South East Water

Position description

Position title	*GRC Assurance Officer*
Group / Branch	*Finance & Technology/BTS*
Reports to (Title)	*Chief Information Security Officer*
Competency level	*Individual Contributor*

Job Purpose

GRC Assurance Officer is responsible to lead South East Water's cybersecurity governance, risk, compliance (GRC) and assurance initiatives. Reporting directly to the CISO, this role is critical in ensuring compliance with regulatory requirements, monitoring cybersecurity risks, and enhancing the SEW's security posture through structured assurance activities. The ideal candidate will have expertise in cybersecurity governance, risk assessments, compliance frameworks, and audit coordination.

Key Accountabilities

- Develop, maintain, and review standards, policies, processes, and procedures to align with security best practices and regulatory requirements.
- Conduct regular reviews to ensure compliance with relevant cybersecurity frameworks, including NIST, VPDSS, and internal security standards.
- Support developing and managing a Common Controls Framework (CCF) to streamline security and compliance controls.
- Conduct regulatory research and interpretation to ensure the SEW complies with evolving laws and industry standards.
- Conduct risk assessments to identify security control gaps, exceptions, and areas for improvement.
- Lead control monitoring activities to ensure security controls are implemented and functioning as intended.
- Oversee Gen AI risk management, ensuring artificial intelligence technologies comply with security and regulatory standards.
- Develop and manage the Cyber Assurance Program, ensuring continuous evaluation of cybersecurity controls and processes.
- Schedule, monitor, and report on assurance activities, ensuring the SEW maintains a strong security posture.
- Coordinate internal and external audits, collaborating with stakeholders to provide necessary evidence and implement corrective actions.
- Ensure Security Awareness Training Compliance Monitoring to verify that all employees meet security education and compliance requirements.

- Serve as a key liaison between security teams, business units, and external regulators on GRC-related matters.
- Provide regular updates and reports to the CISO on cybersecurity risks, compliance status, and assurance activities.

Knowledge, Skills & Experience

- 5+ years of experience in cybersecurity governance, risk, and compliance (GRC) or related functions.
- Strong knowledge of NIST, VPDSS, ISA 62443, ISO 27001, CIS, and other security frameworks.
- Experience conducting risk assessments, control monitoring, and compliance evaluations.
- Familiarity with audit coordination, regulatory compliance, and security assurance programs.
- Excellent communication skills to interact with executives, auditors, technical and non-technical stakeholders.
- Strong analytical and problem-solving skills to assess risks and recommend improvements.
- Experience with GRC tools and platforms for compliance tracking and reporting.
- Knowledge of emerging risks, including AI governance and cloud security compliance.

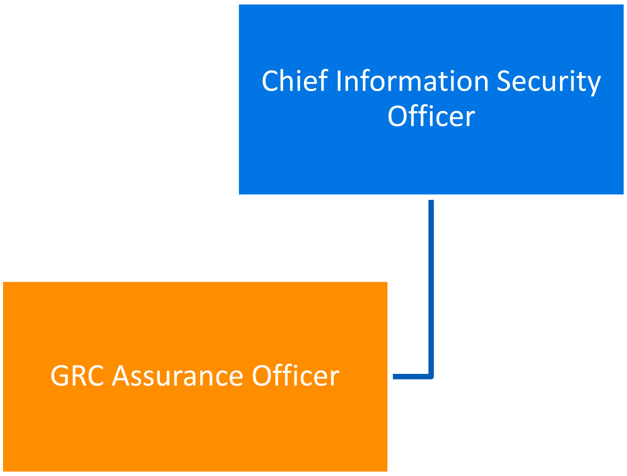
Education and Formal Certifications:

- Bachelor’s degree in Cybersecurity, Information Security, Risk Management, or a related field (or equivalent experience).

- Certifications such as CISM, CRISC, CISSP, CISA, or ISO 27001 Lead Auditor.

Dimensions

Organisational Chart



Number of people managed: N/A

Size of budget managed: N/A

Value of Assets managed:

Describe the level/type of responsibility the role has over the organization's assets, both physical and non-physical

Ensuring a sustainable, resilient organisation:

Authorities outlined in **Instrument of Delegations** None

Compliance management responsibilities outlined in the **compliance and obligations register** None

Security for Critical Infrastructure identified role: No