UNSW SYDNEY

Make it matter.

POSITION DESCRIPTION

Cyber Security Governance & Compliance 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 Governance and Compliance Manager is responsible for leading the development, implementation, and continuous improvement of the University's cyber security governance framework. This role ensures the organisation remains compliant with internal and external cyber security policies, standards, and regulations.

The Cyber Security Governance and Compliance Manager will provide strategic leadership in managing audits, certifications, and regulatory obligations, such as DISP, SOCI, and ISO 27001, whilst improving the maturity of cyber security governance practices across the University. Additionally, the Cyber Security Governance and Compliance Manager will act as a subject matter expert to senior stakeholders on cyber security compliance, risk management, and governance matters. Developing and overseeing key operational metrics for tracking the University's cyber security compliance posture, ensuring the organisation meets its compliance objectives.

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

Accountabilities

Specific accountabilities for this role include:

- Lead the strategic oversight and continuous improvement of the cyber security policy framework, ensuring alignment with industry standards and regulatory requirements.
- Develop, implement and maintain cyber security policies, standards, and guidelines in response to emerging risks and changes in the threat landscape.
- Lead the quarterly Cyber Security Standards Review process, ensuring policies and standards remain current and relevant to organisational needs.
- Oversee the operationalisation and effectiveness of the policy compliance attestation process, ensuring compliance across the University.
- Manage security baselines and associated policies, ensuring their alignment with the organisation's security posture and strategic goals.
- Lead the development and implementation of cyber security compliance strategy and framework, ensuring ongoing compliance with DISP, SOCI, ISO 27001, and other regulatory requirements.
- Oversee bi-annual compliance assessments, ensuring that findings are reported, agreed, and remediated through strategic action plans.
- Provide leadership and support for the DISP accreditation and ISO 27001 certification processes, ensuring full compliance and successful certification.
- Manage the University's compliance with the Security of Critical Infrastructure Act (SOCI) and ensure that PCI-related obligations are continuously met.
- Ensure that all regulatory requirements are tracked, monitored, and integrated into the University's broader cyber security governance strategy.
- Oversee internal and external audit engagements, including NSW Audit Office audits, DISP, SOCI, and other compliance audits, ensuring that all requirements are met, and corrective actions are implemented.
- Lead the strategic coordination of cyber security insurance audits and renewals, ensuring all necessary documentation and compliance requirements are fulfilled.
- Establish and manage key operational metrics for monitoring cyber security audit and insurance processes, ensuring continuous improvement and accountability.
- Lead and mature the Cyber Security GRC (Governance, Risk, and Compliance) Communities of Practice, fostering collaboration and best practice sharing across faculties and divisions.
- Represent the cyber security function at key governance forums, such as the weekly Change Advisory Board (CAB) and monthly Business Partners (BP) forums, ensuring cyber security governance is integrated into decision-making processes.
- Lead the strategic maturity uplift of the Cyber Security Exemption Process, ensuring that all exemptions are justified, managed, and periodically reviewed for ongoing relevance.
- 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.
- Oversee the management of the Security Service Catalogue, ensuring it is regularly updated and accessible.

- Oversee and manage the Asset register in Cyber Security GRC Platform, ensuring all new assets are properly assessed and approved within the cyber security governance framework.
- Align with and actively demonstrate the Code of Conduct and Values
- 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

- Relevant tertiary qualification with extensive experience (7+ years) in cyber security governance, risk management, and compliance, or equivalent competence gained through any combination of education, training and experience.
- Strong knowledge and experience with compliance frameworks, including DISP, SOCI, ISO 27001, PCI-DSS, and other relevant regulatory requirements.
- Proven track record of managing cyber security audits and certifications, with experience coordinating both internal and external audit activities.
- Demonstrated leadership in developing and enforcing cyber security policies, standards, and regulatory requirements across complex organisations.
- Strong strategic and project management skills, with the ability to lead multiple governance and compliance initiatives simultaneously.
- Excellent communication, negotiation, and interpersonal skills, with a proven ability to influence and engage stakeholders at all levels of the organisation.
- Certifications such as CISM, CISSP, CRISC, ISO 27001 Lead Auditor, or related certifications are highly desirable.
- Strong analytical and problem-solving skills, with the ability to present complex governance and compliance information to diverse audiences.
- High level of motivation, resilience, and the ability to lead teams and work effectively within cross-functional environments.
- Experience with cyber security governance and risk management tools, such as Protecht GRC tool, CyberGRX, UpGuard, and Bitsight.
- 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

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.