Position Description

Director Risk Management and Compliance

Classification:	Executive Level 2 (EX02)
Business unit/department:	Legal Office
Work location:	Austin Hospital ☒ Heidelberg Repatriation Hospital ☐ Royal Talbot Rehabilitation Centre ☐ Other ☐ Mount Street site
Agreement:	Victorian Public Health Sector (Health and Allied Services, Managers and Administrative Officers) (Single Interest Employers) Enterprise Agreement 2025-2027
Employment type:	Full-Time
Hours per week:	38
Reports to:	General Counsel
Direct reports:	Nil
Financial management:	Budget: Nil
Date:	November 2026

Austin Health acknowledges the Traditional Custodians of the land on which we operate, the Wurundjeri Woi Wurrung People of the Kulin Nation. We pay our respects to Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Position purpose

The Director Risk Management and Compliance provides organisation-wide leadership, governance and oversight of Austin Health's enterprise risk management, legislative compliance, governance integrity and assurance arrangements. The role ensures organisational, clinical, executive, operational, divisional or departmental, project and local risks are clearly defined, consistently assessed, appropriately escalated and reported to the relevant management and governance bodies.

The Director develops, maintains and activates the Enterprise Risk Management Framework and annual Enterprise Risk Management Program, including the risk profile architecture, reporting cycles, and mechanisms for identifying emerging and systemic risks from data, staff feedback, incidents, key performance indicators and assurance findings.

The role oversees and delivers Austin Health's legislative compliance program, including the compliance framework, legislative obligations register, monitoring and assurance activities, reporting and remediation of identified non-compliance. The role also leads integrity governance and fraud and corruption control

arrangements, coordinates applicable Security of Critical Infrastructure, critical infrastructure risk management program obligations, and drives continuous improvement in organisational risk and compliance maturity, capability, accountability and culture.

The role supports the Executive, Board and relevant Board Committees to understand risk exposure, compliance status, control effectiveness and mitigation priorities and build risk and compliance capability, ownership and accountability by engaging and supporting executives, divisional directors, managers, and accountable owners across Austin Health.

About the Legal Office

The Legal Office provides organisation-wide legal, enterprise risk management, legislative compliance, integrity and related governance and assurance services. The Director Risk Management and Compliance sits within the Legal Office and reports to the General Counsel. There are no direct reports to this role.

Position responsibilities

Enterprise risk management framework and program

- Lead the design, implementation, operation and continuous improvement of Austin Health's Enterprise Risk Management Framework, policies, systems, processes, tools and risk architecture.
- Activate and coordinate the annual Enterprise Risk Management Program, including priorities, schedules, deliverables, accountabilities and progress reporting.
- Maintain accurate and current organisation-level risk information, records and databases.
- Lead the analysis and reporting of risk information (data sets, incidents, performance indicators, staff feedback, assurance findings and external developments) to identify new, emerging, systemic and high-level risks.
- Coordinate the development, review and maintenance of organisational, clinical, executive, divisional or departmental, project, research and local risk profiles, including the quality and consistency of risk descriptions, controls, ratings, treatment plans and accountabilities.
- Ensure Austin Health's risk appetite statement, risk escalation and acceptance processes remain fit for purpose.
- Partner with the Chief Financial Officer (CFO) to coordinate and deliver timely, accurate organisational risk reporting and associated deliverables to meet the requirements of the Audit & Risk Committee

Clinical and National Standards risk oversight

- Maintain National Standards risks and support their reporting to Executive and Board committees as required.
- Lead the redefinition and ongoing development of the Clinical Risk Profile in collaboration with Patient Safety and Clinical Excellence team and senior clinicians.
- Coordinate Executive Committee assessment of relevant data, staff feedback, incidents and key performance indicators to inform the risk assessment, control evaluation, treatment planning and action monitoring of Clinical Risk Profile.

Risk advice, reporting and assurance

- Provide authoritative, practical risk advice to executives, governance committees and risk owners.
- Coordinate proportionate reporting and escalation arrangements across all risk-profile levels.
- Prepare and coordinate the preparation of clear, accurate and decision-useful reporting on material exposure, emerging risks, control effectiveness, treatment progress and overdue actions.

- Establish and coordinate escalation of material and high-rated risks to the appropriate management and governance bodies.
- Lead a risk-based program of reviews and deep dives into material risk areas.
- Support executives, divisional directors, managers and risk owners to understand their responsibilities for risk management and build organisational capability to undertake risk assessment, control evaluation, treatment planning and action monitoring through practical guidance, engagement, templates, education and capability-building activities.
- Coordinate integrated analysis of risk profiles, incidents, KPIs, staff feedback, audit findings and compliance assessments.
- Coordination of enterprise risk with internal audit, legislative compliance, integrity, clinical governance, research governance and incident management.
- Oversight of the quality and completeness of risk and assurance information.

Integrity, legislative compliance, regulatory and critical infrastructure obligations

- Lead and maintain Austin Health's Integrity Governance Framework and Fraud, Corruption Control and Other Losses Policy and associated governance, reporting and improvement activities.
- Coordinate the annual Integrity Governance Self-Assessment, including stakeholder engagement, evidence collection, analysis, reporting and monitoring of agreed improvement actions.
- Oversee and deliver Austin Health's legislative compliance program and supporting framework, policies, procedures, systems and practices, consistent with contemporary compliance-management principles and standards.
- Maintain a current and appropriately assigned legislative obligations register, with clear executive accountability, operational ownership and escalation pathways for material obligations.
- Coordinate periodic and risk-based compliance assessments, including baseline reviews, self-assessments, evidence collection, control evaluation, validation and targeted reviews of higher-risk obligations.
- Monitor legislative and regulatory developments, assess their potential organisational impact, and provide timely, practical advice to executives, directors and accountable business owners on required changes to policies, procedures, systems, controls and practices.
- Establish and maintain mechanisms for identifying, recording, escalating, investigating and monitoring actual or potential non-compliance, including agreed corrective actions and remediation plans.
- Prepare clear, accurate and decision-useful legislative compliance reports for the Executive Committee, Audit & Risk Committee and Board, including material changes, compliance status, key findings, emerging issues, breaches, overdue actions and remediation progress.
- Support accountable executives and compliance owners to understand and discharge their obligations through practical guidance, templates, education and capability-building activities.
- Coordinate independent or specialist compliance reviews where appropriate and monitor implementation of resulting recommendations.
- Promote integration of legislative compliance with enterprise risk management, internal audit, policy governance, integrity, incident management and other assurance activities.
- Coordinate Austin Health's applicable obligations under the Security of Critical Infrastructure framework, including governance of the critical infrastructure risk management program, reporting to the Audit & Risk Committee and Board, and preparation and submission of the required annual report to the Commonwealth Government.
- Monitor relevant government, regulatory and better-practice requirements and ensure risk, compliance and integrity arrangements remain current and fit for purpose.

Leadership, engagement and capability development across Austin Health

- Build risk and compliance ownership and accountability by engaging and supporting executives, divisional directors, managers, committees and accountable owners across Austin Health.
- Design and deliver practical risk and compliance management education, guidance, presentations and capability-building programs.

- Facilitate multidisciplinary risk and compliance improvement activities and support implementation and monitoring of agreed actions.
- Represent Austin Health in relevant health-sector and government risk, compliance, integrity and assurance forums.
- Undertake other activities as directed by the General Counsel.

Selection criteria

Essential knowledge and skills:

- A commitment to Austin Health values: Our actions show we care; We bring our best; Together we achieve; We shape the future.
- Relevant tertiary qualification in business, risk management, governance, audit, compliance, health administration, law or a related discipline.
- Extensive senior experience designing, implementing and improving enterprise risk management and legislative compliance frameworks in a large, complex and highly regulated organisation, preferably within health or the public sector.
- Demonstrated expertise in risk governance, risk appetite, risk profiling, control assessment, treatment planning, compliance obligations management, assurance and executive and Board reporting.
- Demonstrated experience leading a legislative compliance program, including obligations registers, legislative change monitoring, compliance assessments, breach and issue management, remediation and organisational reporting.
- Experience in integrity governance, fraud and corruption control, compliance, internal audit or related assurance disciplines.
- Ability to interpret and apply complex government, legislative, regulatory and policy requirements, including critical infrastructure risk management obligations where applicable.
- Highly developed analytical, conceptual and problem-solving skills, including the ability to identify systemic and emerging risks and compliance issues and translate complex information into clear advice.
- Demonstrated ability to provide authoritative, concise and evidence-informed advice to executives, Boards and Board Committees.
- Exceptional stakeholder engagement, facilitation, influencing, report-writing and presentation skills.
- Capacity to manage competing priorities, establish disciplined annual programs and drive actions to completion through collaboration and influence.
- Demonstrated experience developing organisational risk and compliance capability, accountability and culture.

Desirable but not essential:

- Postgraduate qualification or professional certification in risk management, governance, internal audit, compliance or a related field.
- Knowledge of ISO 31000, ISO 37301, the Victorian Government Risk Management Framework, public sector integrity requirements and contemporary assurance practices.
- Experience with enterprise GRC technology, compliance obligations management, risk analytics and dashboard reporting.

Professional qualifications and registration requirements

Relevant tertiary qualification is required. Professional certification or postgraduate qualification in risk management, governance, internal audit, compliance, law or a related discipline is desirable. No professional registration is required for this role.

Quality, safety and risk – all roles

All Austin Health employees are required to:

- Maintain a safe working environment for yourself, colleagues and members of the public by following organisational safety, quality and risk policies and guidelines.
- Escalate concerns regarding safety, quality and risk to the appropriate staff member, if unable to rectify yourself.
- Promote and participate in the evaluation and continuous improvement processes.
- Comply with the principles of person-centered care.
- Comply with requirements of National Safety and Quality Health Service Standards and other relevant regulatory requirements.

Other conditions – all roles

All Austin Health employees are required to:

- Adhere to Austin Health's core values: our actions show we care, we bring our best, together we achieve, and we shape the future.
- Comply with the Austin Health's Code of Conduct policy, as well as all other policies and procedures (as amended from time to time).
- Comply with all Austin Health mandatory training and continuing professional development requirements.
- Provide proof of immunity to nominated vaccine preventable diseases in accordance with Austin Health's immunisation screening policy.
- Work across multiple sites as per work requirements and/or directed by management.

General information

Cultural safety

Austin Health is committed to cultural safety and health equity for Aboriginal and/or Torres Strait Islander People. We recognise cultural safety as the positive recognition and celebration of cultures. It is more than just the absence of racism or discrimination, and more than cultural awareness and cultural sensitivity. It empowers people and enables them to contribute and feel safe to be themselves.

Equal Opportunity Employer

We celebrate, value, and include people of all backgrounds, genders, identities, cultures, bodies, and abilities. We welcome and support applications from talented people identifying as Aboriginal and/or Torres Strait Islander, people with disability, neurodiverse people, LGBTQIA+ and people of all ages and cultures.

Austin Health is a child safe environment

We are committed to the safety and wellbeing of children and young people. We want children to be safe, happy and empowered. Austin Health has zero tolerance for any form of child abuse and commits to protect children. We take allegations of abuse and neglect seriously and will make every effort to mitigate and respond to risk in line with hospital policy and procedures.