

Risk register – Example

A **risk register** is used by governing bodies to oversee and manage enterprise-level strategic risks through monitoring controls and residual risks. It can also be used by the provider to manage day-to-day operational risks. **Note:** items included in the risk register below are **examples only**. It is the responsibility of each provider to develop and maintain governance tools as appropriate to their own unique circumstances.

Risk register

Risks are rated and coloured coded based on current controls and using a risk matrix.

Owner should be the role accountable for the effective management of the risk.

ID	Risk Description	Risk Type	Causes	Impacts	Key Controls	L	C	Current Rating	Owner	Action	Target Rating
1	Serious privacy breach	S	Poor processes and training	Reputational damage Loss of trust	File restrictions Training Information management and privacy processes	Unlikely	Major	V High	CEO/ Director Legal	Develop new procedures Upgrade content management system	Moderate
2	Fraud and/or staff misconduct	S	No employee screening Poor policies / processes	Reputational damage Lose accreditation Financial loss	Monthly financial reconciliations Employee screening Purchasing policies and procedures	Unlikely	Severe	High	CFO	Strengthen financial controls	Low
3	Occupational violence	O	Poor training Lack of procedures	Physical/ mental Injury to staff	Clinical care procedures	Possible	Major	V High	Director Clinical Care	Implement targeted training for all employees	High
4	Sub-standard clinical practices	O	Poor clinical practices Inadequate resources	Harm to consumers Reputational damage	Supervision by qualified nurses Clinical procedures	Possible	Severe	High	Director Clinical Care	Review workforce structure and uplift skills	Moderate

Having a unique ID helps to track risks.

Risk type shows whether it is strategic (S) or operational (O). Risks can be extracted into separate registers.

Causes should list reasons why the risk might eventuate.

Impacts should list the main effects if the risk occurs.

Key controls are the main systems, processes and practices in place that prevent or mitigate the impacts of a risk. Controls can be preventative, i.e. prevent the risk from occurring or detective, i.e. detect irregularities or errors that may indicate the risk has already eventuated, therefore enabling the impacts to be promptly managed and contained.

Likelihood (L) of risk eventuating based on current controls and using risk matrix likelihood descriptors.

Consequence (C) if risk eventuates based on current controls and using risk matrix consequence descriptors.

The risk treatment action briefly describes the activities to treat the risk to further reduce the likelihood and/or consequence.

Risks are re-rated based on an assumption the risk actions are fully implemented. The target rating is sometimes referred to as 'Residual Risk'.