Make it matter.

POSITION DESCRIPTION

Cyber Security Risk Manager

Faculty/Division	Division of Operations
Classification Level	Professional TFR
	G - Administrative, Clerical, Computing, Professional &
Hours & Span (Category)	Research Staff
Position number	ADMIN ONLY
Shiftwork status	NOT SHIFTWORKER
Allowances	NOT APPLICABLE
On call arrangements	NOT APPLICABLE
Original document creation	25 September 2024

Position Summary

The Cyber Security Risk Manager is responsible for providing strategic leadership in developing and continuously improving the University's cyber security risk management practices, ensuring that risks are continually identified, assessed, prioritised, monitored, and mitigated in line with UNSW's Enterprise Risk Management framework. Key responsibilities include managing cyber security risk registers, leading risk remediation efforts, and developing risk mitigation strategies with measurable key risk indicators (KRIs) and key performance indicators (KPIs). The role also oversees vendor security risk management and annual threat assessments, while delivering regular risk updates to senior leadership and governance forums.

The Cyber Security Risk Manager reports to the Head of Cyber Security Governance & Assurance and has direct reports.

Accountabilities

Specific accountabilities for this role include:

- Provide strategic leadership in the development, execution and continuous improvement of the cyber security risk management practices in alignment with UNSW's Enterprise Risk Management framework.

- Manage Cyber Security Risk Registers, ensuring identified risks are documented, assessed, prioritised, and remediated.
- Lead and direct risk remediation efforts, ensuring timely closure of identified risks.
- Develop and implement effective risk mitigation strategies and ensure alignment with business goals.
- Develop key risk indicators (KRIs) and key performance indicators (KPIs) to measure and track the effectiveness of risk management strategies.
- Ensure new risks are promptly registered and managed following assessments, assurance activities, or security incidents.
- Ensure that the threat, risk and control libraries on the GRC platform are up to date.
- Lead the execution, and continuous improvement of the annual threat and risk assessment process, including maturity assessments
- Lead and deliver the end-to-end vendor security risk management lifecycle process, including annual risk assessments for high-risk vendors, periodic scorecard reviews, and continuous monitoring through platforms such as UpGuard, CyberGRX and BitSight.
- Oversee and deliver the security review process for Requests for Information (RFIs) and Requests for Proposals (RFPs), embedding contractual security requirements in vendor agreements.
- Design and optimise operational metrics to drive continuous improvement of the overall cyber security risk management practice, ensuring timely and accurate reporting through the metrics dashboard for inclusion in the quarterly Risk and Safety Committee submissions.
- Lead the development and delivery of quarterly cyber security risk updates and briefings to IT executives, business partners, and relevant stakeholders, providing detailed insights into risks and mitigation action status and trends.
- Present quarterly risk reports at governance forums, including the GRC Community of Practice (CoP) and Vendor Security Risk Management CoP, while also serving as a subject matter expert on cyber security risk management.
- Lead and manage the Cyber Security Risk Working Group, fostering cross-functional collaboration and driving key security risk management initiatives.
- Monitor internal and external environments for emerging threats, vulnerabilities, and regulatory changes.
- Provide strategic cyber security consulting and advisory services to the Cyber Security Enablement Program and other key initiatives across the University, ensuring alignment with governance and compliance standards.
- Align with and actively demonstrate the Code of Conduct and Values
- Cooperate with all health and safety policies and procedures of the university and take all reasonable care to ensure that your actions or omissions do not impact on the psychosocial or physical health and safety of yourself or others.
- Ensure hazards and risks psychosocial and physical are identified and controlled for tasks, projects, and activities that pose a health and safety risk within your area of responsibility.

Skills and Experience

- Extensive experience (7+years) in cyber security risk management, with demonstrated experience in conducting risk assessments, managing risk registers, and overseeing vendor security risk management programs.
- Proven experience in developing, implementing and operationally running the cyber security risk management practice in large and complex organisations.
- Hands on experience with security tools and platforms for monitoring, managing, and reporting on cyber security risks such as Protecht GRC tool, CyberGRX, UpGuard, and BitSight is highly desirable.
- Certifications such as CISM, CISSP, CRISC, AWS Security Speciality, Azure Security or related certifications are highly desirable.
- Strong knowledge of cyber risk management principles, methodologies, frameworks, such as ISO 27001, ISO 31000, NIST 800-53, FAIR and other industry standards.
- Proven experience in managing vendor security risk and developing operational metrics for risk management.
- Strong project management skills with the ability to balance multiple initiatives and deadlines.
- Excellent communication, negotiation and interpersonal skills, with a proven ability to develop effective relationships and influence key stakeholders at all levels in the organisation.
- Ability to present with credibility and translate technical and complex information concisely for diverse audiences using strong analytical and problem-solving skills.
- Demonstrated experience in presenting risk reports and providing strategic advice on cyber security risk management to senior leadership.
- High level of motivation, resilience, and ability work independently and within a team setting.
- An understanding of and commitment to UNSW's aims, objectives and values in action, together with relevant policies and guidelines.
- Knowledge of health & safety (psychosocial and physical) responsibilities and commitment to attending relevant health and safety training.

Pre-employment checks required for this position

- Verification of qualifications

About this document

This Position Description outlines the objectives, desired outcomes, key responsibilities, accountabilities, required skills, experience and desired behaviours required to successfully perform the role.

This template is not intended to limit the scope or accountabilities of the position. Characteristics of the position may be altered in accordance with the changing requirements of the role.