Position description

Position title	Cyber Security Delivery Specialist (Business Analysis)
Group / Branch	*Enterprise Transformation & Delivery / Enterprise Delivery*
Reports to (Title)	Head of Delivery- Enterprise Systems
Competency level	*Individual Contributor*

Job Purpose

The Cyber Security Business Analyst provides specialist cyber security analysis and delivery capability across South East Water's cyber portfolio. The role translates cyber risks, regulatory obligations, security architecture and business needs into clear requirements, delivery plans, control designs and measurable outcomes across initiatives including Identity and Access Management (IDAM), cyber resilience, IT/OT segmentation, detection and response, vulnerability management, secure access, third-party risk and security governance.

Working across Cyber Security, Enterprise Delivery, Architecture, Technology Services, Operational Technology, Risk and Assurance, Procurement, business teams and delivery partners, the role shapes practical and proportionate security outcomes from discovery through implementation and transition to operations. It ensures that security requirements and non-functional requirements are assessed for applicability, agreed early, embedded in procurement and solution design, traced through delivery, validated before go-live and supported by evidence.

The role strengthens South East Water's ability to deliver current and future cyber investments and maintain an audit-defensible security posture. It supports alignment with the Security of Critical Infrastructure Act and Critical Infrastructure Risk Management Program (CIRMP), Victorian Protective Data Security Standards, ASD Essential Eight and Information Security Manual, NIST Cybersecurity Framework, ISO/IEC 27001, privacy obligations and relevant critical-infrastructure and OT security guidance

Key Accountabilities

1. Cyber Portfolio Delivery and Business Analysis

- Lead cyber security analysis and delivery activities across initiatives such as IDAM, privileged access management, IT/OT segmentation, secure access, detection and response, vulnerability management, cyber resilience and third-party security.
- Plan and facilitate discovery, current-state assessment, gap analysis, requirements elicitation, process design, solution options, impact assessment and implementation readiness activities.
- Translate cyber hazards, threat scenarios, architecture principles, policies and regulatory obligations into clear business, functional, non-functional and control requirements.
- Maintain requirements traceability, decisions, assumptions, risks, dependencies, acceptance criteria and evidence from initiation through design, build, testing, deployment and transition to operations.

- Support business cases, initiative canvases, procurement documentation, vendor evaluations, delivery roadmaps, operating models and governance reporting.
- Provide hands-on technical support across cyber infrastructure and networking by reviewing designs and configurations, supporting implementation and troubleshooting, and validating security controls across firewalls, routing and switching, segmentation, secure connectivity, cloud, endpoint, identity, logging and monitoring technologies.
- Work with project managers, architects, engineers, testers, change specialists and vendors to resolve delivery issues and ensure agreed security outcomes are implemented in a practical and sustainable way.

2. Security Requirements, Controls and Assurance

- Apply South East Water's cyber security non-functional requirements and non-negotiable controls using a risk-based, system-criticality and solution-context assessment.
- Engage Architecture early to determine which requirements are mandatory, applicable, desirable or require an approved exception, including for SaaS, cloud, on-premises, legacy and OT solutions.
- Ensure applicable security requirements are considered in business cases and procurement, embedded in contracts and designs, and validated through delivery rather than treated as a late project checklist.
- Cover relevant control domains including identity and privileged access, least privilege, authentication and MFA, encryption and key management, secure configuration, vulnerability and patch management, logging and monitoring, incident response, resilience and recovery, secure development, data protection and third-party security.
- Define acceptance criteria and assurance evidence, support design and control reviews, coordinate security testing and remediation, and confirm residual risks and exceptions are documented and approved before go-live.
- Contribute to reusable cyber requirements, control mappings, patterns, templates and guidance, including ongoing refinement as threats, technology and obligations evolve.

3. Regulatory Alignment and Evidence Readiness

- Support current compliance obligations and future maturity uplift under the SOCI Act and CIRMP by linking cyber initiatives and controls to relevant cyber, personnel, supply-chain and operational hazards.
- Maintain traceability between obligations, risks, controls, requirements, implementation evidence, assurance findings and remediation actions.
- Support alignment to VPDSS, ASD Essential Eight and ISM, NIST Cybersecurity Framework, ISO/IEC 27001, privacy and breach-notification obligations, and relevant critical-infrastructure and OT security guidance such as IEC 62443.
- Prepare clear evidence packs, control status reporting, risk and compliance updates, and decision material for governance forums, audits and assurance reviews.
- Monitor regulatory, policy and framework changes with control owners and help translate them into prioritised delivery actions, roadmap updates and measurable capability improvements.

4. Stakeholder Engagement and Continuous Improvement

- Act as a trusted liaison between cyber specialists, business owners, delivery teams, operational technology teams, risk and assurance functions, procurement and suppliers.
- Communicate complex cyber risks, control gaps, dependencies and recommendations in clear business language for technical and non-technical audiences.

- Facilitate evidence-based decisions, resolve ambiguity and build stakeholder agreement on scope, priorities, risk treatment and implementation responsibilities.
- Support transition to business-as-usual ownership by defining roles, processes, service measures, documentation, training and continuous control monitoring needs.
- Build organisational cyber delivery capability through coaching, knowledge sharing, reusable artefacts and lessons learned.

Knowledge, Skills & Experience

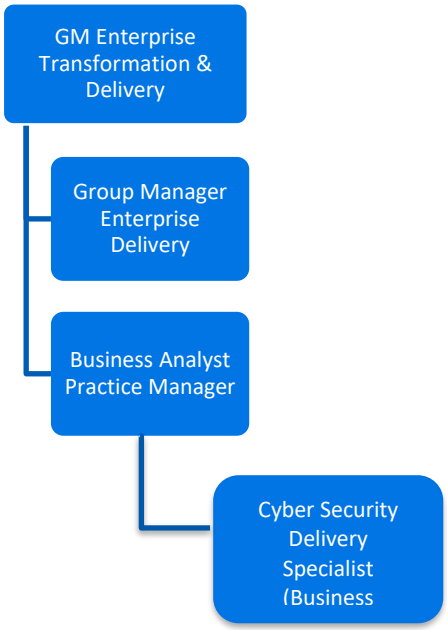
- Substantial experience delivering cyber security initiatives in a complex, regulated environment; experience in critical infrastructure, utilities or operational technology is highly desirable.
- Demonstrated capability across cyber security business analysis and delivery, including discovery, requirements, process and control design, risk assessment, assurance, implementation planning and operational transition.
- Strong practical knowledge of IDAM, IGA, PAM, MFA, joiner-mover-leaver processes, access reviews, service and non-human identities, RBAC, least privilege and identity logging.
- **Demonstrated hands-on technical experience** in cyber security infrastructure and networking, including network architecture, firewalls, routing and switching, segmentation, secure remote access, proxies, DNS, identity integration, cloud connectivity, endpoint security, logging and monitoring. The role must be able to interpret configurations and technical designs, support implementation and troubleshooting, validate that controls operate as intended, and work effectively with infrastructure, network, cloud, security operations and OT engineers across on-premises, cloud and operational technology environments.
- Experience defining and applying cyber security functional and non-functional requirements and integrating them into procurement, contracts, solution design, testing and acceptance.
- Knowledge of the SOCI Act and CIRMP, VPDSS, ASD Essential Eight and ISM, NIST Cybersecurity Framework and ISO/IEC 27001; familiarity with IEC 62443 or other OT security guidance is desirable.
- Ability to map obligations, risks, controls and evidence; assess control gaps; support exceptions and residual-risk decisions; and produce audit-ready documentation and governance reporting.
- Strong stakeholder facilitation, vendor engagement, written communication and executive briefing skills, with the ability to make complex cyber matters clear and actionable.
- Sound judgement, commercial awareness and the ability to balance security outcomes, delivery constraints, operational reliability and cost.

Education and Formal Certifications

- Bachelor’s degree in Cyber Security, Information Technology, Computer Science, Engineering, Business Analysis or a related discipline, or equivalent relevant industry experience.
- Relevant professional certification such as CISSP, CISM, CISA, CRISC or equivalent is desirable.
- Business analysis or delivery certification such as CBAP, CCBA, PMI-PBA, PRINCE2, SAFe or equivalent is desirable.
- Identity, privileged access, cloud security, security architecture or risk and compliance certification is advantageous.
- GICSP, ISA/IEC 62443 or equivalent OT and industrial cyber security certification is advantageous where supporting OT initiatives.

Dimensions

Organisational Chart



Number of people managed:

N/A

Size of budget managed:

N/A

Value of Assets managed:

N/A