POSITION DESCRIPTION

Manager – Governance, IT Risk and Assurance

POSITION DETAILS

Position Title	Manager – Governance, IT Risk and Assurance
Classification	HEW 9
Position Number	NEW
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

This role leads the Governance, Risk & Assurance (GRA) portfolio within ITDS Security & Digital Operations. As part of Line 1, it ensures cyber and IT risks are effectively governed, managed, and assured within ITDS, providing confidence to institutional leadership, Audit & Risk Committee, and regulators that controls are fit-for-purpose and operating effectively. The role spans governance and policy alignment, Line 1 IT risk management and cyber assurance, assurance testing (design/document reviews, penetration testing, red teaming, control validation), cyber security architecture (secure-by-design oversight), and cyber awareness & engagement.

The position is responsible for embedding strong risk practices, secure-by-design principles, and a positive cyber culture across the University, while ensuring ITDS remains aligned with NIST CSF 2.0 and best practice standards and within the University's risk appetite.

It also provides strategic leadership across a complex and evolving regulatory environment, ensuring the University maintains an effective, risk-aware culture and meets its obligations as a custodial steward of critical digital assets.

The role operates as a trusted advisor to the CISO and contributes to University-wide governance and risk forums. The role reports directly to the Executive Director, Security & Digital Operations (CISO).

KEY ACCOUNTABILITIES

Risk & Assurance

- Develop and maintain the ITDS GRC framework (including policies, standards and procedures), the Line-1 control library, and risk/issues registers, ensuring alignment with NIST CSF 2.0, best-practices, and the University's risk appetite.

- Oversee the Line-1 assurance plan and control testing program mapped to NIST CSF 2.0 functions/categories, ensuring findings are risk-rated, assigned owners, tracked to closure, and validated.
- Define, monitor and report KRIs/KPIs, control-effectiveness metrics, and cultural metrics to CISO, ITDS leadership, and governance committees.
- Build strong partnerships with Line 2 Risk & Compliance, Line 3 Audit, and external regulators, ensuring alignment, transparency, and credibility of ITDS assurance activities.

Architecture & Secure-by-Design

- Lead solution security architecture oversight, embedding secure-by-design principles and reference architectures, patterns, and guardrails into technology roadmaps and projects.

Provide strategic advice to ITDS leaders on emerging risks, compliance obligations, and mitigation strategies, with emphasis on third-party and outsourcing risks.

Culture & Awareness

- Lead the cyber culture, awareness and engagement program, shaping behaviours, training and targeted campaigns that uplift cyber resilience across staff, students, and partners.
- Foster collaboration with internal stakeholders and external partners to enhance cyber resilience, culture, and operational effectiveness.

Governance & Engagement

- Integrate governance, risk management, assurance, architecture oversight, and culture into a unified strategy that supports institutional priorities.
- Manage and develop direct reports, ensuring alignment with ITDS objectives, regulatory obligations, and risk appetite.
- Translate complex risk and technical insights into clear advice for senior leadership, Board committees, and sector forums, while contributing to governance initiatives (e.g., incident readiness, business continuity, lessons learned).

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Tertiary qualifications in Information Technology, Cybersecurity, Risk Management or a related field, or equivalent professional experience.
- Postgraduate qualifications or professional certifications in risk management (e.g., Certified Risk Manager, ISO 31000, or equivalent) are highly regarded.
- Extensive experience in governance, risk, and assurance leadership roles within complex organisations, ideally higher education, government, or financial services.
- Experience managing cross-functional GRA teams with competing strategic and operational priorities.
- Proven expertise in cyber and enterprise IT risk management frameworks, particularly NIST CSF 2.0 (primary), ISO/IEC 27001/27005, ISO 31000, ACSC Essential Eight, and related standards.
- Proven expertise in cyber and enterprise IT risk management frameworks, particularly NIST CSF 2.0 (primary), with strong working knowledge of ISO/IEC 27001/27005, ACSC Essential Eight, and related standards.
- Demonstrated experience in leading or overseeing assurance testing programs
- Strong knowledge of enterprise architecture and secure-by-design principles, with the ability to integrate security into technology roadmaps and projects.
- Experience in cyber culture, awareness, and engagement programs, including training, communications, and stakeholder behaviour change.
- Excellent leadership skills, with a record of accomplishment of building and developing high-performing specialist teams.

- Outstanding communication and stakeholder engagement skills, with the ability to translate technical and risk concepts for executive and governance audiences.
- Demonstrated ability to provide strategic advice to senior leaders on emerging risks, compliance obligations, and mitigation strategies.
- Proven ability to integrate Line 1 risk functions with broader institutional risk governance structures and forums. Commitment to University values of boldness, integrity, fairness and excellence.
- Requirement to obtain and maintain any clearances necessary to perform the role *(including, but not limited to, a NSW Police Force Professional Suitability clearance).*

Technical Proficiency

- Deep understanding of GRC tools and platforms.
- Familiarity with security operations and architecture methodologies, including threat modelling, control validation, red/purple teaming, and control design/effectiveness reviews.
- Proficiency in interpreting and applying cyber-specific regulatory standards such as ISO 27001, NIST CSF, ACSC Essential 8, ISM, and PSPF.

Desirable

- Relevant certifications such as CISM, CISA, CRISC, CISSP, SABSA, CGEIT, ISO/IEC 27001 Lead Implementer/Auditor, or FAIR (Factor Analysis of Information Risk).
- Experience in delivering Line 1 assurance within a three lines-of-defence model.
- Prior experience working with Boards or subcommittees (e.g., Audit & Risk).
- Active participation in cyber governance, risk management, or assurance forums.
- Understanding of sector-specific risks, including higher education cyber threats, regulatory obligations, and critical infrastructure requirements.

KEY RELATIONSHIPS

This position reports to: Executive Director, Security & Digital Operations (CISO)

This position supervises:

- Principal Cyber Solutions Architect
- Specialist IT Assurance Analyst & Testers
- Specialist Risk Advisor
- Specialist Cyber Awareness & Engagement Advisor

Key internal relationships:

- IT & Digital Services
- Enterprise Architecture and Project Delivery teams
- Risk, Audit and Compliance
- Office of General Counsel
- Academic and Professional Units

Key external relationships:

- Technology vendors and consultants
- Regulatory bodies
- Assurance Providers
- Industry networks and forums

CHALLENGES

- Delivering a broad governance, risk, and assurance portfolio through a focused team of senior specialists, requiring clear prioritisation, sequencing, and effective delegation.
- Ensuring integration and alignment between diverse functions so they operate as a cohesive unit.
- Balancing strategic leadership and oversight with maintaining visibility of operational detail across specialist domains.
- Providing credible, evidence-based assurance to executive, board, and governance committees that reflects both technical depth and strategic context.
- Leveraging external vendors, internships and sector partnerships (e.g., for penetration testing, red teaming, and awareness programs) to complement internal capability and extend outcomes.
- Staying ahead of evolving regulatory, compliance, and sector obligations
- Translating technical assurance, cultural insights, and architectural findings into clear strategic advice that informs decision-making at the senior leadership and governance levels.
- Driving continuous uplift in maturity and embedding secure-by-design principles, measurable KRIs/KPIs, and a positive risk-aware culture across the University

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

SFIA Capability	Code	Level	Rationale
Information assurance	INAS	6	Leads university-wide assurance functions to assess cyber control effectiveness, **validate remediation outcomes**, and provide confidence in digital governance.
Risk management	BURM	6	Designs and maintains frameworks aligned to risk appetite, regulatory standards, and institutional policy, owning the ITDS risk register, control library, and KRIs.
Governance	GOVN	6	Leads governance strategy for cyber and IT risks, operating at the interface of Line 1 and University-level governance.
Solution architecture	ARCH	6	Provides strategic oversight of secure-by-design principles and cyber architecture within broader ITDS planning, via reference patterns and guardrails.
Security testing	PENT	5	Oversees the assurance testing strategy (penetration testing, red/purple teaming, vulnerability reviews), ensuring findings are risk-rated, prioritised, tracked, and validated; delivery delegated to specialists and vendors.
Measurement	MEAS	5	Tracks KRIs and KPIs for risk and assurance performance, providing data for leadership reporting and trend analysis.
Stakeholder relationship management	RLMT	6	Interfaces with senior stakeholders including the Board, CISO, audit and regulatory partners.
People management	PEMT	6	Leads a multidisciplinary team spanning three specialist functions with different operating rhythms.

Learning and development management	ETMG	5	Leads awareness and cultural uplift initiatives across the University though not a formal L&D function owner.
Compliance	COMP	5	Ensures cyber activities align with standards, though ownership of compliance frameworks sits within Line 2.

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: