PROFESSIONAL STAFF
POSITION DESCRIPTION

VICTORIA UNIVERSITY

Risk and Assurance Coordinator

HEP Level 8

POSITION NUMBER	954750
ORGANISATIONAL UNIT	Digital and Campus Services (DCS) --> Office of the Chief Information Security Officer (CISO)
POSITION REPORTS TO	Chief Information Security Officer (CISO)
OVERALL PURPOSE	The **Risk and Assurance Coordinator** plays a critical role in supporting the identification, coordination and management of risk and assurance activities across the Digital and Campus Services (DCS) portfolio. Working in close partnership with portfolio leadership, DCS business units and the Enterprise Risk & Compliance team, this role helps to build and mature integrated governance, risk, compliance, and assurance practices spanning digital infrastructure, cyber security, physical security, data platforms, projects, and operations (including third party risk and technology risk management). The coordinator ensures DCS maintains a clear and current view of its operational and strategic risk landscape, including risks related to technology, infrastructure, third-party suppliers and people. Acting as a trusted advisor, the role drives risk transparency, supports compliance, and enables informed decision-making through structured assessments, effective reporting, and ongoing controls assurance. It also contributes to the development and enforcement of strong risk and security practices across university operations and strategic programs, including the definition of key risk indicators, policies, standards, and governance processes.
ORGANISATIONAL CONTEXT AND RELATIONSHIPS	**Within the University the position:** ◆ Reports to the CISO ◆ Works closely with the Enterprise Risk & Compliance team, Cyber Security, Legal, Internal Audit, Procurement and all teams within DCS. ◆ Provides guidance and coordination to project managers, people leaders and operational staff within DCS on risk-related matters. ◆ May be required to engage with vendors, service providers, and external stakeholders during risk assessments or audits.
LOCATION/CAMPUS	The position is currently located at the Footscray Park Campus of the University. The position and incumbent may be relocated to any other existing or future University work locations where it conducts its operations.

KEY CAPABILITIES

Victoria University is committed to building core capability across VU through investment in our staff, our systems and our processes. We will develop the capabilities of our staff to:

Deliver - Excellence Results-driven, accountability, problem solving focus.

Engage - Customer service mind-set internally, externally and particularly for students.

Collaborate and Partner - Build successful relationships, communicate effectively, influence and negotiate.

Innovate - Entrepreneurship, growth, continuous improvement, digital transformation.

Lead - Inspire direction, lead change, manage and develop people.

OUR ORGANISATION

Victoria University (VU) is a dual sector (higher education and TAFE) tertiary institution based in Melbourne, Australia. VU has academic colleges, each covering a broad discipline of study, and several research institutes and research centres. The University has campuses in Melbourne's CBD and western region, and a campus in Sydney and Brisbane. It also offers courses at partner institutions throughout Asia. Over 40,000 students, including around 14,000 international students, study VU courses worldwide. In 2016, VU celebrated its 25th anniversary as a university, which also marked its 100 years as an educational institution.

Commitment to Protecting Country:

Victoria University honours its deep diversity as a foundation for collaboration and social progress. We will demonstrate sensitivity in respecting First Nation perspectives. We will ensure that we respect our Indigenous voices and commit to sustainable Protecting Country. We will take leadership responsibility, in all that we do, to improve the health and wellbeing of our local and global communities, and the planet that we share.

Commitment to Diversity and Inclusion at VU:

Victoria University believes that diversity of the workforce adds value to the University and creates a stronger, richer working environment for everyone. We are committed to making reasonable adjustments to ensure that our employees have positive, barrier-free work environments that accommodate their access needs. Employees who require adjustments are encouraged to discuss their needs with their line manager.

ORGANISATIONAL UNIT

Victoria University's Digital and Campus Services department is focused on high quality customer engagement with a service excellence and innovation mindset, implementing process enhancements that will drive better outcomes for students, staff and our extended community as we seek to be relentlessly customer centric. Digital and Campus Services is responsible for modernising technology platforms and the University's infrastructure on a comprehensive scale to ensure VU is a thriving place to study and work. Working closely with our customers and suppliers, we provide workforce solutions in areas including infrastructure, data, application development, digital solutions and innovation. This portfolio includes:

- Business Partnering and Governance
- Enabling Technology
- Office of the Chief Information Security Officer (CISO)
- Estate Management and Campus Security
- Campus Services
- AI Technology and Delivery

MAJOR TASKS AND ACCOUNTABILITIES

- Implement and mature the risk management framework within the DCS portfolio, including support for localised frameworks and processes to manage operational risks, while ensuring alignment with the University's enterprise-wide risk policies and appetite.
- Support the proactive identification, assessment, and documenting of risks across all DCS domains, including projects, systems, infrastructure, and third-party suppliers.
- Provide technical advice on designing effective control environments across DCS and manage a controls assurance program to monitor ongoing effectiveness.
- Act as a trusted advisor to DCS leadership and project teams, offering practical, timely expertise on technology, cyber security, physical security, and infrastructure risk.
- Champion a positive risk culture across DCS, embedding governance, risk and compliance principles into daily decision-making and driving risk awareness.
- Lead third-party risk management and assurance activities for DCS, ensuring consistent evaluation of vendor and partner risks aligned with University’s centralised standards.
- Ensure DCS initiatives and operations meet the University's regulatory obligations including but not limited to the NIST Cybersecurity Framework, Security of Critical Infrastructure Act (SOCI), Australian Privacy Principles (APP), and TEQSA requirements.
- Collaborate with the CISO to enhance and maintain threat-informed risk models that effectively articulate cyber and digital risks relevant to DCS operations and assets.
- Contribute to the development and continuous improvement of the University's Information Security Management System (ISMS), driving its implementation and adoption within DCS.
- Drive the continuous improvement and maturity of risk management practices by enhancing policies and procedures and incorporating emerging threats and assurance methodologies.
- Translate changes in the external regulatory and threat landscape into actionable insights and guidance for DCS leadership and stakeholders.

TYPICAL/MAJOR CHALLENGES

- Balancing diverse and sometimes competing priorities across the DCS portfolio, while fostering shared accountability for risk at all levels.
- Translating complex technical or operational risks into clear, actionable insights for a wide range of stakeholders.
- Promoting a forward-looking and proactive approach to risk identification amidst an evolving threat and regulatory landscape.
- Staying current with relevant legislation, regulatory changes, and emerging best practices in risk, assurance and information security.
- Exercising sound independent judgment and initiative while also contributing to collaborative decision-making processes across Digital and Campus Services.
- Clearly documenting, assessing, and communicating risks, exposures and control measures in a structured and effective manner.

LEVEL OF SUPERVISION

Operates under broad direction from the Chief Information Security Officer and may be required to manage other administrative, technical and/or professional staff**.**

PROFESSIONAL AND ORGANISATIONAL KNOWLEDGE

- Demonstrated expertise in security risk management, governance and reporting frameworks with strong knowledge of standards such as NIST CSF, COBIT 5, ISO27000 series and ISO31000.
- Holds or is working towards relevant industry certifications (e.g. SANS LDR519, ISACA CRISC) that reflect a commitment to ongoing professional development.
- Strong analytical and problem-solving capabilities complemented by highly effective communication and presentation skills.
- Sound understanding of legislative and regulatory obligations relevant to the role, with a preference for familiarity with the University-specific legislation and compliance frameworks.
- Ability to develop in-depth knowledge of University’s operations, governance structures and decision-making processes, including quality assurance and other applicable regulatory requirements.

KEY SELECTION CRITERIA

Essential

1. Knowledge or Training equivalent to: Post graduate qualifications or progress towards postgraduate qualifications and extensive relevant experience, or extensive experience and management expertise, or an equivalent combination of relevant experience and/or education.
2. Minimum three years' experience with Information Risk analysis and Management, and / or Enterprise Risk and Assurance, compliance or governance roles, preferably within a complex, multi-disciplinary environment.
3. Proven ability to coordinate and support risk assessments, assurance activities and compliance reviews across diverse business areas, including technology and operational services.
4. Strong working knowledge of risk management and compliance frameworks (e.g., ISO 31000, ISO 27001, NIST CSF) and relevant regulatory environments.
5. Demonstrated experience working with policies, controls, or standards, including documenting, assessing, and reporting risks and issues and ability to make recommendations on actions required to close out audit items
6. Ability to translate complex or technical information into clear, actionable insights for business and operational stakeholders.
7. Highly developed written and verbal communication skills with a proven ability to influence, collaborate, and present across all levels of the organisation.
8. Demonstrated capacity to work both independently and collaboratively, managing competing priorities with attention to detail and sound judgement.
9. Commitment to university policies and practices, including OH&S, equity and diversity, and ongoing professional development.

Desirable

10. Prior experience contributing to risk assurance in higher education sector or regulated industries (e.g. education, health, finance or critical infrastructure).
11. Familiarity with cyber and physical security risks and how they align with enterprise risk practices.
12. Experience working in large or complex organisations, with exposure to enterprise-level risk management practices.