POSITION DESCRIPTION

Principal Cyber Solutions Architect

POSITION DETAILS

Position Title	Principal Cyber Solutions Architect
Classification	HEW 9
Position Number	NEW
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

This role leads the design and governance of secure, scalable, and resilient cyber solution architecture solutions that underpin the University's digital ecosystem. It provides expert guidance on cyber solution design, contributes to enterprise architecture strategy, and ensures alignment with cybersecurity frameworks and compliance obligations. The role supports the University's strategic goals by enhancing digital trust, operational continuity, and cyber maturity.

This role also plays a critical role in embedding secure-by-design principles across all technology domains, enabling innovation while safeguarding information assets.

KEY ACCOUNTABILITIES

- Design and implement enterprise cyber architecture solutions that align with security frameworks and support scalable digital infrastructure.
- Guide the integration of cybersecurity controls into digital platforms, applications, and cloud environments to ensure compliance and resilience, informed by threat modelling and MITRE ATT&CK.
- Collaborate with enterprise architects and IT delivery teams to embed secure-by-design principles into technology roadmaps, solution lifecycles including reference architectures and Architecture Decision Records (ADRs).
- Evaluate emerging technologies and threat landscapes to inform architectural decisions and risk mitigation strategies.
- Develop and maintain architecture standards and patterns that reflect best practice in cybersecurity and digital service delivery.
- Provide expert advice to senior stakeholders on architectural risks, trade-offs, and mitigation strategies.
- Contribute to strategic planning and governance forums to ensure alignment between cyber

architecture and institutional priorities.
- Maintain high standards of documentation and knowledge sharing to support operational continuity and capability uplift.
- Lead security design assurance activities across the solution delivery lifecycle, ensuring alignment with risk appetite and enterprise controls.
- Partner with compliance and audit functions to ensure architectural controls meet regulatory and internal assurance requirements.

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Postgraduate qualifications in Cybersecurity, Information Technology, or a related field, or equivalent professional experience.
- Extensive experience in designing and implementing cyber architecture within complex digital environments.
- Deep knowledge of security frameworks (e.g., NIST SP800-53, ISO 27001), cloud security, and enterprise architecture methodologies.
- Proven ability to influence architectural decisions and lead secure solution design across diverse technology platforms.
- Strong stakeholder engagement and communication skills, including the ability to translate technical concepts for non-technical audiences.
- Demonstrated capacity to contribute to strategic initiatives and drive continuous improvement in cybersecurity practices.
- Demonstrated experience integrating cyber controls across multi-cloud and hybrid environments.
- Strong understanding of secure software development practices and DevSecOps principles, including CI/CD security controls

Technical Proficiency

- Proficiency in enterprise architecture tools (e.g. ArchiMate, TOGAF), cloud platforms (e.g. AWS, Azure), and CI/CD pipelines.
- Working knowledge of Zero Trust architectures and identity & access management (IAM) design.
- Data security (discovery/classification, DLP, encryption, KMS) and observability (centralised logging, SIEM content requirements, detection hand-offs to SOC).

Desirable

- Industry certifications such as SABSA, TOGAF, AWS/Azure Security, or CISSP.
- Experience in higher education, government, or regulated sectors.

KEY RELATIONSHIPS

This position reports to: Manager, Governance, IT Risk and Assurance

This position supervises: None, but may mentor more junior members

Key internal relationships:

- Enterprise Architecture
- IT Delivery and Operations
- Cybersecurity and Risk Assurance
- Legal and Compliance
- Academic and Professional Units

Key external relationships:

- Cybersecurity vendors and consultants
- Regulatory bodies
- Industry forums and architecture communities

CHALLENGES

- Balancing security, usability, and performance in solution design across diverse platforms and stakeholder needs, while aligning to risk appetite and total cost of control.
- Navigating complex regulatory and compliance requirements in a rapidly evolving threat landscape.
- Embedding secure-by-design principles in fast-paced digital delivery environments, using threat modelling and Zero Trust patterns within agile/iterative delivery.
- Influencing architectural decisions across distributed teams and legacy systems, including federated research environments, while maintaining privacy and ethics requirements.

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

SFIA Capability	Code	Level	Rationale
Solution architecture	ARCH	6	Leads design of secure architecture aligned to enterprise strategy and security requirements.
Information security	SCTY	6	Ensures security controls are embedded in digital solutions and cloud environments.
Enterprise IT governance	GOVN	6	Participates in governance forums to align architectural direction with business risk posture.
Innovation	INOV	5	Assesses emerging technologies and contributes to secure innovation.
Systems integration	SINT	5	Oversees secure integration of applications, APIs, and infrastructure platforms.
Stakeholder relationship management	RLMT	6	Advises senior stakeholders and influences decisions on architecture trade-offs and risks.
Methods and tools	METL	5	Develops and maintains reusable architecture methods, tools, and patterns.
Security administration	SCAD	5	Designs and validates secure configurations and access controls across platforms.
DevSecOps (mapped to Programming/Software Engineering and related SFIA capabilities)	PROG / SWDN	4–5	Supports secure software delivery through architectural guidance on DevSecOps practices.

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

→ Code of Conduct
→ Work Health and Safety and Wellbeing Management System
→ Enterprise Agreement or Award
→ Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by:

Date: