Risk Register Guidance Notes

The following note is a guide on how Risk is managed within TVCA **for information only** and is not a reflection of how we expect others to manage risk within their organisation.
If others adopt the same approach, TVCA accept no liability for any repercussions of doing so.

Context of Risk Management

The ISO standard on Risk Management describes ***risk*** as "*the effect of uncertainty on objectives".* Risk is the probability of an internal or external situation (an incident) with the potential to impact successfully achieving objectives, delivering services, or capitalising on opportunities.

Risks are an everyday occurrence that could potentially positively or negatively impact the ability to meet obligations to stakeholders and the community, while some risks cannot be fully eliminated, they can be identified, controlled, and managed to an acceptable level.

Risk management is defined as *"the coordinated activities to direct and control an organisation with regard to risk".*

Risk Identification

The purpose is to identify all risks; what, when, why and how incidents might impact on the achievement of objectives.

A systematic process includes working through each goal, objective, or planned implementation action, identifying the things that may inhibit, detract from, or prevent the achievement of the goal or enhance the opportunity to meet the objective. A range of tools and approaches to determine potential risks, including:

- Team based brainstorming with experienced and knowledgeable staff.
- Structured techniques (such as SWOT analysis, process mapping, flow charting, systems analysis, or operational modelling)
- Annual strategic, project planning, budget, and risk identification workshops.
- Regular compliance reviews (internally and externally).

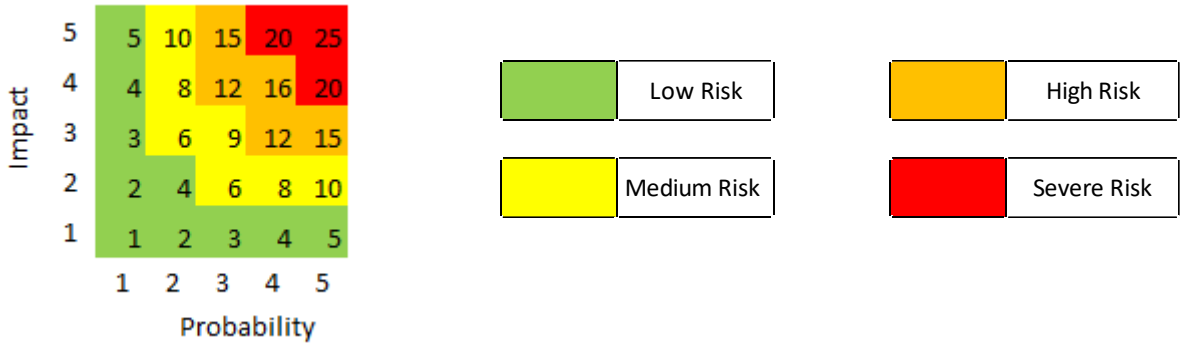
A risk event relates to the failure of people, processes, and systems or from external factors (e.g., fire, flood, assault, or damage).

Recording identified risks occurs through the development of a description of the risk and entry into the appropriate risk register. The risk description should contain a statement of the risk and include those factors which could cause or contribute to the occurrence of the risk event.

Risk analysis

Analysis involves developing an understanding of the risk, the likelihood of the risk occurring and the full range of potential impact/consequences. Identification of likelihood and impact is not scientific: it is a qualitative exercise based on perception and history.

Risk is calculated using a 5 x 5 impact and probability matrix which is aligned to a risk status.



Inherent Risk Score

The initial analysis provides the inherent risk rating which is made up by considering the likelihood and impact. At this stage, the analysis assumes that all controls have failed or there were no effective controls in place.

Residual Risk Score

When the controls have been assessed and rated, the residual risk (the amount of risk left over after inherent risks have been reduced by controls) rating is determined.

Risk Registers

Risk registers provide a mechanism for documenting, managing, monitoring, reviewing, updating, and reporting risk information. Risk register design, use and related processes are developed and maintained by the Risk Manager.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

Risk response

Treat the risk – implement a control/action plan to mitigate, discourage, identify and/or limit the impact and likelihood of the risk occurring.

Transfer the risk - Risk transfer may be achieved by taking out insurance to facilitate financial recovery against the realisation of a risk**:**

- Compensating a third party to own the risk because the other party is more able to effectively manage the risk.
- Risk may be wholly transferred, or partly transferred (that is, shared).
- It is important to remember that it is almost impossible to transfer risk completely. In almost all risk sharing arrangement, a degree of the original risk remains and there is inevitably financial or other consideration for the sharing of the risk. In addition, a new risk is inherited; one dependent on a third party to manage the original risk.

Terminate the risk - Some risks may only return to acceptable levels if the activity is terminated. Seek to eliminate the event leading to the risk.

Tolerate the risk - Seeks to reduce (or eliminate) the impact, probability, or both, of the risk to some acceptable level. A risk may be accepted because:

- The probability or consequences of the risk is low or minor.
- The cost of treating the risk outweighs any potential benefit.
- The risk falls within the agency's established risk appetite and/or tolerance levels.

Target Risk Score

Each risk should be allocated a target risk score which every endeavour must be made to attain. This gives confidence that the threat/opportunity is being managed at the optimal level.

Action Plans

Where control weaknesses are identified and the decision is taken that further mitigation is required (i.e., the residual exposure is not accepted), an action plan must be established.

For project-based risk assessments, the risk treatment action plan provides the project manager with a tool to continuously monitor project improvement through the implementation of the plan. Issues and delivered risks identified through the course of the project must be assessed and included in the project risk register, having gone through the full risk assessment process outlined above. This will ensure the continuing relevance of the risk assessment.
All actions must be:

- Owned: who is responsible for ensuring the action is addressed
- Specific: the exact activities that will be undertaken

- Timely: must be completed within appropriate time frames, commensurate with the significance of the gap/weakness
- Achievable: the action/activities must be realistic to ensure appropriate mitigation
- Measurable: it must be possible to quantify the action or have a means of assessing progress
- Justified: can demonstrate a further reduction in the residual likelihood and/or impact
- Governed: tracked, managed, and reported.