

# Risk management roles and responsibilities



Use this reference to describe roles and responsibilities when it comes to managing risk.

We recommend that you

* tailor them so they belong to your organisation
* be ready to advise and show leadership on how to perform them
* make them part of performance management
* put in place training and communication so they people perform their roles and carry out their responsibilities appropriately
* design your support for your responsible body and executive team so that they can perform their roles and carry out their responsibilities appropriately.

|  |  |
| --- | --- |
| Role | Responsibilities |
| Responsible body *Oversight* | * + Ensures that an appropriate risk management framework is in place and authorises the risk management policy   + Ensures that a positive risk culture is in place   + Defines risk appetite   + Directs strategy and reviews strategic risks   + Reports risks of significance (defined by the board) to the appropriate Minister or department   + Reports state significant risks to the appropriate Minister or department   + Attests that the organisation complies with mandatory requirements of the Victorian Government Risk Management Framework (VGRMF) |
| Audit and Risk Committee (ARC)*Key Advisor to Board* | * + Oversees the risk management framework   + Shows leadership on risk culture   + Makes recommendations for improvement to the responsible body   + Recommends how risk management work should be resourced   + Advises the responsible body on how significant risks in the internal and external context are changing   + Alerts the responsible body to risks they are newly aware of   + Monitors key risk indicators for any trends or signals that risks are increasing   + Oversees the management of key risks and implementation of risk treatment plans   + Reviews the entity’s insurance program and make recommendations to address any gaps in covering insurable risks   + Analyses incidents and events and communicate insights to the responsible body and executive team   + Directs and monitors the internal audit program to assess the effectiveness of internal controls that mitigate risk   + Verifies the attestation statement |
| Risk management sub-committee*Operational role* | * + Monitors the effectiveness of the risk management framework   + Implements improvements to the risk management framework   + Provides expert resources for reviewing operational risk, e.g. clinical risk, financial risk, risk to health and safety, …   + Manages the risk transfer through insurance or third-party contracts   + Assesses risks and reports the assessment to the ARC   + Demonstrates a positive, risk-aware culture to the organisation |
| Internal audit team*Provides assurance to the responsible body* | * + Reports to the ARC that the system of internal control and risk management is effective   + Reports to the ARC on the effectiveness of management of specific risks   + Demonstrates a positive, risk-aware culture to the organisation |
| External audit ***Provides assurance to the community*** | In carrying out its audit role to the parliament and community, external audit provides valuable information about the effectiveness of internal control and risk management systems to the responsible body and ARC in its reports. For many agencies, the external auditor’s job is confined to auditing the annual financial statements. |
| Clinical QualitySub-Committee(Operational) | * + Reports significant clinical risk issues to the responsible body   + Guides the organisation on clinical practice and patient care in line with the Victorian Clinical Governance Framework.   + Oversees development and implementation of clinical risk management processes, aligning with the organisation’s risk management policy and procedures   + Monitors key clinical risk indicators and trends   + Identifies new clinical risks and oversees progress in implementing treatment plans   + Analyses incidents, clinical risk management reports and clinical risk management information in the central risk register   + Reviews the effectiveness of processes for assessing and managing risk, particularly strategic clinical risk   + Demonstrates a positive, risk-aware culture across the organisation |
| Chief Executive Officer | * + Leads the development, implementation and review of the organisation’s risk management policy and procedures, and compliance obligations   + Endorses key policies and procedures for the relevant governing authority   + Ensures the management of risk is adequately resourced   + Monitors the organisation’s internal and external contexts for new or changing risks   + Monitors high risks   + Embeds risk management in strategic and operational planning and reporting   + Ensures that the executive team, and the rest of the organisation, understand their responsibilities when it comes to managing risk   + Demonstrates a positive, risk-aware culture across the organisation   + Oversees communication and reporting to the responsible body and its committees   + Approves the closure of operational risks   + Takes the lead on shared risk, build relationships with other agencies, and engage with stakeholders to manage shared risk effectively |
| Executive team and senior management group | * + Carries out the risk management policy, strategy, and others aspects of the organisation’s risk management framework   + Follows risk management processes   + Participates in the development, testing and embedding of the organisation’s risk management framework and processes   + Monitors risk register and use it as a source of risk management insights   + Watches the organisation’s key risk indicators for changes in the likelihood or consequences of risks   + Watches the organisation’s internal and external context for new risk   + Identifies risk owners for new risks so they can be understood and monitored   + Ensures that risk owners have the knowledge, authority and resources to manage risk effectively   + Communicates risk information back to the organisation   + Informs the Risk and Audit Committee of risks and issues   + Advises responsible body of new risks and changes to strategic risks   + Reports progress of risks to the Board Committee   + Allocates resources to managing risk   + Demonstrate a positive, risk-aware culture across the organisation |
| Chief Risk Officer / Risk Manager | * + Coordinates the periodic review of the risk management policy and other elements of the risk management framework   + Designs processes for managing risk and implement them across the organisation   + Ensures staff members understand their responsibilities with respect to risk management and are supported with training and assistance   + Manages the risk register   + Analyses key risk indicators and the risk register for insights on risk   + Watches the internal and external context for new risk   + Prepares reports to the Audit and Risk Committee and the responsible body   + Coordinates communication and reporting between roles in the organisation’s governance model   + Demonstrates a positive, risk-aware culture across the organisation |
| Managers | * + Manages risk in their area of responsibility and shared risk with other business units and organisations   + Ensures that risks are assessed, controlled, monitored, reported, escalated and closed in line with the organisation’s procedures   + Makes sure their teams understand their responsibility to manage risk and have the skills, capability and resources to do so   + Assesses new risk and monitor change in known risks   + Demonstrates a positive, risk-aware culture across the organisation |
| Staff and volunteers | * + Manages risk within their area of influence   + Follows risk management policy and procedures   + Participates in a risk-aware culture   + Assesses new risk and monitor change in known risks   + Contributes to the continuous improvement of risk management frameworks, processes and culture |