Position description

Position title	Cyber Security Governance, Risk and Compliance (GRC) Specialist
Position number	201161
Classification level	F
Group	Enterprise Services
Reports to	Manager, Enterprise Architecture & Security
Location	1010 La Trobe Street, Docklands 3008
Date	March 2026
Tenure	Permanent Full-Time

Our organisation

VicTrack owns Victoria's rail transport land, assets and infrastructure. As a commercially focused government agency delivering for Victoria, we work to protect and grow the value of the portfolio, to support a thriving transport system and make travel and living better for all Victorians. With much of our asset portfolio dedicated to rail transport – our land, infrastructure, buildings and telecommunication networks – our focus is on strategic asset management and supporting the delivery of better transport solutions.

Whether we're planning and managing the use of transport land, upgrading the telecommunication network or partnering on major infrastructure projects, our job is to ensure the state's assets continue to serve Victoria now and well into the future.

Our business is made up of specialist groups including Innovation, Assets Optimisation & Technology, Property and Telecommunications. These are supported by groups that provide strategic, financial and operational services to the organisation.

About the group

This position is based in **Enterprise Services**.

This Group provides enterprise-wide support to run VicTrack's operations. It is responsible for a wide range of specialist functions that enable our business to be accountable, transparent and operate effectively including Enterprise IT, People & Culture, Legal & Compliance and Asset Governance.

Our vision

As a part of the transport portfolio, we share a common vision as defined in the *Transport Integration Act 2010*:

"To meet the aspirations of Victorians for an integrated and sustainable transport system that contributes to an inclusive, prosperous and environmentally responsible state".

In realising this vision, we are working towards a transport system that promotes:

- social and economic inclusion
- economic prosperity
- environmental sustainability
- integration of transport and land use
- efficiency, coordination and reliability
- safety, health and wellbeing.

Our mission

To protect and grow our rail transport assets and drive reinvestment to service Victorians now and into the future.

Our values

- Professional – We make decisions with integrity and respect. By behaving professionally and ethically we win the trust of our colleagues, stakeholders and customers.
- Collaborate – We collaborate to get things done efficiently and effectively. We have greater opportunity through leveraging our collective knowledge, building stronger bonds and respecting each other.
- Achieve – We perform our roles with integrity and skill. We hold ourselves accountable for delivering what is needed and own both our successes and mistakes.
- Innovate – We embrace all new ideas that bring about change that adds value. We become more efficient, effective and competitive.

About this position

Reporting relationships

The Cyber Security GRC Specialist reports to the Manager Enterprise Architecture & Security in the Corporate Services Group.

Budget

N/A

Purpose of the position

The Cyber Security Governance, Risk and Compliance (GRC) Specialist is responsible for overseeing and managing the cyber security governance, risk and compliance functions within VicTrack. The role ensures the organisation's cyber security policies, standards, procedures and controls are aligned with best practices and VicTrack's regulatory compliance requirements.

This position involves identifying, evaluating, mitigating, and monitoring the organisation's cyber security risks. The position also coordinates and facilitates operational functions such as cyber security audits, risk assessments, reporting activities, providing guidance and support to the Manager, Enterprise Architecture & Security, the Security team and other VicTrack stakeholders.

Key accountabilities/functions

- Information security governance and compliance, including:
  - Understand the legal and regulatory environment within which VicTrack operates and ensure compliance with these obligations.
  - Develop and maintain the cyber security governance framework, including cyber security policies, standards, procedures and guidelines.
  - Facilitate the creation of suitable awareness training to guarantee that the cyber security governance framework, policies and standards are effectively communicated throughout the organisation.
  - Manage an exception review and approval process, and ensure exceptions are documented and periodically reviewed.
  - Assist with the evaluation of the effectiveness of the information security program by developing, monitoring, gathering, and analysing information security and compliance metrics for management.
  - Prepare and present cyber security reports and dashboards to the management and relevant committees providing insights and recommendations on the cyber security performance and improvement opportunities.
  - Support the continuous improvement of the cyber security framework and processes and identify and implement opportunities for enhancing the cyber security maturity and resilience of the organisation.
- Third-party supplier and vendor risk management
  - Perform third-party supplier risk assessments to ensure supply chain risk is managed throughout the supplier's lifecycle.
  - Maintain inventory of relevant suppliers/vendors, controls, and risks for ongoing vendor risk management activities.
  - Identify and advise on the technical, physical, personnel and procedural risks associated with third party relationships, particularly vendors, contractors and suppliers.
  - Ensure the third-party cyber and information security capabilities/services delivered by external parties operate as defined and deliver on contractual obligations.
  - Review of information security sections within supplier contracts, identifies gaps, and recommends security requirements to close gaps.
- Threat assessment and information risk management, including:
  - Identify, analyse, evaluate, and document information security risks and controls based on established risk criteria.
  - Conduct and analyse risk assessments to identify potential cyber security threats and vulnerabilities within the organisation's IT and telecommunications infrastructure, systems, and applications.
  - Develop and implement security risk management plans and mitigation strategies based on the findings and recommendations of the risk assessments and audits.
  - Assess and validate information on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues.
  - Predict and prioritise threats to VicTrack telecommunications services and their methods of attack.
- Assurance: audit, compliance and testing, including:
  - Lead and manage the Cyber Security Compliance Assurance program, scope of which includes meeting cyber security related obligations, internal assessments, and facilitating audits and assurance of cyber security activities and objectives.

  - Conduct control assurance testing of the information and cyber security controls in line with regulatory requirements and advise on corrective measures.
- Guidance and advice
  - Provide guidance and advice on cyber security best practices and compliance obligations to the business groups and the Enterprise IT teams.

Customer focus

VicTrack staff practise customer focus by recognising the importance of valuing customers (internal and external) and ensuring that all activities are oriented towards meeting customer needs. We listen to customers about their expectations and focus on delivering solutions that address their needs. Customer focus also includes proactively seeking and acting on feedback to enhance the customer experience.

Safety and environmental responsibilities

Ensure safety and environmental instructions are adhered to and report any inappropriate practices and incidents. Comply with the *Occupational Health and Safety Act,* as it applies to self, tenants and customers, and environmental legislation in regard to preserving the environment.

Rail safety

All staff who may be required to come into contact with rail activity, including design work and the management of other staff, must:

- be responsible for their actions where those actions can in any way affect or compromise railway safety
- be aware of the railway safety requirements associated with their duties and responsibilities
- take whatever action is possible to prevent unsafe conditions and/or incidents
- report any railway safety problems/hazards to the Manager Safety
- safely access the rail corridor.

Individual attributes

Qualifications

- A bachelor's degree or diploma in information technology (IT), computer science, software engineering, information systems, cybersecurity, data science or related technology field

In addition to the above qualifications, to be certified for this position, the incumbent must have one or more of the following industry-recognised Governance, Risk and Compliance certifications:

- Certified in Risk and Information Systems Control (CRISC) from ISACA (Information Systems Audit and Control Association)
- Certified Information System Security Professional (CISSP) from ISC2 (International Information System Security Certification Consortium)
- Certified Information Systems Auditor (CISA) from ISACA
- Certified in the Governance of Enterprise IT (CGEIT) from ISACA
- Certification in Risk Management Assurance (CRMA) from IIA (Institute of Internal Auditors)
- GRC Professional (GRCP) from OCEG (Open Compliance and Ethics Group)
- CompTIA Security+ from CompTIA
- Certified Ethical Hacker (CEH) certification from EC-Council
- Certified Information Security Manager (CISM) from ISACA
- Systems Security Certified Practitioner (SSCP) certification from ISC2

Knowledge and experience

The incumbent shall demonstrate previous knowledge and experience across all of the following areas:

- A minimum three years' experience working in a cyber security role, including technical hands-on roles or a similar GRC role.
- A minimum of two years of experience managing governance, compliance and risk related activities.
- Significant working knowledge of the laws, policies, and standards applicable to cyber security, privacy, cyber risk management, and cyber security aspects of protecting critical infrastructure with demonstrable experience interpreting obligations into cyber security practices and delivery within an organisation or enterprise.
- Experience developing and maintaining information security management systems using recognised formal Cyber Security Frameworks in the context of large complex organisations (e.g., VPDSF, NIST, ISM, Essential 8, ISO 27000 etc)
- Experience managing business and enterprise risk, including identification, analysis, mitigation, escalation and resolution.
- Experience with the administration of the cyber security third-party risk management.
- Knowledge of various IT domains, such as infrastructure, software, data, security, cloud, etc, obtained through previous technical hands-on roles or project experience.
- Experience and knowledge working in project teams under direction from project managers.
- Experience engaging and managing government departments and agencies.

Skills

- A proven ability to conduct information security risk assessments and audits, and to develop and implement information security policies and procedures
- Highly organised and able to prioritise conflicting deadlines and manage the expectations of others
- Keen attention to detail and a commitment to quality and accuracy
- Well-developed interpersonal skills with the ability to effectively work and engage with all levels within the business
- Excellent verbal, written and presentation skills
- Experience writing executive and board level reports and dashboards
- Experience managing stakeholder communication, including developing and executing communication plans, preparing and delivering reports and presentations, and facilitating meetings and workshops.

Interpersonal and other features

Internal relationships

- All VicTrack employees

External relationships

- Government departments and agencies
- All VicTrack customers
- Regulators
- Sub-contractors
- Carriers and vendors