All staff have responsibilities for proactively identifying, reporting and managing risks and opportunities.

Departmental, system wide and project risks shall be assessed using the Procedure for Risk Assessment and Treatment.

Risk owners will review their risks within defined timeframes.

An active risk register will be maintained in QHRisk.

Risk Management

Implementation Standard for Risk Management

1. Purpose
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).

2. Scope
This standard applies to all Department of Health employees and contracted staff (permanent, temporary and casual) employed in the department’s divisions and commercialised business units.

3. Supporting documents
Authorising Policy and Standard/s:
- Risk Management Policy

Procedures, Guidelines and Protocols:
- Procedure for Risk Assessment and Treatment (includes Risk Analysis Matrix, Department of Health Executive Risk Decision Map and Communication Guide V1.2 and the Risk Treatment Planning Sheet)
- Quick Guides – library of Quick Guides available on QHEPS on risk management topics
- Department of Health Executive Risk Decision Map and Communication Guide V1.2

Forms and templates:
- Risk Treatment Planning Sheet

4. Related documents
5. **Requirements**

5.1 **Legislative Requirements**

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

5.2 **Governance and Accountabilities**

5.2.1 The Directors-General and Department Management Team (DMT) members shall determine and communicate the departments risk appetite to effectively manage and prioritise risks to meet obligations.

5.2.2 The Deputy Directors-General/Chief Executives of accountability areas 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.

5.2.3 The Deputy Directors-General/Chief Executives of accountability areas shall:

- promote and oversee the implementation of an integrated approach to risk management
- nominate a Risk Coordinator for their accountability area to represent the Division/Commercialised Business Unit (CBU) on the Risk Management Working Group
- establish local processes that are consistent with the Risk Management Policy for identifying, communicating, reporting and managing risks and opportunities in accordance with the Procedure for Risk Assessment and Treatment and Department of Health Executive Risk Decision Map and Communication Guide V1.2 (Decision Map)
- 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 (see Quick Guide for QHRisk)
- contribute to risk management including risk identification, communication, monitoring and oversight.
5.2.4 Department of Health executives, executive committees, senior management and governance groups in accountability areas 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.

5.2.5 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 Procedure for Risk Assessment and Treatment
- notify DMT/SMT of any organisational risks or of risks with relevance to other business areas or functions in accordance with the Procedure for Risk Assessment and Treatment.

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

5.2.7 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 Risk Management Working Group to aid implementation and ensure risks are effectively communicated, monitored and understood at appropriate levels and business areas across Divisions and CBUs
- 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 DMT/SMT in accordance with established reporting timetable and the Decision Map
- establish the Health System Risk Working Group.
5.2.8 All staff shall:

- proactively identify and manage risks and opportunities 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 risks with relevance to other business areas or functions to their responsible executive and/or governance board.

5.3 Risk Information

5.3.1 Risk Owners and Risk Coordinators shall ensure that risk information is recorded in QHRisk and includes, at a minimum:

- a risk description (see 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 (see 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
- a responsible position assigned to each risk treatment (additional control)
- an assessment to determine the level of risk rating (current and projected) in accordance with the Procedure for Risk Assessment and Treatment.

**Note:** QHRisk must be used to record all risks, including program and portfolio risks. The only exception to this requirement is project risks which may be managed as part of an integrated project management software solution.

5.3.2 Risk Owners shall:

- record accurate and complete risk information in the risk register
- assess departmental and system-wide risks using the Procedure for Risk Assessment and Treatment
- review and moderate risks in accordance with the Risk Analysis Matrix (see Response to Risk table)
- 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’ level and closed when appropriate
- work with risk coordinators to ensure risks are communicated in accordance with the Risk Analysis Matrix and executive risk profile requirements.
5.3.3 Risk Coordinators for accountability areas shall:
- support risk owners in the analysis, recording and communication of risk
- act as the QHRisk superuser for the accountability area (see Fact Sheet for QHRisk)
- monitor and coordinate the identification, analysis and reporting of risks
- produce risk reports for chief executives, executive committees and risk owners as required and consistent with the Risk Analysis Matrix
- produce risk reports to inform the executive risk profile at monthly intervals or as required
- participate in the Risk Management Working Group on behalf of their Division/CBU.

5.3.4 Contract managers, service managers and project managers shall:
- maintain a risk register for their project, program or contract arrangement
- ensure appropriate risk monitoring and governance
- 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.

5.5 Health System Risk (system risk)

5.5.1 The Chief Risk Officer shall establish and maintain a Health System Risk Working Group to ensure system risks are effectively communicated, monitored and understood across the health system.

5.5.2 A risk which is identified for sharing or transferring across the health system shall be notified to the Chief Risk Officer for consideration by the Health System Risk Working Group.

5.5.3 Accountable executives and managers shall contribute to identification, management and assessment (in accordance with health system risk tools) for risks that:
- relate to the overarching Queensland Health objectives and/or overall system effectiveness and efficiency
- require coordination between accountability areas across the department and/or multiple Hospital and Health Services (system risk) or with other government departments (see the Health System Process Map)

5.5.4 Health System Governance Bodies shall ensure risk management in their areas of accountability is effectively integrated and reporting occurs in accordance with the Procedure for Risk Assessment and Treatment.
6. **Review**
   This Standard is due for review on: 6/11/17
   **Date of Last Review:** 6/11/14

**Supersedes:**
Implementation Standard for Risk Management (QH-IMP-070-1:2013)

7. **Business Area Contact**
   Risk and Governance Unit, Governance Branch and Legal Branch, Department of Health
## 8. 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>Chair, 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</td>
<td>Risk Management Policy is current and aligned with department objectives</td>
</tr>
<tr>
<td></td>
<td>• Maintain the department’s risk profile and ensure it is communicated to DMT in accordance with agreed timetable</td>
<td>Risk Management Policy is current and aligned with department objectives</td>
</tr>
<tr>
<td></td>
<td>• Monitor, evaluate and report on risk management framework implementation</td>
<td>Risk Management Policy is current and aligned with department objectives</td>
</tr>
<tr>
<td></td>
<td>• Establish the Risk Management Working Group</td>
<td>Risk Management Policy is current and aligned with department objectives</td>
</tr>
<tr>
<td></td>
<td>• Establish the Health System Risk Working Group</td>
<td>Risk Management Policy is current and aligned with department objectives</td>
</tr>
<tr>
<td>Contract Managers, Service Managers and Project Managers</td>
<td>• Maintain a current risk register for their accountability area</td>
<td>Compliance with Procedure for Risk Assessment and Treatment</td>
</tr>
<tr>
<td></td>
<td>• Proactively communicate risk with relevance to other areas to their respective executive or governance body</td>
<td>Compliance with Procedure for Risk Assessment and Treatment</td>
</tr>
<tr>
<td>Department of Health Project, Program and Portfolio governance bodies</td>
<td>• Support and enable effective risk management within accountability areas</td>
<td>Compliance with Procedure for Risk Assessment and Treatment</td>
</tr>
<tr>
<td></td>
<td>• Ensure treatment plans are effective and coordinated and that risks are monitored and reassessed</td>
<td>Compliance with Procedure for Risk Assessment and Treatment</td>
</tr>
<tr>
<td></td>
<td>• Report organisational risks and risks with relevance to other business/functional areas to DMT/SMT.</td>
<td>Compliance with Procedure for Risk Assessment and Treatment</td>
</tr>
<tr>
<td>Deputy Director-Generals/Chief Executives</td>
<td>• Incorporate risk management into management processes</td>
<td>Local processes reflect Risk Management Policy requirements.</td>
</tr>
<tr>
<td></td>
<td>• Establish local processes consistent with the Risk Management Policy</td>
<td>Risk Coordinator nominated</td>
</tr>
<tr>
<td></td>
<td>• Nominate a Risk Coordinator within their area of accountability</td>
<td>Risk Coordinator nominated</td>
</tr>
<tr>
<td>Director-General</td>
<td>• Fulfil legislative responsibilities under the <em>Financial Accountability Act 2009</em></td>
<td>System of risk management implemented</td>
</tr>
<tr>
<td>Department Management Team</td>
<td>• Determine the departments risk appetite</td>
<td>Risk appetite is discussed on the DMT agenda</td>
</tr>
<tr>
<td></td>
<td>• Monitor the risk profile</td>
<td>Risk appetite is discussed on the DMT agenda</td>
</tr>
</tbody>
</table>
9. Definitions of terms used in the policy and supporting documents

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition / Explanation / Details</th>
<th>Source</th>
</tr>
</thead>
</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 relate to the effectiveness of a Branch or team in delivering its required outcomes. Branch risks should be regularly reviewed and communicated with the Divisional/Agency leadership team.  
A Branch risk may be transferred to Divisional/Agency if it requires moderation by multiple Branches/teams in the Division/CBU or is identified as a risk shared by more than one Branch/team in the Division. | (AS/NZS ISO 31000:2009) |
| Consequence | Outcome of an event effecting objectives. | (AS/NZS ISO 31000:2009) |
| Control | Measure that is modifying risk.  
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. | (AS/NZS ISO 31000:2009) |
### Corporate risks

Risks that relate to the delivery of the Strategic Plan and/or require cross divisional/CBU moderation. If realised, corporate risks effect strategic objectives and operational plan delivery.

Corporate risks are typically identified by the Department Management Team (DMT), functional working groups or executive committees/boards and governing bodies. This includes program and project boards. Corporate risks may also be transferred from Division/CBUs where cross-divisional moderation is required.

Corporate risk includes specific functions required by the DMT such as OHS and fraud risk. These risks are managed collectively on a functional basis due to their interdependencies. As such, the risk described and communicated via the Executive Risk Profile may also be the aggregate of multiple operational risks.

### Division/CBU Risks

Risks that require Divisional/CBU oversight (e.g. by the senior leadership team) or moderation by multiple Branches/teams in the Division and relate to the delivery of the Division/CBU Operational Plan. These risks should be regularly monitored and reviewed by the Divisional/Agency leadership team.

Where a risk requires cross-divisional moderation or effects multiple Divisions/CBUs, the risk owner may remain but the risk is defined as a Corporate risk.

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.

### Issue

A present problem requiring immediate resolution and/or action. Consequences have already occurred.

### Likelihood

Chance of something happening.  
(Whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically).

(AS/NZS ISO 31000:2009)

### Program/Project risks

Risks to a defined program or project. These risks are not generally provided for DMT oversight as part of the Department of Health Risk Profile. These risks are to be regularly reviewed and communicated with the Project Executive and Project Board/Program Office.

Program or projects with high levels of risk may pose a defined risk to the delivery of an outcome or objective in the Strategic Plan. This is a corporate risk and must be communicated as such (see corporate risk).
### QHRisk
An online risk management information system, accessible through the QH intranet, to assist managers to identify, analyse and manage risks within their areas of responsibility and accountability in a near real-time environment.

The use of QHRisk for program/project risks may be subject to some exceptions - see *Implementation Standard for Risk Management* for further information.

### Risk
Effect of uncertainty on objectives.

An effect is a deviation from the expected – positive and/or negative.

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/ CBU, branch/team, program/project).

### Risk Matrix
Tool used to determine the level of risk expressed in terms of the combination of consequence(s) and likelihood. Refer to *Procedure for Risk Assessment and Treatment*.

### Risk Appetite
Amount and type of risk that an organisation is willing to pursue or retain.

### Risk Co-ordinator
A position responsible for:
- supporting the implementation of the Risk Management Policy,
- supporting risk owners in the analysis, recording and communication of risks
- acting as QHRisk superuser for their division/CBU

### Risk Owner
Person or entity with the accountability and authority to manage a risk.

A position with the most responsibility for the risk.

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.

As a matter of principle, each risk has only one Risk Owner.

### Risk Rating (Current and Projected)
#### Current Risk Rating
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.

#### Projected Risk Rating
Expected level of risk on completion of risk treatments

(AS/NZS ISO 31000:2009)
The term is synonymous with the terms ‘Residual Risk’ and ‘Retained Risk’.

Risk Register | Record of risk information maintained in QHRisk or project management software.

Responsible Position | A position vested with the responsibility for treatments. In some circumstances the Risk Owner and Responsible Position can be the same position. In other circumstances, multiple treatments are endorsed and allocated to different Responsible Positions, all reporting to the one Risk Owner.

Strategic risks | Risks that may affect the agency’s ability to meet its strategic objectives and require oversight by senior executives.

System risks | Risks that require moderation by Department of Health in partnership with HHSs. These risks are usually strategic and relate to Blueprint for Better Healthcare in Queensland delivery and not a single entity strategic plan.

Treatment | Process that is modifying risk. A risk treatment is an approved task/activity/program/project or other initiative that when implemented/completed will reduce the likelihood and/or consequence. A risk treatment may also be to improve, maintain or monitor the effectiveness of current controls. Once implemented/completed the risk treatment becomes a risk control. (AS/NZS ISO 31000:2009)

10. Approval and Implementation

Policy Custodian:
Chief Risk Officer, Risk and Governance Unit, System Support Services Division

Responsible Executive Team Member:
Annette McMullan, Chief Legal Counsel, Department of Health

Approving Officer:
Michael Cleary, Chief Operating Officer, Department of Health

Approval date: 19 November 2014
Effective from: 01 December 2014

Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Prepared by</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>14/11/13</td>
<td>Nicola Seymour</td>
<td>Final for policy site</td>
</tr>
<tr>
<td>1.2</td>
<td>6/11/14</td>
<td>Linda Moule</td>
<td>Review post implementation evaluation</td>
</tr>
</tbody>
</table>