1. **Statement**

All staff have responsibilities for proactively identifying, reporting, managing and communicating risks and opportunities in a timely manner. All risks shall be assessed using the Risk Assessment and Treatment Guideline.

2. **Scope**

This policy applies to all employees, contractors and consultants within the Department of Health.

3. **Requirements**

This implementation standard identifies the minimum mandatory requirements for the governance and management of risks, including the identification, reporting and communication of risk. It also identifies the responsibilities of individual positions in relation to these requirements within the Department of Health (the department).

3.1 **Overview**

The Director-General shall establish and maintain appropriate systems of internal control and risk management in accordance with the *Financial Accountability Act 2009*, *Financial and Performance Management Standard 2009* and *Public Sector Ethics Act 1994*.

3.2 **Governance**

The Director-General and Department Leadership Team (DLT) members shall determine and communicate the department’s risk appetite to effectively manage and prioritise risks to meet obligations and provide oversight of risk management within the department.

Oversight and governance responsibilities shall be delegated to peak governance bodies and executive teams where appropriate (Refer to 3.5.3).

3.3 **Risk Information**

Risk Owners and Risk Coordinators shall ensure that all risk information is recorded in QHRisk with the exception of project risks where they are otherwise recorded in project management software. When identifying potential project risks please refer to the [Guide for Assessing Project Risk](#).

Risks shall be assessed and managed using the Risk Analysis Matrix and Risk Assessment and Treatment Guideline with the exception of health system risks (Refer to 3.4)

Minimum risk information to be recorded includes:

- a risk description (Refer to Quick Guide for Writing a Risk Description)
- a single risk owner (by position not name). When there is shared responsibility the ‘person most responsible’ will take the lead as the risk owner
- a risk review date (Refer to Quick Guide for Risk Reviews)
- current control/s which clearly define actions that are currently in place
• risk treatment/s (additional controls) which clearly define agreed actions intended to be undertaken to further moderate the risk where necessary
• an assessment to determine the level of risk rating (current and projected) in accordance with the Risk Assessment and Treatment Guideline
• a treatment owner be assigned to each risk treatment (additional control)
• a treatment due date is assigned to each risk treatment to identify when the risk treatment is to be implemented/completed
• evidence of consideration and decision on risk treatment and effectiveness

3.4 Health system risk (system risk)
The department is responsible for leading, providing stewardship and managing the performance of the State’s health system. In line with this, health system risk management is the responsibility of the department through effective health system partnerships, governance arrangements and clear responsibilities.

Accountable executives and managers shall contribute to identification, management and assessment (in accordance with the Health System Risk Management Framework) for system risks that:

• require moderation by the department and multiple Hospital and Health Services.
• manifest from the delivery of national and state public health outcomes and critical system wide functions and programs. Need to be managed dynamically, across divisions, business units and organisational boundaries in a way that is congruent with the strategic direction and priorities of the Queensland public health system.

In addition to contributing to the management of system risks, organisations within the health system also have responsibilities in supporting the management of any risks shared with other health system entities where there are shared objectives or through for example service agreements, contracts and shared programs.

Health system governance bodies shall ensure risk management in their areas of accountability is effectively integrated and reporting occurs in accordance with the responsibilities set out in this standard (Refer to 3.5).

System risks shall be identified assessed, managed and communicated across the health system in accordance with the Health System Risk Management Framework.

3.5 Responsibilities

3.5.1 The Deputy Directors-General/Chief Executives of divisions/business units shall incorporate risk management into organisational processes in the following ways:

• as a standing agenda item for executive, senior management and governance group meetings
• in the development or review of strategic and operational plans
• in new or revised project plans, submissions and briefs
• in new or revised allocation of significant resources
• in purchasing, procurement and contract arrangement decisions
• in the review of significant issues or events
• in performance reporting and contract management
in compliance with legislation and Government policy
In change management

3.5.2 The Deputy Directors-General/Chief Executives of divisions/business units shall:
• promote and oversee the implementation of an integrated approach to risk management
• nominate a Risk Coordinator for their division/business unit to represent the division/business unit on the Risk Management Working Group
• establish local processes that are consistent with the Risk Management Policy, Standard and Guideline and the Health System Risk Management Framework
• ensure staff are aware of their roles and responsibilities to ensure risk management is undertaken effectively
• maintain an active risk register in QHRisk for their area of responsibility (Refer to Quick Guide for QHRisk)
• contribute to risk management including risk identification, communication, monitoring and oversight

3.5.3 Department of Health executive committees and boards shall:
• oversee and monitor areas of risk within their responsibility
• drive better governance outcomes by applying the principles of risk management to decision-making and discussions

3.5.4 The Department of Health Audit and Risk Committee shall:
• ensure that the committee provides independent assurance and assistance to the Director-General regarding the Department’s risk, control and compliance frameworks and external accountability responsibilities as prescribed in relevant legislation and standards

3.5.5 Department of Health executives and senior management officers of divisions/business units shall:
• identify and monitor areas of risk within their responsibility
• regularly review and manage risks and ensure an integrated approach to risk management is used
• contribute to risk management and provide support and advice to the risk owner and officer/s responsible for coordinating actions such as implementing agreed risk treatments, monitoring outcomes and reassessing risks
• notify the appropriate department executive committee and/or boards of any organisational risks or of risks with relevance to the committee and/or boards function in accordance with the Risk Assessment and Treatment Guideline

3.5.6 Department of Health project, program and portfolio governance bodies shall:
• incorporate risk as a standing agenda item for all project, program and portfolio board meetings
• support and enable project and program teams to effectively identify and manage risks, ensuring treatment plans are coordinated, regularly reviewed, outcomes reported and risk reassessed in accordance with the Risk Assessment and Treatment Guideline
• notify their appropriate Department of Health executive officer (or Senior Responsible Officer) and / or executive committee of any organisational risks or of risks with relevance to other business areas or functions in accordance with the Risk Assessment and Treatment Guideline
3.5.7 The Chief Risk Officer shall:

- develop an effective risk framework; coordinate and support its implementation; and monitor evaluate and report on its effectiveness
- provide advice in relation to risk management
- establish a community of practice to support implementation and ensure best practice advice and risks are effectively communicated and understood at appropriate levels and business areas across the department and health system
- establish and maintain the department’s risk profile and identify emerging trends with the assistance of the Risk Management Working Group
- ensure the department’s risk profile and other relevant risks are communicated to the Department Leadership Team/Senior Leadership Team in accordance with established reporting timetable and the DLT direction

3.5.8 Risk Owners shall:

- ensure accurate and complete risk information is recorded in the risk register.
- assess departmental and system-wide risks using the Risk Assessment and Treatment Guideline
- review and moderate risks in accordance with the Risk Analysis Matrix (Refer to Response to Risk table within Risk Analysis Matrix)
- review their risk portfolio following a significant change to the risk or risk context
- ensure risks are managed to an as low as reasonably practicable (ALARP) level and closed when appropriate
- work with risk coordinators to ensure risks are communicated in accordance with the Risk Analysis Matrix and the Decision Map
- work with other business areas that may be able to assist with the moderation of the risk

3.5.9 Risk Coordinators for divisions/business units shall:

- work with risk owners to record accurate and complete risk information in the risk register
- support risk owners in the analysis, recording and communication of risk
- act as the QHRisk SuperUser for Divisions/business units (Refer to Quick Guide for QHRisk)
- monitor and coordinate the identification, analysis, review and reporting of risks produce risk reports for chief executives, executive committees and risk owners as required
- ensure risk information on the system (QHRisk) is up-to-date prior to the generation of the executive risk profile report
- participate in the Risk Management Working Group on behalf of their Division/business units

3.5.10 Managers (Operational/Program/Project) shall:

- identify and monitor areas of risk within their area of responsibility
- carry out risk owner responsibilities as applicable
- proactively communicate risks with relevance to other business areas or functions to their responsible executive and/or governance board
3.5.11 All staff shall:

- proactively identify and manage risks and opportunities within their area of responsibility in accordance with the Risk Management Policy
- communicate or escalate risks outside of their area of responsibility to the prospective risk owner in writing
- proactively communicate relevant risk information to other business areas or functions to their responsible executive and/or governance board
- Adhere to and support management in the implementation of risk controls and treatments

4. Supporting documents

- Risk Management Policy (QH-POL-070)
- Risk Assessment and Treatment Guideline (includes Risk Analysis Matrix) (QH-GDL-070-1-1)
- Department of Health Risk appetite statement
- Department of Health Executive risk decision map and communication guide
- Health System Risk Management Framework
- Risk treatment planning sheet
- Quick guide for writing a risk description
- Quick guide for risk reviews
- Quick guide for QHRisk
- A Guide for assessing project risk
- AS/NZS 5050:2010 Business continuity – Managing disruption-related risk

5. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Control</td>
<td>See ‘Treatment’</td>
</tr>
</tbody>
</table>
| As low as reasonably practicable (ALARP) | Risk management is not about eliminating risks but about managing them to as low as reasonably practicable level. That is, risk is tolerable if:  
  - further risk reduction is impractical  
  - if cost of further risk reduction would exceed the improvements/benefits gained  
  - if no treatment/control is available |
| Branch/team risks           | Risks that may affect the effectiveness of a branch or team in delivering its required outcomes. Branch risks should be regularly reviewed and communicated with the appropriate Divisional leadership team.  
  A branch risk may be transferred to a divisional level risk profile if it requires moderation by multiple branches/teams in the division or is identified as a risk shared by more than one branch/team in that division. |
| Control | Any action taken to manage/modify risk. (Based on AS/NZS ISO 31000:2009)  
Controls may include process, policy, device, practice or other actions which modify risk. Any action that reduces the likelihood of a risk occurring and/or reduces its consequence if it does occur. Controls may be selected based on the hierarchy of risk control such as elimination, substitution, isolation and/or reduction. |
|---|---|
| Corporate risks | Major risks that may affect the department’s ability to execute its Strategic Plan and/or require cross divisional moderation. If realised, corporate risks affect strategic objectives and operational plan delivery.  
Corporate risks are typically monitored by the Department Leadership Team (DLT), executive committees/ boards and governing bodies or functional working groups (including program and project boards). They are managed collectively on a functional basis due to their interdependencies.  
Divisional risks may be transferred to the corporate risk profile where cross-divisional moderation is required. |
| Divisional/business unit risks | Risks that may affect the division/business units ability to execute their operational plan and/or require divisional oversight (e.g. by the senior leadership team) or moderation by multiple branches/teams in the division/business unit.  
These risks should be regularly monitored and reviewed by the division/business unit’s leadership team.  
Where a risk requires cross divisional moderation or affects multiple divisions/business units the risk may be transferred to the corporate risk profile.  
A division risk profile may also only include those risks posed by the program or project to the business. Risk to the portfolio, program or project may be subject to other specified governance oversight. Refer to definition for program/project risks. |
| Executive Risk Profile | The Executive Risk Profile is made up of Strategic, Corporate and System risks. This profile is regularly provided to DLT for monitoring and oversight. |
| Issue | A present problem requiring immediate resolution and/or action.  
Consequences have already occurred at least once. |
| Peak governance bodies / Audit and Risk Committee / Department Leadership Team | The Department of Health and health system governance is supported by peak governance bodies (committees and forums) which sit across a three tier structure. These are sometimes referred to as executive committees.  
The Audit and Risk Committee is a Tier 1 committee. The Department Leadership Team membership includes the Director-General, Deputy Director-General/Chief Executives across the department and is a Tier 2 committee. |
| Program/Project risks | Risks that may affect or are created by objectives/deliverables of a defined program or project. These risks are to be regularly reviewed and communicated with the project executive (Senior Responsible Officer) and/or the program/project board or program office.  
Risk outside the delegations of the program or project and those risks which may pose a risk to the delivery of an objective or strategy in the Strategic Plan are to be reported and/or escalated to an appropriate level if management. This may result in the risk transferring to the corporate risk profile for moderation. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>QHRisk</td>
<td>An online risk management information system, accessible through the Queensland Health intranet, to assist risk coordinators and managers to identify, analyse, manage and report on risks within their areas of responsibility and accountability.</td>
</tr>
<tr>
<td></td>
<td>All risks must be recorded in the QHRisk with the exception of project risks where they are recorded in project management software.</td>
</tr>
<tr>
<td>Risk</td>
<td>Effect of uncertainty on objectives. (Sourced from AS/NZS ISO 31000:2009)</td>
</tr>
<tr>
<td></td>
<td>An effect is a deviation from the expected – positive and/or negative.</td>
</tr>
<tr>
<td></td>
<td>Objectives can be strategic, operational or functional (such as financial, fraud, clinical or OHS) and can apply at different levels (such as system, corporate, division/business unit, branch/team, program/project).</td>
</tr>
<tr>
<td>Risk Analysis Matrix</td>
<td>Tool used to determine the level of risk expressed in terms of the combination of consequence(s) and likelihood. Refer to Risk Assessment and Treatment Guideline.</td>
</tr>
<tr>
<td>Risk Appetite</td>
<td>Amount and type of risk that management within an organisation are willing to pursue or retain. (Sourced from ISO 73:2009)</td>
</tr>
<tr>
<td>Risk Coordinator</td>
<td>A position responsible for:</td>
</tr>
<tr>
<td></td>
<td>• supporting the implementation of the Risk Management Policy,</td>
</tr>
<tr>
<td></td>
<td>• supporting risk owners in the analysis, recording and communication of risks</td>
</tr>
<tr>
<td></td>
<td>• acting as QHRisk SuperUser for their division or business unit</td>
</tr>
<tr>
<td></td>
<td>• participation in the Risk Management Working Group.</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>A person with the accountability and authority to manage a risk.</td>
</tr>
<tr>
<td></td>
<td>A position with the most responsibility for the risk.</td>
</tr>
<tr>
<td></td>
<td>Most responsible means able to coordinate risk treatments and engage with other business areas that may have some responsibility for an aspect of the risk and/or delegation to support risk treatment.</td>
</tr>
<tr>
<td></td>
<td>As a matter of principle, each risk has only one Risk Owner.</td>
</tr>
<tr>
<td>Risk Rating</td>
<td><strong>Current Risk Rating</strong></td>
</tr>
<tr>
<td></td>
<td>A level of risk (= likelihood x consequence/s) assessed at the time when the risk is identified and as a part of the review of the effectiveness of any implemented controls.</td>
</tr>
<tr>
<td></td>
<td><strong>Projected Risk Rating</strong></td>
</tr>
<tr>
<td></td>
<td>Expected level of risk on completion of risk treatments The term is synonymous with the terms ‘Residual Risk’ and ‘Retained Risk’.</td>
</tr>
<tr>
<td>Risk Register</td>
<td>A record of risk information is to be recorded and maintained in an active risk register.</td>
</tr>
<tr>
<td></td>
<td>All risks must be recorded in the QHRisk with the exception of project risks where they are recorded in project management software.</td>
</tr>
<tr>
<td>Strategic risks</td>
<td>Risks that may affect or are created by the department’s Strategic Plan and strategic objectives. These risks are typically owned and monitored by the DLT.</td>
</tr>
<tr>
<td>System risks</td>
<td>Risks that may affect or are created by the overarching Queensland Health strategic direction and objectives. These risks require moderation by Department of Health and multiple HHSs and are typically owned and monitored by the DLT.</td>
</tr>
</tbody>
</table>
Treatment Any process that involves actions which manage/modify risk. (Based on AS/NZS ISO 31000:2009)

A risk treatment is an approved task/activity/program/project or other initiative that when implemented/completed will reduce the likelihood and/or consequence of the current level of risk. A risk treatment may also be to improve, maintain or monitor the effectiveness of current controls.

Once implemented/completed the risk treatment may become a risk control.

Treatment Owner A position vested with the responsibility for a treatment/s. In some circumstances the Risk Owner and Treatment Owner can be the same position. In other circumstances, multiple treatments may be endorsed and allocated to different Treatment Owners, all reporting to the one Risk Owner.

Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>2013</td>
<td>Implementation Standard for Risk Management</td>
</tr>
<tr>
<td>Version 1.3</td>
<td>17 June 2016</td>
<td>Minor changes to system risks definition.</td>
</tr>
<tr>
<td>Version 1.4</td>
<td>24 February 2017</td>
<td>Review post risk maturity evaluation</td>
</tr>
</tbody>
</table>

Appendix 1: Responsibilities

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibility</th>
<th>Audit criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>All staff</td>
<td>Proactively identify, report and manage risks and opportunities.</td>
<td>Compliance with the Risk Management Policy.</td>
</tr>
<tr>
<td>Audit and Risk Committee</td>
<td>Provide independent assurance and advice that legislative responsibilities are being met.</td>
<td>Advice is provided on the effectiveness of the risk management system.</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>Policy custodian for the Risk Management Policy. Maintain the department's risk profile and ensure it is communicated to DLT in accordance with established reporting timetables. Monitor, evaluate and report on risk management framework implementation. Establish a risk management community of practice.</td>
<td>Risk Management Policy is current and aligned with department objectives.</td>
</tr>
<tr>
<td>Department of Health executive committees and/or boards</td>
<td>Overseer and monitor areas of risk within their responsibility by maintaining a risk register. Drive better governance outcomes by applying the principles of risk management to decision-making and discussions.</td>
<td>Endorsed Terms of Reference includes responsibilities outlined in this standard. Compliance with Risk Assessment and Treatment Guideline.</td>
</tr>
<tr>
<td>Department of Health executives and senior management officers</td>
<td>Identify and monitor areas of risk within their responsibility. Regularly review and manage risks and ensure an integrated approach to risk management is used. Contribute to risk management and provide support and advice to the risk owner and officer/s responsible for coordinating actions such as implementing agreed risk treatments, monitoring outcomes and reassessing risks. Report organisational risks and risks with relevance to the executive committees and/or boards</td>
<td>Compliance with Risk Assessment and Treatment Guideline.</td>
</tr>
<tr>
<td>Department of Health project, program and portfolio governance bodies</td>
<td>Support and enable effective risk management within divisions/business units. Ensure treatment plans are effective and coordinated and that risks are monitored and reassessed. Report organisational risks and risks with relevance to other business/functional areas to Department of Health executive officer (or Senior Responsible Officer) and / or executive committee.</td>
<td>Compliance with Risk Assessment and Treatment Guideline.</td>
</tr>
<tr>
<td>Department Leadership Team (DLT)</td>
<td>Determine the department’s risk appetite. Monitor the Executive Risk Profile.</td>
<td>Risk appetite is discussed on the DLT agenda.</td>
</tr>
<tr>
<td>Health System Risk Working Group</td>
<td>Ensure the communication and monitoring of health system wide risks are shared/managed across health system participants.</td>
<td>Endorsed Terms of Reference.</td>
</tr>
<tr>
<td>Managers (Operational /program/project)</td>
<td>Maintain a risk register for their area of responsibility. Proactively communicate risk with relevance to other areas to their respective executive or governance body.</td>
<td>Compliance with Risk Assessment and Treatment Guideline.</td>
</tr>
<tr>
<td>Risk and Governance Unit</td>
<td>Provide advice on the application of the Risk Management Policy. System administrator for QHRisk.</td>
<td>Accurate advice is provided in a timely manner.</td>
</tr>
<tr>
<td>Risk Coordinator</td>
<td>Support Risk Owners in analysis, recording, reviewing and reporting of risks. Produce risk reports as required. Act as the QHRisk SuperUser for division/business unit.</td>
<td>Risk Management Policy implemented across the divisions and business units.</td>
</tr>
<tr>
<td>Risk Management Working Group</td>
<td>Support the effective implementation of the department’s risk management framework</td>
<td>Endorsed Terms of Reference.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>Record and maintain accurate risk information. Manage risks within defined tolerances and delegations.</td>
<td>Risk reviews are conducted. Management actions are within delegations.</td>
</tr>
</tbody>
</table>