Cyber & Information Security Architect

# Reporting To

Head of Cyber & Information Security

# Role Purpose

This role is responsible for defining and guiding the implementation of cyber and information security architecture across the organisation and customer environments.

The post holder will lead the development of technical security standards, provide architectural assurance, and support secure design and delivery of critical infrastructure services.

The role requires deep technical expertise, strategic thinking, and strong stakeholder engagement skills. It involves working across IT, DevOps, and Cyber functions to embed secure-by-design principles, support change control processes, and ensure compliance with ISO27001, NIST CSF, and contractual obligations.

# Key Responsibilities

Define and maintain cyber and information security architecture standards aligned to policy, regulatory, and industry frameworks.

Lead the design of secure solutions and technical controls across infrastructure, applications, and data.

Provide architectural assurance and act as the security approver in change control processes.

Collaborate with IT Ops and DevOps teams to embed DevSecOps principles and secure development practices.

Deliver technical consultancy and security architecture support for customer projects.

Monitor emerging threats and advise on appropriate countermeasures.

Promote adoption of consistent security patterns and technical standards across the organisation.

Support the development of secure NOC services in collaboration with hyperscalers and telecoms providers.

# Required Experience

Proven experience in cyber security architecture roles within complex environments.

Strong understanding of ISO27001, NIST CSF, and enterprise security frameworks.

Experience designing and implementing security controls across hybrid infrastructure and cloud platforms.

Ability to influence senior stakeholders and lead cross-functional collaboration.

Familiarity with secure development practices and DevSecOps methodologies.

Experience in risk management, solution architecture, and enterprise architecture.

Excellent communication and stakeholder engagement skills.

# Desirable Skills & Knowledge

Demand management, strategic planning, IT infrastructure, and information assurance.

Data protection, governance, audit, and quality management.

Experience with Azure, Microsoft 365, and hyperscaler environments.

Certifications such as CRISC, CISA, ISO 27001 Internal Auditor, CCSK, CCSP, MS-500.

# Qualifications

Essential:

- CISM and/or CISSP

- Azure Solutions Architect (AZ-305) and/or Microsoft Cybersecurity Architect (SC-100)

Desirable:

- CRISC, CISA, ISO 27001 Internal Auditor, CCSK, CCSP, Microsoft 365 Security Administrator (MS-500)

# Key Performance Indicators (KPIs)

Adoption of security architecture standards across projects and platforms.

Quality and completeness of architectural assurance and change control documentation.

Stakeholder satisfaction and engagement in security design processes.

Reduction in risk exposure and alignment to compliance requirements.

Timely delivery of secure solutions and technical consultancy.

# SFIA 9 Skill Alignment

|  |  |  |  |
| --- | --- | --- | --- |
| **Skill** | **Code** | **Level** | **Description** |
| Information Security | SCTY | 6 | Defines and governs security architecture and policy. |
| Solution Architecture | ARCH | 6 | Leads development of secure solution architectures. |
| Enterprise & Business Architecture | STPL | 6 | Aligns technology strategy with business objectives. |
| Risk Management | BURM | 6 | Leads organisation-wide risk management processes. |
| Requirements Definition & Management | REQM | 6 | Drives requirements definition and prioritisation for complex initiatives. |
| Stakeholder Relationship Management | RLMT | 6 | Builds strategic relationships and manages stakeholder engagement. |
| Data Management | DATM | 6 | Leads data governance and master data management. |
| Change Management | CHMG | 5–6 | Supports secure change control and impact analysis. |
| Security Governance | GOVN | 6 | Ensures compliance with security policies and standards. |