# Position description

| | |
|---|---|
| **Position title** | *Manager - Cyber and Device Security* |
| **Group / Branch** | *Iota* |
| **Reports to (Title)** | *Product Director* |
| **Competency level** | *Individual Contributor* |

## Job Purpose

This position is responsible for leading and managing the delivery of Iota's cyber and device security initiatives and processes to approved schedule, budget, scope and quality while meeting business outcomes and security objectives.

## Key Accountabilities

Iota is a subsidiary of South East Water and is responsible for the commercialisation of technology and devices developed by South East Water.

The Manager – Cyber and Device Security role sits within Iota's Product Team and reports directly to the Product Director. The Product Team oversees key functions including product development, solution architecture, and customer delivery.

This role is responsible for ensuring the cybersecurity of Iota's products throughout their lifecycle, particularly in relation to customer deployments such as South East Water and other water authorities.

Key responsibilities include leading the delivery of cybersecurity initiatives, managing internal and external stakeholders, coordinating with vendors, overseeing communication strategies, and maintaining control over risk, schedules, and budgets.

The successful candidate will possess a strong understanding of business requirements across diverse stakeholder groups and deliver solutions that effectively mitigate cybersecurity risks in a dynamic and evolving environment.

This role is accountable for:

**Cybersecurity Delivery & Governance**

- Lead internal and external cybersecurity initiatives, ensuring delivery on time, within budget, and to quality and compliance standards.
- Establish governance frameworks including risk management, reporting, and issue tracking.
- Prepare business cases and documentation to support cyber initiatives and secure funding.

**Security Architecture & Strategy**

- Develop and maintain a security architecture blueprint aligned with business goals, technology strategy, and threat landscape.
- Define scope and objectives for cyber roadmap initiatives in line with enterprise priorities.
- Implement and validate security controls using frameworks such as NIST, SOC2, IEC62443, OWASP, and Essential 8.

**Threat & Risk Management**

- Monitor emerging threats and assess their impact on Iota and its customers.
- Manage penetration testing and remediation across platforms and devices.
- Ensure compliance with regulatory requirements and mitigate third-party and operational risks.

**Stakeholder & Vendor Engagement**

- Build strong relationships with internal teams and external partners including South East Water.
- Collaborate with BTS, OT, Risk, Legal, and Procurement to manage dependencies and drive change.
- Source, negotiate, and manage vendors supporting cybersecurity initiatives.

**Secure Development & Incident Response**

- Embed security into platforms and devices through collaboration with architects, SMEs, and development teams.
- Promote secure coding practices, DevSecOps, and secure data governance.
- Support incident response with technical expertise and remediation guidance.

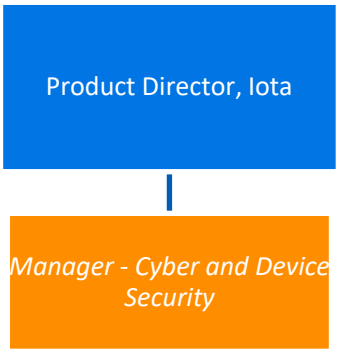
# Knowledge, Skills & Experience

- Proven experience delivering complex cybersecurity programs end-to-end.
- Strong understanding of threat landscapes and risk mitigation strategies.
- Expertise in designing and maintaining security architecture.
- Practical knowledge of frameworks like NIST, SOC2, IEC62443, OWASP, and Essential 8.
- Skilled in engaging cross-functional teams and external partners.

- Experience sourcing, negotiating, and managing cybersecurity vendors.
- Deep understanding of regulatory requirements and compliance standards.
- Ability to ensure alignment across platforms, devices, and customer environments.
- Familiarity with DevSecOps, secure coding, threat modelling, and secure data governance.
- Ability to embed security into development lifecycles and validate controls.
- Hands-on experience supporting security incidents and remediation.
- Ability to assess vulnerabilities and manage penetration testing outcomes.
- Strong skills in roadmap planning, business case development, and program governance.
- Capable of managing budgets, schedules, risks, and reporting.

# Dimensions

## Organisational Chart




## Number of people managed:

This role has zero direct reports. Potential for external vendor team management.

## Size of budget managed:

Budget management is related to the Instrument of Delegations and business case approval limits.