Job Title	Cyber Resilience Coordinator
Reports To	Head of Cyber Resilience
Grade	Grade 4

Purpose	This role is a key supporting position within the Cyber Resilience programme, responsible for driving operational excellence and cross-functional coordination across planning, finance, procurement, vendor management, training, and regulatory reporting. This role ensures the successful delivery cyber projects across IT and OT domains, managing multiple budgets and supporting regulatory compliance through structured governance and reporting. Acting as a central point of integration between cyber teams, senior leadership, and other corporate functions, this role enables informed decision-making, optimised resource utilisation, and continuous improvement. This role is critical to maintaining programme momentum, enhancing team capability, and assisting the organisation meets its cyber resilience commitments.

Key Accountabilities	**Coordination & Oversight** • Provide ownership on the planning, execution, and continuous improvement of cyber PCD programme of works, ensuring alignment with key milestones, regulatory obligations, and broader organisational objectives. • Oversee the coordination and reporting of assurance activities—including penetration testing, vulnerability assessments, and tabletop exercises—while ensuring optimal utilisation and governance of all 4 Cyber Call-Off Agreements. • Drive the development, optimisation, and governance of administrative systems and knowledge management platforms (e.g., SharePoint, Verity), ensuring documentation and artefacts are accurate, accessible, and audit-ready. • Deliver high-level operational and administrative support to the senior cyber leadership team. • Establish and monitor key performance indicators (KPIs) to evaluate programme effectiveness, team productivity, and assurance outcomes, driving data-informed decision-making and reporting. **Finance** • Provide financial oversight for the Cyber Resilience programme, working in close with Finance to ensure robust budget planning, forecasting, accrual tracking, and resource allocation across multiple funding streams. • Monitor and support 4 cyber budgets across two cost centres (IT & OT for OPEX and CAPEX), covering the full scope of the cyber programme—over 60 projects—ensuring financial alignment with programme regulatory allowances, internal budgets and objectives. • Work closely with finance to analyse financial performance and variances across projects, providing timely insights and recommendations to senior leadership to support strategic decision-making and optimise resource utilisation. • Coordinate reviews with the support of Finance, preparing detailed reports and dashboards that communicate our current positions. • Act as a key liaison between Cyber teams and Finance, translating technical delivery needs into financial requirements and ensuring funding is aligned to evolving programme demands. **Procurement & Contract Management** • Support the planning, coordination, and execution of all procurement events within Cyber Resilience under the Cyber Procurement Framework. Ensure procurement activities are aligned with regulatory obligations, and objectives. • Ensure all procurement activities adhere to WWU's procurement policies, frameworks, and standards. Maintain documentation and audit trails to be compliant with internal and external requirements. • Establish and maintain robust relationships with external vendors, service providers, and license partners. Act as the primary point of contact for cyber-related engagements, collaboration, resolving issues, and ensuring timely delivery of goods and services. • Where necessary collaborate with internal stakeholders to define requirements, develop evaluation criteria, and manage bid processes. Ensure procurement outcomes deliver best value, mitigate risk, and support strategic cyber objectives. • Ensure procurement decisions are aligned with all cost centres, across Cyber IT and OT, including OPEX and CAPEX. • Lead the tracking and reporting of procurement activities, provide clear and concise updates to senior management and regulatory bodies, including Ofgem,

	ensuring visibility of procurement impact and alignment with programme milestones. **Vendor Management** • Establish and maintain strong working relationships with external vendors and service/license providers. Act as the point of contact for cyber-related engagements, ensuring clear communication, timely delivery, and alignment with organisational goals. • Be responsible for the coordination of vendor onboarding, contract management, and renewals, working closely with Procurement and Legal teams to ensure compliance. • Maintain a view of vendor engagements across cyber, ensuring effective communication between internal teams and external partners. **Cyber Training (L&D)** • Have oversight of the teams continuous learning and development plans for the Cyber Resilience Team, ensuring training programmes are aligned with regulatory PCD expectations, and organisational goals. • Monitor training through feedback using insights to refine delivery methods and delivery with external vendors. • Fully develop and operationalise the Cyber Team's training programme, embedding clear KPIs, structured development, and defined budgetary allowances. **Regulatory & Reporting** • Support the preparation and coordination of high-quality regulatory submissions to Ofgem, ensuring accuracy, clarity, and alignment with programme milestones and requirements. • Be responsible for the production of high-level programme artefacts, including regular PCD project KPIs, dashboards, and performance reports. • Develop and deliver high-level reporting materials, including slide decks and briefing packs to support oversight and decision-making.

Technical Know-How & Skills	• Strong financial knowledge with experience managing multiple budgets and allowances. • Deep understanding of WWU procurement processes and vendor management. • Excellent stakeholder engagement and communication skills. • Strong organisational and analytical skills, with experience in regulatory performance reporting. • Good understanding of Cyber Security, CAF objectives and principles. • Excellent SAP skills
Qualifications	• Professional Accounting Qualification • Certified Information Security Management Principles (CISMP) • Prince2 Agile Project Management • SANS SEC405 • National Security Vetting – SV
Job Dimensions	• Vendor Management –The role holder will liaise with multiple high value vendors within the Cyber Procurement Framework and beyond. • Management of cyber budgets and procurement activities. • Providing high-level administrative support to the senior cyber management team and beyond.