Position description

Position title	Cyber Security Assurance & Reporting Specialist
Position number	201163
Classification level	E
Group	Corporate Services
Reports to	Manager Enterprise Architecture & Security
Location	1010 La Trobe Street, Docklands 3008
Date	July 2025
Tenure	Permanent full time

Our organisation

VicTrack is custodial owner of Victoria's rail transport land, assets and infrastructure. 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, trams, trains 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 core functions include:

- delivering telecommunications infrastructure and services that form the backbone of the transport network from signalling, driver communications, public information displays and myki ticketing
- managing land set aside for transport purposes, including the development and sale of land no longer required for transport to optimise its use
- generating income through land sales and commercial leases that is reinvested into the state's transport system
- providing project management, engineering and construction services to deliver a range of government transport projects from Victoria's Big Build to station and car park upgrades
- managing transport facilities and assets, including the open access Dynon Rail Freight Terminal, heritage buildings and environmental preservation.

VicTrack is the custodial owner of most of Victoria's tourist and heritage assets and performs the role of Tourist and Heritage Registrar.

Our business groups

Our business is made up of two specialist delivery groups – Property and Telecommunications – supported by Corporate Services, Strategy & Transformation and the Office of the Chief Executive.

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.

Dimensions

Reporting relationships

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

Budget

N/A

Purpose of the position

The Cyber Security Assurance & Reporting Specialist is responsible for leading and conducting the cyber security assurance activities across VicTrack, providing technical security expertise to ensure that existing and new ICT systems, services and products meet the security compliance requirements. The role is responsible for conducting various audits and monitoring the effectiveness of implemented security controls and determining deviations from acceptable configurations, policy, or standards, and providing expertise in risk treatment management and compliance requirements for internal and external reviews.

The Specialist will also develop cyber security reporting tailored for various internal stakeholders to provide a view of cyber security posture through a risk and compliance lens.

Key accountabilities/functions

- Assurance: Audit, Compliance and Testing, including:
    - Lead and manage the Cyber Security Compliance Assurance program and schedule, the scope of which includes meeting cyber security related obligations, internal assessments, and facilitating audits and assurance of cyber security activities and objectives.
    - Lead the monitoring of the effectiveness of implemented security controls to maintain compliance with internal and external security policies and standards.
    - Drive the coordination, monitoring and evaluation including tracking, collating, and analysing data on security assurance activities (e.g. vulnerability management, penetration testing, account management and audits).
    - Conducting control assurance testing of the cyber security controls in line with regulatory requirements and advise on corrective measures.
    - Liaise with internal stakeholders to ensure alignment with between Cyber Security Assurance and Enterprise Assurance activities to fulfill the requirements of the Enterprise Assurance Program.
    - Manage the penetration testing program, and report to management and track test findings and remediation.
    - Work closely with operations teams to ensure that systems are properly protected, and security baselines are applied correctly.
    - Lead and participate in information security audits, security reviews and risk assessments, to minimise risk exposure and ensure VicTrack is in continuous compliance.

- Reporting: Cybersecurity Metrics and Dashboards, including:
    - Collate cybersecurity metrics from various sources, including vulnerability management and security awareness platforms, and utilising this data to produce comprehensive cybersecurity reports.
    - Provide regular reporting while improving the internal processes to promote consistent evaluations, automation, and reporting of metrics.
    - Prepare and present comprehensive cybersecurity reports and dashboards to management and key stakeholders, offering insights and recommendations based on cybersecurity testing results, as well as updates on program status, compliance, and operational risk posture.

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 technical background, to be certified for this position, the incumbent must have one or more of the following audit and assurance certifications or equivalent certification:

- ISO/IEC 27001 Lead Auditor
- Certified Information Systems Auditor (CISA) from the Information Systems Audit and Control Association (ISACA)
- Certified in Risk and Information Systems Control (CRISC) from ISACA
- Certification in Risk Management Assurance (CRMA) from IIA (Institute of Internal Auditors)

Knowledge and experience

- A minimum five years' experience working in a cybersecurity role, including audit, assurance, compliance and broader cybersecurity governance, risk and compliance (GRC) activities that provide a sound understanding of cybersecurity practices.
- Demonstrated capability to perform tasks independently or collaboratively within a team, fostering inclusive and effective relationships while contributing to a constructive team environment.
- Working knowledge of the Victorian Government compliance requirements and other security frameworks and standards such as VPDSF, Australian Government PSPF, NIST, Essential 8 and ISO/IEC 27001.
- Experience with delivering cyber assurance activities across various security technologies, including technologies such as firewalls and network based cybersecurity controls, intrusion detection systems, anti-malware, EDR/XDR systems, web and cloud-based cybersecurity controls, modern identity security systems, log management, and content filtering.
- Experience with developing cybersecurity metrics and dashboard reporting that provide management and other stakeholders with visibility of cybersecurity posture and practices.
- Proficient in using Microsoft Power BI to ingest data feeds, design and produce effective reports and visually informative dashboards.

- Experience in identity and access management principles as well as coordinating penetration testing and vulnerability scans.
- Experience managing stakeholder communication, including developing and executing communication plans, preparing and delivering reports and presentations, and facilitating meetings and workshops.
- Experience writing executive reports and dashboards.
- 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.

Skills

- Strong written and verbal communication skills.
- Highly organised and able to prioritise conflicting deadlines and manage the expectations of others.
- A keen attention to detail and a commitment to quality and accuracy.

Interpersonal and other features

Internal relationships

- All VicTrack employees

External relationships

- Government departments and agencies
- All VicTrack customers
- Regulators
- Subcontractors
- Carriers and vendors