JOB DESCRIPTION

Specialist Cyber Security Assurance

ROLE TITLE	Specialist Cyber Security Assurance
SECTION/DIVISION:	IT Assurance and Cyber Security, Digital Division
REPORTS TO:	Senior Manager Assurance and Continuity
DIRECT REPORTS (FTE):	Nil
INDIRECT REPORTS (FTE):	Nil
PRIMARY PURPOSE OF THE ROLE:	Consult on, assess, report on, and track cyber security assurance activities across Otago's digital projects and information assets. Act as a trusted internal advisor on our security controls framework and advises digital projects on the application of appropriate security controls. The assurance processes the role is responsible for involves assisting teams in following a secure by design approach, application of security controls, and validating those controls to ensure our information assets are secure. Conduct and assist in auditing activities and subsequent management of risks, working closely with the Office of Risk and Assurance. The roles proactive approach helps safeguard the university's operations and minimizes the impact of potential crises
ACCOUNTABILITIES:	**Information assurance, INAS: Level 5** Interprets information assurance and security policies and applies these to manage risks. Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines. Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain. Contributes to the development of policies, standards and guidelines. **Consultancy, CNSL: Level 5** Takes responsibility for understanding client requirements, collecting data, delivering analysis and problem resolution. Identifies, evaluates and recommends options. Collaborates with, and facilitates stakeholder groups, as part of formal or informal consultancy agreements. Seeks to fully address client needs and implements solutions if required. Enhances the capabilities and effectiveness of clients, by ensuring that proposed solutions are fully understood and appropriately exploited. **Information security, SCTY: Level 5** Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Contributes to development of information security policy, standards and guidelines.

Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements.

Develops new architectures that mitigate the risks posed by new technologies and business practices.

Specialist advice, TECH: Level 4
Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations.

Actively maintains knowledge in one or more identifiable specialisms.

Recognises and identifies the boundaries of their own specialist knowledge.

Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs.

Audit, AUDT: Level 4
Contributes to planning and executing of risk-based audit of existing and planned processes, products, systems and services.

Identifies and documents risks in detail.

Identifies the root cause of issues during an audit, and communicates these effectively as risk insights.

Collates evidence regarding the interpretation and implementation of control measures. Prepares and communicates reports to stakeholders, providing a factual basis for findings.

Risk management, BURM: Level 4
Carries out risk management activities within a specific function, technical area or project of medium complexity.

Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business.

Involves specialists and domain experts as necessary.

Stakeholder relationship management, RLMT: Level 4
Deals with problems and issues, managing resolutions, corrective actions, lessons learned, and the collection and dissemination of relevant information.

Implements stakeholder engagement/communications plan. Collects and uses feedback from customers and stakeholders to help measure the effectiveness of stakeholder management.

Helps develop and enhance customer and stakeholder relationships.

KEY RELATIONSHIPS:	Internal IT Services Division staff Project Management Office Procurement Office Strategy, Analytics and Reporting Office (SARO) Senior managers and staff Director Risk, Assurance and Compliance Committees Students External Industry and tertiary sector peers Government agencies such as NZ Police, Department of Internal Affairs Internet Service Providers Vendors, service providers, contractors, consultants
QUALIFICATIONS AND EXPERIENCE:	Essential Tertiary level Computer Science qualification or recognised qualification(s) appropriate to the role. Significant experience in the computing industry of which 3+ years' have been in information security or cyber security. Experience in applying security frameworks (e.g. NIST CSF, ISO 27002, CIS Critical Controls, or PSR). Proven engagement experience and a consultative and partnering approach with stakeholders. Preferred Postgraduate qualifications or certifications in cyber security, quality assurance, compliance, or business continuity (e.g. Certified Internal Auditor (CIA), or Certified Information Systems Auditor (CISA), are highly valued. A deep understanding of the interdependent relationship between IT infrastructure, information security and the applications/services they enable. Experience in leading and advocating the use of Te Reo, tikanga and mātauranga Māori in the workplace.
TECHNICAL SKILLS AND KNOWLEDGE:	Essential Strong understanding of New Zealand's regulatory requirements and standards, especially those related to the education sector, public sector governance, and health and safety Continuous improvement methodologies (e.g. Lean Six Sigma) Demonstrated experience with a range of technologies e.g. Microsoft Server and Client operation system and infrastructure applications. Experience in technical cyber security consulting, applying security controls, and conducting risk assessments.
SPECIAL REQUIREMENTS:	Some travel may be required to attend other sites. After hours or on - call work will be required on occasion. A police vetting check from a relevant agency satisfactory to the University will be a condition of employment. At the University, we are required to be compliant with the Public Records Act 2005 and Privacy Act 2020. Staff are expected to participate in available training to understand these requirements and effectively manage information accordingly.
DIRECT BUDGET ACCOUNTABILITY:	Nil
MĀORI STRATEGIC FRAMEWORK:	Act in a manner consistent with the principles and implications, as well as the University's commitment to the Treaty as articulated in the Māori Strategic Framework.

PACIFIC STRATEGIC FRAMEWORK:	Act in a manner consistent with the strategies and goals contained in the University's Pacific Strategic Framework, role-modelling and promoting Pacific values, equity and diversity principles and cultural safety practices.
HEALTH AND SAFETY:	Act and work in a manner compliant with current health and safety at work legislation and University procedures, frameworks and guidelines. Role model safe behaviour and practices, share the responsibility to prevent harm and contribute to a safe campus and work environment, including raising workplace health and safety concerns for self, students, visitors and other staff.
SUSTAINABILITY:	Act in a manner consistent with the University's sustainability commitments; role-modelling sustainable practices, with a particular emphasis on minimising the environmental impact of day-to-day activities.

SKILLS FRAMEWORK FOR THE INFORMATION AGE (SFIA)

Specialist Cyber Security Assurance

Role Type: Specialist

SFIA Levels of responsibility

Autonomy	4	Influence	4	Complexity	5	Business Skills	5	Knowledge	4

SFIA Skills Profile

Category	Subcategory	Skill	Code	L1	L2	L3	L4	L5	L6	L7
Strategy and architecture	Security and privacy	Information assurance	INAS					■		
Strategy and architecture	Advice and guidance	Consultancy	CNSL					■		
Strategy and architecture	Security and privacy	Information security	SCTY					■		
Strategy and architecture	Advice and guidance	Specialist advice	TECH				■			
Strategy and architecture	Governance, risk and compliance	Audit	AUDT				■			
Strategy and architecture	Governance, risk and compliance	Risk management	BURM				■			
Relationships and engagement	Stakeholder management	Stakeholder relationship management	RLMT				■			

https://help.sfia.nz/hc/en-nz/sections/4407230514201-Levels-of-responsibility

https://sfia-online.org/en/sfia-8/sfia-views/full-framework-view?path=/glance