuity capabilities within WWU. – Collaborate with IT, security, internal audit and business continuity teams to align business continuity efforts with WWU's overall organisational resilience. – Conduct risk assessments specific to business continuity, identifying potential threats and vulnerabilities. – Analyse the impact of cyber incidents on business processes and prioritise mitigation efforts. – Conduct Business Impact Analysis (BIA) to identify critical cyber assets and determine their impact on business operations. – Define recovery time objectives (RTO) and recovery point objectives (RPO) for cyber-related processes and systems. – Integrate cyber continuity plans with WWU's incident response framework. – Collaborate with incident response teams to ensure a coordinated and effective response to cyber incidents. – Develop and execute testing and exercise scenarios to evaluate the effectiveness of business continuity plans.

	– Collaborating with other internal teams, conduct tabletop exercises and simulated cyber incidents, as required, to enhance preparedness. – Coordinate with 3rd parties, such as vendors, to enhance cyber resilience. – Maintain comprehensive documentation of continuity plans, procedures and testing results. – Generate regular reports for senior leaders in WWU as required. – Implement measures to mitigate the impact of technology failures or cyber incidents in WWU. – Continuously assess and improve business continuity plans based on lessons learned from testing, incidents and industry developments. – Stay informed about emerging cyber threats and vulnerabilities. – Ensure business continuity efforts are aligned with all relevant regulatory requirements and industry standards. – Participate in audits and assessments related to business continuity.
Technical Skills	– In depth experience in a similar role, ideally some of which has been spent in a CNI environment. – Architecture of business continuity capabilities to achieve operational resilience
Qualifications	<u>Essential</u>: – ISO 22301 related qualification or certification. – ITIL v4 foundation or higher – Proven experience in business continuity or cyber security roles, with a focus on business continuity planning. – Experience of working in a disaster recovery role or similar – Strong knowledge of cyber threats, vulnerabilities and incident response planning. – Excellent communication and interpersonal skills. <u>Desired</u>: – Bachelor's or master's degree in cyber security, Business Continuity or related field. – Other relevant cyber security certifications such as CISSP or CISM – SABSA or TOGAF Certified Architect
Additional Information	– National Security Vetting to SC level clearance.