Make it matter.

POSITION DESCRIPTION

Cyber Security Risk Advisor

Position Level	9
Faculty/Division	Operations
Position Number	ADMIN ONLY
Original document creation	March 2022

Position Summary

The Cyber Security Risk Advisor is a key contributor to the operational delivery of a fit-for-purpose and adaptive Cyber Security Governance framework and Information Security Management System (ISMS). This role is responsible for the management and assessment of information security risks associated with ICT services and IT initiatives, and the provision of cyber security subject matter expertise, risk assessment, assurance, and advisory services to university stakeholders.

The Cyber Security Risk Advisor reports to the Cyber Security Advisory Manager and has no direct reports.

Responsibilities

Specific responsibilities for this role include:

- Delivery of risk advisory and risk assessment services to University stakeholders.
- Review solution/capability design and architecture artefacts, identify and assess security risks, recommend and prepare high quality reports detailing security issues and risk treatment actions.
- Perform and oversee risk assessment of 3rd party/supply chain risk exposure.
- Update and manage the cyber risk register with risks from projects, penetration tests, and exemptions.
- Socialise the risks to the relevant teams and administer the completion of risk treatment and policy compliance initiatives prior to deployment or change.
- Guide and educate University stakeholders in the practical application of security and risk management concepts, principles, strategies and relevant industry standards.
- Provide expert advice on cyber security compliance by ensuring and communicating adherence to policies, standards, architecture and strategies (including surrounding cloud services).
- Ensuring any non-compliance, control under-performance or risk beyond appetite is appropriately recorded and effectively escalated for remediation.
- Drive penetration testing scope validation, penetration test report review, risk assessment and re-testing recommendations of IT systems and infrastructure as a part of project assurance.
- Analyse and advise on new or complex exemptions requests.

- Identify and recommend required changes to cyber security policies and standards.
- Deliver periodic cyber security risk advisory service SLA and KPI metrics to drive compliance.
- Support the independent audit of cyber security controls on behalf of the University, including statutory audits completed by the Audit Office of NSW.
- Continually stay up to date and aware of legal, regulatory compliance and contractual obligations that arerelevant to the University's management of cyber security risk.
- Promote awareness of the University's internal and external environment for emerging cyber security threats.
- Develop and manage effective working relationships with internal and external stakeholders to develop innovative solutions that meet business needs.
- Promote a culture of continuous improvement, championing professional standards, innovation, and methods.
- Other duties appropriate and in line with to this position as requested by the Cyber Security Risk Advisory Manager.
- 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 health and safety of yourself or others.
- Align with and actively demonstrate the UNSW Values in Action: Our Behaviours and the UNSW Code of Conduct.

Skills and Experience

- Minimum 5 years' experience in the delivery of cyber security risk assessment, consulting, and advisory services, ideally with experience working for a global consulting firm, technology giant or large government agency or defence consultancy.
- A relevant Degree with extensive experience in cyber security governance, compliance, risk management or cyber security operations within major organisations or an equivalent level of knowledge gained through any other combination of education, training, and experience.
- Strong cyber security GRC fundamentals and strong knowledge of cyber security principles and practices.
- Excellent understanding of industry-wide security standards and compliance frameworks such as ISO 27001, NIST 800-53, CSA, Essential 8, PCI DSS, COBIT 5, Mitre ATT&CK etc.
- Relevant industry certification(s) such as CISSP (Ideal), CEH, CISM, CRISC, GSEC, AWS Security Speciality, Microsoft Azure (highly desirable).
- Excellent understanding of current security technologies, products, and services, including native cloud security controls in AWS and Azure.
- Strong interpersonal, communication and negotiation skills including 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 high level of personal motivation, resilience, and ability to work effectively individually or in teams.
- An understanding of and commitment to UNSW's aims, objectives, and values in action, together with relevant policies and guidelines.
- Knowledge of health and safety responsibilities and commitment to attending relevant health and safety training

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.