Role Description
Chief Information Security Officer

Role Description Fields	Details
Cluster	Education
Department/Agency	TAFE NSW
Division/Branch/Unit	Systems Group
Role number	
Classification/Grade/Band	PSSE Band 1
Senior executive work level standards	Work Contribution Stream: Professional/Specialist
ANZSCO Code	262112
PCAT Code	226368
Date of Approval	22 November 2022
Agency Website	

Agency overview

TAFE NSW's purpose is to skill the workforce of the future. It is Australia's leading provider of vocational education and training with over 500,000 annual enrolments and a proud history for setting the benchmark for quality service. As the NSW public provider, it supports the NSW Government's priority to grow skills for the economy and jobs of tomorrow. Critically, TAFE NSW plays a vital role in providing vocational education in rural and regional NSW, and job training pathways for the most vulnerable in the community.

TAFE NSW offers the best of campus-based delivery as well as flexible, online and work-based learning. The TAFE NSW values of Customer First, Collaboration, Integrity and Excellence guide our team in strengthening communities, delivering world-class training for our students and producing job ready graduates for employers. The operating environment for TAFE NSW is dynamic as we leverage our scale, expertise, passion and reputation to meet the rapidly changing VET landscape.

TAFE NSW is committed to its students and customers and the role it plays in changing lives and opening up opportunities through learning.

Primary purpose of the role

The Chief Information Security Officer (CISO) is responsible for driving the development, implementation and support of ICT best practice standards and ensuring compliance to deliver secure and reliable systems.

The CISO develops and implements TAFE NSW's information technology (IT) security strategy whilst protecting the business from information security breaches and cyber environment threats.

Key accountabilities

1. Identify and analyse TAFE NSW and sector IT security issues to ensure compliance with business, statutory and legislative obligations.
2. Develop, maintain and implement TAFE NSW's ICT security strategy, governance framework, architecture and practice to drive the provision of secure ICT services, which support business outcomes through effective risk management strategies.
3. Lead, develop and communicate innovative ICT cyber and information security policy, standards, training and compliance systems to drive awareness and secure use of information systems.

4. Manage, measure and monitor information security threats, incidents and investigations to ensure the timely response and containment of security issues.
5. Provide expert, authoritative and professional advice to the Chief Information Officer and senior management on ICT security matters to inform and influence decisions that effectively enhance systems security and minimise risk.
6. Ensure alignment of information security strategies with business objectives, collaborating with stakeholders on TAFE NSW's overall business continuity and disaster recovery strategies.
7. Drive implementation of a comprehensive program of security management audits and controls, including vulnerability testing, ensuring proactive identification and assessment of threats, weaknesses and non-conformance to effectively address current and future risks.
8. Manage financial budgeting, reporting and resourcing to achieve service delivery outcomes and savings targets.
9. Demonstrate a genuine commitment to safety excellence and safety leadership. This includes actively consulting, promoting and contributing to initiatives, monitoring safety performance, and making decisions and acting on health, safety and wellbeing matters.
10. Place the customer at the centre of all decision making.
11. Build and develop a high performance team, aligned to the core values of integrity, collaboration, excellence and a customer first attitude, through effective leadership, support and feedback.
12. Collaborate with staff to ensure the development and regular review of meaningful individual performance development and review plans that are clearly aligned to strategic objectives and focused to develop the individual.

Key challenges

- Engaging and influencing stakeholders to ensure relevant ICT security governance frameworks and risk management practices are effectively implemented.
- Responding appropriately to threats as they emerge in a context where disciplines around security and risk management are evolving.
- Embedding a consistent and high level of ICT security protection and risk mitigation practice across TAFE NSW as a mainstream operational standard.
- Proactively and responsively managing both the diversity and complexity of security matters and associated risk in a commercially sensitive business delivery context.
- Providing high-level risk informed advice on IT security strategies and solutions that both minimizes threats and business services delivery disruption.

Key relationships

Internal

Who	Why
Chief Information Officer	- Receive leadership, advice and support. - Provide expert strategic and technical advice to influence decisions regarding ICT security initiatives and innovation. - Alert to significant issues, providing risk informed advice and options to address.
Direct Reports	- Provide leadership, advice and support. - Guide on decisions and actions regarding implementation of security and risk management strategies. - Support with complex issues management and resolutions.

TAFE NSW Executive and senior management level committees and forums	• Provide information and reporting on IT security related issues and activities. • Build awareness and knowledge on IT security issues, innovations and trends to assist inform business planning, strategies and operational decision making.
TAFE NSW corporate services and business managers and stakeholders	• Provide expert advice and guidance on IT security and cyber threat issues. • Support with awareness of IT security risks and embedding practical approaches to minimising risk.
TAFE NSW managers and staff	• Provide communications and access to documents and resources to build awareness and assist with IT security related policies, processes and practices.

External

Who	Why
Specialist contractors and services providers	• Manage relationships, provide work specifications and oversee performance.
Whole of government ICT forums	• Build networks, share learnings and optimise synergies to deliver improved IT security management strategies and practices. • Work with central agencies and other clusters to collaborate on initiatives and strategies of benefit to the sector and to TAFE NSW.

Role dimensions

Decision making

- Makes decisions on highly complex and sensitive issues where there may be no readily available source of advice and guidance and outcomes may break new ground for the organisation
- Manage functional expenditure and resourcing within relevant policy and delegation frameworks.
- Matters requiring a higher level of approval are referred to the Reporting Line Manager.

Reporting line

Chief Information Officer

Direct reports

~3

Budget/Expenditure

TBA

Key knowledge and experience

1. Demonstrated experience developing and implementing an enterprise level IT security strategy for a large and diverse organisation.
2. Proven record of achievement addressing IT security issues, protecting against cyber threats and effectively managing associated risks.
3. Significant experience providing strategic management advice based on professional knowledge and expertise in ICT security and embedding best practice standards in operations.

Essential requirements

1. Degree qualification in related field or equivalent significant experience.
2. Ability to address and meet focus capabilities as stated in the Position Description.

Capabilities for the role

The NSW public sector capability framework describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for roles with managerial responsibilities. These groups, combined with capabilities drawn from occupation-specific capability sets where relevant, work together to provide an understanding of the capabilities needed for the role.

The capabilities are separated into focus capabilities and complementary capabilities

Focus capabilities

Focus capabilities are the capabilities considered the most important for effective performance of the role. These capabilities will be assessed at recruitment.

The focus capabilities for this role are shown below with a brief explanation of what each capability covers and the indicators describing the types of behaviours expected at each level.

Focus capabilities

Capability group/sets	Capability name	Behavioural indicators	Level
Personal Attributes	**Manage Self** Show drive and motivation, an ability to self-reflect and a commitment to learning	• Promote and model the value of self-improvement and be proactive in seeking opportunities for growth and new learning • Actively seek, reflect on and integrate feedback to enhance own performance, showing a strong capacity and willingness to modify own behaviour • Manage challenging, ambiguous and complex issues calmly and logically • Model initiative and decisiveness	Highly Advanced

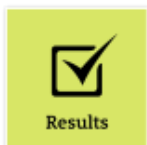|	**Commit to Customer Service** Provide customer-focused services in line with public sector and organisational objectives	• Promote a customer-focused culture in the organisation and consider new ways of working to improve customer experience • Ensure systems are in place to capture customer service insights to improve services • Initiate and develop partnerships with customers to define and evaluate service performance outcomes • Promote and manage alliances within the organisation and across the public, private and community sectors • Liaise with senior stakeholders on key issues and provide expert and influential advice • Identify and incorporate the interests and needs of customers in business process design and encourage new ideas and innovative approaches • Ensure that the organisation's systems, processes, policies and programs respond to customer needs	Advanced
	Work Collaboratively Collaborate with others and value their contribution	• Recognise outcomes achieved through effective collaboration between teams • Build cooperation and overcome barriers to information sharing, communication and collaboration across the organisation and across government • Facilitate opportunities to engage and collaborate with stakeholders to develop joint solutions • Network extensively across government and organisations to increase collaboration • Encourage others to use appropriate collaboration approaches and tools, including digital technologies	Advanced
	Influence and Negotiate Gain consensus and commitment from others, and resolve issues and conflicts	• Influence others with a fair and considered approach and present persuasive counter-arguments • Work towards mutually beneficial 'win-win' outcomes • Show sensitivity and understanding in resolving acute and complex conflicts and differences • Identify key stakeholders and gain their support in advance • Establish a clear negotiation position based on research, a firm grasp of key issues, likely arguments, points of difference and areas for compromise • Anticipate and minimise conflict within the organisation and with external stakeholders	Advanced

	Deliver Results Achieve results through the efficient use of resources and a commitment to quality outcomes	• Seek and apply the expertise of key individuals to achieve organisational outcomes • Drive a culture of achievement and acknowledge input from others • Determine how outcomes will be measured and guide others on evaluation methods • Investigate and create opportunities to enhance the achievement of organisational objectives • Make sure others understand that on-time and on-budget results are required and how overall success is defined • Control business unit output to ensure government outcomes are achieved within budgets • Progress organisational priorities and ensure that resources are acquired and used effectively	Advanced
	Think and Solve Problems Think, analyse and consider the broader context to develop practical solutions	• Undertake objective, critical analysis to draw accurate conclusions that recognise and manage contextual issues • Work through issues, weigh up alternatives and identify the most effective solutions in collaboration with others • Take account of the wider business context when considering options to resolve issues • Explore a range of possibilities and creative alternatives to contribute to system, process and business improvements • Implement systems and processes that are underpinned by high-quality research and analysis • Look for opportunities to design innovative solutions to meet user needs and service demands • Evaluate the performance and effectiveness of services, policies and programs against clear criteria	Advanced

	Demonstrate Accountability		Advanced
Results	Be proactive and responsible for own actions, and adhere to legislation, policy and guidelines	• Design and develop systems to establish and measure accountabilities • Ensure accountabilities are exercised in line with government and business goals • Exercise due diligence to ensure work health and safety risks are addressed • Oversee quality assurance practices • Model the highest standards of financial probity, demonstrating respect for public monies and other resources • Monitor and maintain business-unit knowledge of and compliance with legislative and regulatory frameworks • Incorporate sound risk management principles and strategies into business planning	
Business Enablers	**Technology** Understand and use available technologies to maximise efficiencies and effectiveness	• Support research and expert advice on the application of emerging technologies to achieve organisational outcomes • Ensure that effective governance frameworks are in place to efficiently and effectively apply technology within the organisation • Establish effective governance to ensure organisational compliance with cyber security and acceptable use of technology policies • Critically assess business cases supporting the introduction of technology to improve the organisation's efficiency and effectiveness • Ensure that effective policy and procedures are in place for records, information and knowledge management to meet government and organisational requirements	Highly Advanced
People Management	**Inspire Direction and Purpose** Communicate goals, priorities and vision, and recognise achievements	• Champion the organisational vision and strategy, and communicate the way forward • Create a culture of confidence and trust in the future direction • Generate enthusiasm and commitment to goals and cascade understanding throughout the organisation • Communicate the parameters and expectations surrounding organisational strategies • Celebrate organisational success and high performance, and engage in activities to maintain morale	Highly Advanced

Capability group/sets	Capability name	Behavioural indicators	Level

Optimise Business Outcomes

Manage people and resources effectively to achieve public value

- Engage in strategic and operational workforce planning that effectively uses organisational resources to achieve business goals
- Resolve any barriers to recruiting and retaining people of diverse cultures, backgrounds and experiences
- Encourage team members to take calculated risks to support innovation and improvement
- Align systems and processes to encourage improved performance and outcomes

Advanced

Occupational Specific Focus Capabilities

Capability group/sets	Capability name	Behavioural indicators	Level
SFIA	Strategy and Architecture – Information Strategy **Information Governance**	Understands the implications of information, both internal and external, that can be mined from business systems and elsewhere. Makes decisions based on that information, including the need to make changes to the systems. Reviews new change proposals and provides specialist advice on information and records management, including advice on and promotion of collaborative working and assessment and management of information-related risk. Creates and maintains an inventory of information assets, which are subject to relevant legislation. Prepares and reviews the periodic notification of registration details and submits them to the relevant regulatory authorities. Ensures that formal information access requests and complaints are dealt with according to approved procedures. Contributes to development of policy, standards and procedures for compliance with relevant legislation.	Level 5 IRMG
SFIA	Strategy and Architecture – Advice and Guidance **Specialist Advice**	Actively maintains recognised expert level knowledge in one or more identifiable specialisms. Provides definitive and expert advice in their specialist area(s). Oversees the provision of specialist advice by others, consolidates expertise from multiple sources, including third party experts, to provide coherent advice to further organisational objectives. Supports and promotes the development and sharing of specialist knowledge within the organisation.	Level 5 TECH

SFIA	Strategy and Architecture – Business Strategy and Planning **Business Risk Management**	Carries out risk assessment within a defined functional or technical area of business. Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. Co-ordinates the development of countermeasures and contingency plans.	Level 5 BURM
SFIA	Strategy and Architecture – Information Strategy **Information Security**	Develops and communicates corporate information security policy, standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks. Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with experts in other functions such as legal, technical support. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines.	Level 6 SCTY
SFIA	Delivery and Operation – Service Operation **Security Administration**	Develops policies, standards, processes, guidelines for ensuring the physical and electronic security of automated systems. Ensures that the policy and standards for security administration are fit for purpose, current and are correctly implemented. Reviews new business proposals and provides specialist advice on security issues and implications.	Level 6 SCAD
SFIA	Delivery and Operation – Service Operation **Penetration Testing**	Takes a comprehensive approach to seeking vulnerabilities across the full spectrum of organisation policies, processes, and defences in order to improve organisational readiness, improve training for defensive practitioners, and inspect current performance levels. Determines testing policy and owns the supporting processes. Takes responsibility for the management of all vulnerability testing activities within the organisation. Assesses and advises on the practicality of testing process alternatives. Initiates improvements to test processes and directs their implementation. Assesses suppliers' development and testing capabilities. Manages client relationships with respect to all testing matters.	Level 6 PENT

|	Skills and Quality – Quality Conformance	Plans formal reviews of activities, processes, products or services.	Level 5 CORE
IIIII SFIA	**Conformance Review**	Evaluates and independently appraises the internal control of processes, based on investigative evidence and assessments undertaken by self or team.	
		Ensures that independent appraisals follow agreed procedure and advises others on the review process.	
		Provides advice to management on ways of improving the effectiveness and efficiency of their control mechanisms.	
		Identifies and evaluates associated risks and how they can be reduced.	

Complementary capabilities

Complementary capabilities are also identified from the Capability Framework and relevant occupation-specific capability sets. They are important to identifying performance required for the role and development opportunities.

Note: capabilities listed as 'not essential' for this role are not relevant for recruitment purposes however may be relevant for future career development.

Capability group/sets	Capability name	Description	Level
Personal Attributes	Display Resilience and Courage	Be open and honest, prepared to express your views, and willing to accept and commit to change	Advanced
Personal Attributes	Act with Integrity	Be ethical and professional, and uphold and promote the public sector values	Advanced
Personal Attributes	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Intermediate
Relationships	Communicate Effectively	Communicate clearly, actively listen to others, and respond with understanding and respect	Advanced
Results	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Adept
Business Enablers	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Adept
Business Enablers	Procurement and Contract Management	Understand and apply procurement processes to ensure effective purchasing and contract performance	Adept

Business Enablers	Project Management	Understand and apply effective planning, coordination and control methods	Adept
People Management	Manage and Develop People	Engage and motivate staff, and develop capability and potential in others	Adept
People Management	Manage Reform and Change	Support, promote and champion change, and assist others to engage with change	Advanced