Position Description

Our Values

We value life

We make every conversation count

We will find a better way, today

We make the complicated simple

Position Title	Digital Security Governance Manager
Position Number	
Band / Job Group	JG6 / Band 10
Division	**IT Shared Solutions** IT Shared Solutions (ITSS) is a collaborative division that delivers IT services to the TAC and WorkSafe. The division is made up of employees from both the TAC and WorkSafe.
Branch	Digital Security & Assurance
Location	Geelong
Reports To	Senior Manager, Digital Security & Assurance
Number of Direct Reports	Nil
Working with Children	Is a Working with Children check required for this position? ☐ Yes ☒ No
Financial Delegation	Nil
Job Purpose	The Digital Security Governance Manager will provide governance leadership to the organisation driving focus and prioritisation within ITSS through establishing governance principles and processes aligned to best practice and regulatory requirements. This role proactively partners with internal and external stakeholders, including audit, external service providers, technology and business partners to influence the development, implementation, monitoring, assessment, and reporting of compliance requirements, control processes, documentation and risk activities to ensure compliance to internal, Government and Industry policy and standards. A crucial element of this role is working with learning and development partners to plan and promote information security awareness programs to ensure adequate attention across the organisation.

KEY ACCOUNTABILITIES

1. Within ITSS, determines the requirements for the appropriate digital security governance of enterprise IT, ensuring clarity of responsibilities and authority, goals and objectives. Puts in place and maintains governance practices to enable governance activity to be conducted. Ensures reviews are conducted as necessary to ensure management decision-making is transparent, and that an appropriate balance between benefits, opportunities, costs and risks can be demonstrated to principal stakeholders. Establishes and maintains the governance activities for digital security compliance with the organisation's obligations (including legislation, regulatory, contractual and agreed standards/policies), holding the management team to account. Acts as the organisation's contact for relevant regulatory authorities. Ensures proper relationships between the organisation and external parties, with valid interest in the organisation's governance, are in place.
2. Develops guidelines for digital security management ensuring that uniformly recognised and accepted processes are developed and applied throughout the organisation. Identifies the impact of any relevant statutory, internal or external regulations on the organisation's use of information and develops strategies for compliance. Leads and plans activities to communicate and report on digital security management strategies. Supports and coordinates resources to meet specific business objectives whilst maintaining the principles of professional standards, accountability, openness, equality, diversity and clarity of purpose. Implements systems and controls to measure performance and manage digital security risk.
3. Maintains an awareness of the global needs of digital security and promotes (to both technology and business management) the benefits that a common approach to information and technology governance will bring to the business as a whole. Coordinates information security governance to support the secure acquisition, development, and implementation of information systems and services in close liaison with those responsible for management and strategy.
4. Monitor the development of organisational policies, standards, and guidelines for information security management which allow the organisation to respond quickly, to deliver secure services, make decisions and take actions. Champions and leads in the development of an organisational information security knowledge management approach and supporting technologies, processes and behaviours. Promotes information security knowledge-sharing through the organisation's operational business processes and systems. Monitors and evaluates information security knowledge-sharing initiatives, including external bench-marking. Manages reviews of the benefits and value of information security knowledge management. Identifies and recommends improvements. Shares experiences across communities of practice, business units, and networks on innovative approaches in information security knowledge sharing and management.

5. Plans and manages the implementation of organisation-wide processes and procedures, tools and techniques for the governance of identification, assessment, and management of security and technology risk inherent in the operation of business processes and of potential risks arising from planned change.
6. Partner with the Learning and Development (L&D) team to specify solutions for use in learning and development programs in the workplace or in compulsory, further or higher education relating to information and digital security awareness. Supports the L&D team to commission the development of learning materials, allocate resources to learning teams, define learning outcomes. Leads information and digital security learning programs, recommends and specifies learning interventions for design, development and deployment according to agreed learning outcomes.
7. Specifies organisational procedures for the internal or third-party assessment of external service providers, process, product or service, against recognised criteria. Develops plans for review of management systems, including the review of implementation and use of standards and the effectiveness of security operational and process controls. May manage the review, conduct the review or manage third party reviewers. Identifies and reports areas of risk. Recommends improvements in assessment processes and control procedures. Authorises the issue of formal reports to management on the extent of compliance of systems with standards, regulations and/or legislation.

Organisational Responsibilities

As defined by the Occupational Health and Safety Act 2004 - Victoria employees of TAC and WorkSafe Victoria are to take reasonable care to ensure their own safety, not place others at risk by any act or omission, follow safe work procedures, report hazards and injuries and cooperate with the employer to meet work health safety obligations.

Role model all TAC Leadership Model capabilities and behaviors; Adapt & Learn, Embrace Accountability, Cultivate Partnerships, Empower Others, Exercise Judgment, Deliver Outcomes, Shape Strategy & Direction and Lead Transformation.

Participate in identification and development of initiatives, risks, changes, recommendations and implementation of appropriate work practices, policies and guidelines to improve efficiency and/or effectiveness of work.

KEY SELECTION CRITERIA

Relevant Qualifications, Work Experience & Specialised Knowledge

1. Extensive experience in risk management in complex technology environments including, but not limited to, strategic adoption of cloud based solutions, Agile delivery, innovative solutions and transformational technology change.
2. Significant experience in a similar role, managing the Governance activities in a multi faceted environment.
3. Demonstrated ability to engage and influence external providers to deliver services that meet the business strategic outcomes in a safe and secure manner.
4. Highly developed interpersonal and verbal communication skills, with strong customer focus and ability to understand issues, manage expectations, gain agreement, resolve conflicts and translate technical information into business language.
5. Strong conceptual and analytical skills to drive improvements in innovation and service quality. Demonstrated achievements in driving innovative solution delivery.
6. Knowledge of the Government and industry compliance landscape.

Capabilities

Adapt and Learn: Demonstrates a range of successful strategies to maintain focus and resilience in difficult and changing circumstances

Cultivate Partnerships: Builds cross-functional networks and tailors influencing approach to gain support for ideas, projects or actions that are in the organisation’s, clients and stakeholders interests

Deliver Outcomes: Supports a performance driven culture across the business or project by providing an environment for self and others to achieve shared goals and stretch targets

Embrace Accountability: Takes responsibility for own and business area’s mistakes and uses these as an opportunity for self and others to learn

Exercise Judgement: Undertakes objective analysis and draws accurate conclusions to resolve business issues, consulting with subject matter experts as needed

Shape Strategy and Direction: Demonstrates an understanding of key industry trends and the implications for one's own area

"Improving the IT Experience"