
# Risk management glossary

This glossary provides an overview of terms used throughout the risk management process. They are based on the terms used in the Victorian Government Risk Management Framework (VGRMF).

|  |  |
| --- | --- |
| Term | Description |
| Risk | The effect of uncertainty on objectives.An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.Objectives can have different aspects and categories and be applied at different levels.  |
| Risk culture | Risk culture refers to the system of beliefs, values and behaviours throughout an organisation that shapes the collective approach to managing risk and making decisions. A positive risk culture is one where every person in the agency believes that thinking about and managing risk is part of their job. |
| Risk appetite  | The types and amounts of risk that an agency is willing to accept in the pursuit of its strategic and business objectives. |
| Risk management | Coordinated activities to direct and control an organisation with regard to risk |
| Stakeholder | Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity. |
| Risk source | Element which alone or in combination has potential to give risk to risk. |
| Event | Occurrence or change of a particular set of circumstances.An event can have one or more occurrences and can have several causes and several consequences. |
| Consequence | Outcome of an event.A consequence can be certain or uncertain and can have positive or negative or direct or indirect effects on objectives. |
| Likelihood | Chance of something happening. In risk management, ‘likelihood’ is used to refer to the change of something happening, whether defined, measure or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.  |
| **Term** | **Description** |
| Control | Measure that maintains and / or modifies risk.Controls include, but are not limited to, any process, policy, device, practice, or other conditions and / or actions which maintain and / or modify risk. |
| Residual risk | The risk remaining after risk treatment; also known as retained risk. Can include unidentified risk. |
| Risk analysis | Process to understand the nature of the risk and to determine the level of risk. |
| Risk criteria | Terms of reference against which the significance of risk is evaluated. Based on organisational objectives and internal and external contexts. Risk criteria can be derived from standards, laws, policies and other requirements. |
| Risk evaluation | The process of assessing risk analysis results to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists the decision about risk treatment and needs to consider the risk appetite and risk tolerance of the organisation. |
| Risk event | An occurrence or change of a particular set of circumstances. May have one or more occurrences and can have several causes. An event can consist of something not happening and may also be referred to as an ‘incident’. |
| Risk identification | The process of finding, recognising and describing risks. Involves the identification of risk sources, events and potential consequences. Can involve historical data, theoretical analysis, informed and expert opinions and stakeholder needs. |
| Risk management framework | Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. |
| Risk maturity | The benchmarking of an agency’s risk management framework relative to leading practice |
| Risk profile | A description of any set of risks. The set of risks can contain those that relate to the whole organisation or part of the organisation. |
| **Term** | **Description** |
| Risk management process | Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| Key risk indicator | A metric used to measure the likelihood of a risk event or the effectiveness of controls that prevent a risk event. They provide an early signal of increasing risk exposures. |
| Risk register | Record of information about identified risks. |
| Risk strategy | A risk management strategy (may be referred to as the risk plan or risk policy) that outlines and describes the key elements of the risk management framework. It specifies the approach, the management components and resources to be applied to the management of risk. |
| Risk tolerance | The organisation’s readiness to bear the risk after risk treatment in order to achieve objectives. Risk tolerances are based on the maximum level of acceptable risk and may be expressed in various ways depending on the nature of the risk. |
| Risk treatment | Process to modify risk, may include deciding to take, retain, avoid, remove, change or share the risk. Risk treatments that deal with negative consequence may also be referred to as risk mitigation. |
| Agency | Any department or public body as defined in the *Financial Management Act 1994*. |
| Accountable Officer | In relation to a department or public body, means the accountable officer for that department or public body as determined under section 42 of the *Financial Management Act 1994*. |
| Audit Committee | The Standing Directions of the Minister for Finance require that an audit committee be appointed to oversee and advise the department or agency on matters of accountability and internal control. This committee is a subset of the Responsible Body (or Board) which has been formulated to deal with issues of a specific nature. |
| Responsible Body | For a department, the accountable officer is the responsible body. For other agencies, it is the board or the person or body with ultimate decision making authority. |