Position Description

Information Security Compliance Analyst

June 2026

TEAM Information Security	**DEPARTMENT** Technology Services
REPORTS TO Information Security Manager	**DIRECT REPORTS** Nil
EMPLOYMENT TYPE Full Time - Permanent	**LOCATION** Hybrid Working (3:2 Office/WFH) Primary Location: Melbourne/Newborough
AWARD Banking, Finance & Insurance Award *Level 3*	**KEY CONTACT** Information Security Manager Chief Technology Officer

WHO IS LATROBE?

At Latrobe, our people are at the heart of what we do. We are committed to creating an environment where diversity is celebrated, equity is achieved and inclusion and belonging are prioritised and celebrated.

We're known for being the *health fund with heart* - a not-for-profit, regional private health insurer with more than 100,000 members across Australia. We support our members through the highs and lows of their health, and we give back to our community.

Our aspirational vision is to be a leading not-for-profit Private Health Insurer transforming health and wellness outcomes for all Australians. Our purpose is supported by 5 key values:

We display trust and respect always	*We focus on shared results*	*We engage & empower*	*We are accountable*	*We create a positive work environment*

POSITION OBJECTIVE

The Information Security Compliance Analyst performs second line (Line 2) information security assurance and compliance activities. The role provides independent oversight and challenge to ensure that the organisation's information security control environment is designed and operating effectively to meet regulatory, legal, and internal obligations, with a primary focus on APRA Prudential Standard CPS 234 – Information Security.

The role works closely with Technology, Security, and Risk teams to translate regulatory obligations into practical security control expectations, and to provide evidence-based assurance that controls are providing the expected value.

Position Description

REQUIREMENTS OF THE POSITION

Key duties and responsibilities

- **Compliance Assurance**
  - Support the organisation in meeting CPS 234 accountability requirements, including providing assurance inputs to management and Board attestations.
  - Working with data domain owners and stewards, ensure information assets are appropriately classified (criticality and sensitivity).
  - Ensure testing is conducted periodically and commensurate with the criticality and sensitivity of information assets.
  - Maintain the enterprise security control register, including mapping to risks and compliance obligations.
  - Provide clear Line 2 challenge and advice on control design and operation without assuming ownership of controls.
- **Control Design Effectiveness Testing**
  - Define, document, and deliver a fit-for-purpose, risk-based information security controls testing framework.
  - Assess the design effectiveness of information security controls to determine whether they are appropriately designed to meet stated objectives and compliance requirements.
  - Review security policies, standards, procedures, and technical designs to validate alignment to CPS 234 and internal risk appetite.
  - Identify control gaps, weaknesses, or overlaps and document findings in a clear, risk-based manner.
- **Control Operational Effectiveness Testing**
  - Plan and perform operational effectiveness testing of information security controls across people, process, and technology domains.
  - Facilitate independent and internal assurance activities, including:
  - Penetration testing and vulnerability assessments
  - Secure configuration and hardening reviews
  - Disaster recovery and technology resilience tests
  - Cyber security incident response simulations and table-top exercises
  - Perform or coordinate assurance activities over third-party and service provider security controls where information assets are managed externally.
  - Assess test results, validate remediation actions, and track closure of findings.
- **Risk, Issues, and Reporting**
  - Document assurance activities, outcomes, issues, and recommendations in clear and concise reports and dashboards, suitable for senior management and risk committees.

    - Support the uplift of Latrobe's security risk posture through thematic insights and trend analysis.
    - Contribute to regulatory responses, audits, and management attestations relating to information security.
    - Escalate material control weaknesses to the Chief Risk Officer.

- Stakeholder Engagement
    - Provide support and information as requested by the Technology, Risk & Compliance, Data and Security teams.
    - Support members of the Risk and Compliance team in conducting technology assurance tests.
    - Engage with the Risk and Compliance team to ensure consistent interpretation and application of CPS 234 obligations.
    - Provide advice and guidance to control owners on regulatory expectations and better-practice control implementation.

Leadership teamwork and relationship building

- Model the Latrobe Way values and behaviours in the delivery of individual performance; actively contribute to a constructive, high performing team and organisational culture.
- Develop and maintain professional relationships with peers and stakeholders at all levels across the business to support inter-departmental collaboration.
- Independently prioritise work to support consistent achievement of individual and team key performance indicators; appropriately escalate issues impacting either performance and/or the business; and demonstrate a flexible, adaptable, mobile and energised (FAME) mindset.
- Be a highly effective team member with energy, enthusiasm and creativity – able to work autonomously and as part of a team.

Accountability and extent of authority

- Always ensure compliance with the Private Health Insurance Code of Conduct and all applicable policies and procedures.
- The role is accountable for providing independent, objective oversight and assurance over the organisation's information security control environment.
- The role is authorised to:
    - Define and execute Line 2 information security assurance activities in accordance with approved plans and priorities.
    - Request information, evidence, and access from Technology, Security, and Risk teams to perform control assessments and testing.
    - Engage internal and external assurance providers (e.g. penetration testers, incident response exercise facilitators) in line with approved procurement and governance processes.
    - Provide formal assurance opinions, findings, and recommendations to management, risk committees, and the Chief Risk Officer.

- Escalate material control weaknesses, non-compliance, or emerging risks through appropriate risk and compliance channels.

- The role is not authorised to:
  - Own, implement, or operate information security controls.
  - Accept or approve information security risks on behalf of the organisation.
  - Direct Line 1 technology or security teams outside of agreed assurance activities.
- Authority is exercised within the framework of the organisation's risk management, compliance, and delegated authority policies
- Actively maintain awareness of all risk and compliance obligations defined through Latrobe's Risk Management Framework.
- Consistently achieve individual goals and objectives and actively lead own growth and achievement planning and implementation.

Judgement and decision making

- Interpret and work within organisational policy and procedure and/or legislation applicable to the position.
- Actively offer and implement a course of action and solutions based on evaluation and analysis of numerical and written information focussed on results.
- Make decisions which are objective and free from undue influence consistent with Latrobe's risk culture and approved strategic priorities and objectives.
- Make decisions consistent with Latrobe's operational delegations and delegate or escalate matters appropriately.
- The Information Security Compliance Analyst is required to exercise sound professional judgement in assessing the adequacy and effectiveness of information security controls, often in complex and evolving risk environments. Key judgement and decision-making requirements include:
  - Determining the scope, depth, and frequency of assurance activities based on risk, regulatory expectations, and organisational priorities.
  - Evaluating control design and operational effectiveness, including forming balanced views where evidence may be incomplete or inconsistent.
  - Assessing the materiality and severity of control deficiencies and determining appropriate escalation paths.
  - Balancing independence and constructive challenge while maintaining effective working relationships with stakeholders.
  - Interpreting regulatory guidance, industry standards, and better practice and applying them pragmatically to Latrobe's operating context.
  - Make decisions which are objective and free from undue influence consistent with Latrobe's risk culture and approved strategic priorities and objectives.
  - Make decisions consistent with Latrobe's operational delegations and delegate or escalate matters appropriately.

- Decisions are guided by established policies, regulatory obligations, risk appetite, and professional standards, with significant matters escalated to the Information Security & Data Governance Manager and, where appropriate, the Chief Risk Officer.

Experience skills and knowledge

Essential

- Demonstrated experience in information security, risk, or compliance roles (Line 2 or Internal Audit preferred).
- Strong understanding of information security control frameworks, particularly NIST CSF 2.0, and regulatory obligations.
- Experience testing control design and operational effectiveness.
- Ability to analyse complex technical information and translate it into clear risk and compliance insights.
- Experience designing and delivering information security risk reports and dashboards.
- Strong written and verbal communication skills.

Desirable

- Experience in APRA-regulated environments.
- Experience providing information security assurance within Agile and DevSecOps environments.
- Experience coordinating penetration tests, disaster recovery exercises, or cyber incident simulations.
- Exposure to frameworks such as ISO/IEC 27001 or COBIT.
- Relevant certifications (e.g. CISA, CRISC, CISSP, or similar).

Mandatory checks

- An Australian Police check will be conducted for all new employees to Latrobe Health Services prior to commencing in a role.
- Employment at Latrobe Health requires candidates to have Australian citizenship or to be a permanent resident of Australia or to have a valid visa that provides work rights in Australia.