1. Statement
This guideline describes the processes for risk assessment and treatment planning to actively manage uncertainty on a cost/benefits basis. This includes reducing risk exposure and consequences that may impact on objectives if the risk were to occur.

2. Scope
This guideline is mandatory for all employees, contractors and consultants within the Department of Health divisions and business units.

3. Requirements
This guideline should be read with the Implementation Standard for Risk Management and the Health System Risk Management Framework.
Risks (the effect of uncertainty on objectives), can be identified in a variety of settings and activities that relate to all areas of the business. Examples include project, portfolio and program management, planning (including business planning), team meetings and functional activities which may be related to occupational health and safety, finance, information technology, security, procurement, fraud and corruption control and change management.
Risks identification can occur through risk workshops or by discussions within relevant business areas to understand and capture the uncertainty surrounding achievement of objectives. The risk is usually written as a structured statement that can be easily understood. Some methods for identification include brainstorming, flowcharting and audits.
This guideline focuses on risk assessment using tools such as the risk analysis matrix (Attachment 1) and risk treatment planning sheet. The risk treatment planning sheet can be used for sections 3.1-3.10 of this guideline.
When a Department of Health or system risk is identified, complete the following risk management processes:

3.1 Risk ownership
Establish a risk owner. The risk owner is the person most responsible for managing the risk and must be involved in risk assessment and treatment planning. A risk coordinator may facilitate risk assessment and treatment of risks in conjunction with risk owners and other business areas that may have some responsibility for one or more risk treatment. Risk treatments may be owned by other business areas but will be collectively monitored and updated in consultation with the risk owner.
Risk ownership may necessarily be transferred if the identified risk owner no longer the person most responsible for managing the risk. This may occur if there has been a change to the scope of the risk or if the responsibilities under the risk have been assigned to another person. When this occurs agreement needs to be sought from both the current and proposed risk owner prior to transfer.

3.2 Risk assessment
3.2.1 Current controls
Identify all controls that currently prevent or moderate the risk, its likelihood and/or consequences (e.g. a control may be a process or plan that is approved and has already been implemented). Consider the effectiveness of the current controls when assessing both consequence and likelihood.
3.2.2 Consequences
Department of Health risks shall be assessed against the Department of Health consequence table (Attachment 1: Risk analysis matrix – Part 1 consequence table).
System risks shall be assessed against the system risk consequence table (Refer to Attachment 1 of the Health System Risk Management Framework)
Consider the range and severity of consequences of the risk and determine the highest consequence rating. This is the area of consequence most affected if a risk should occur.

3.2.3 Likelihood
Assess how likely/how often the risk is expected to occur (Attachment 1: Risk analysis matrix - Part 2 likelihood table). Use either the likelihood description or the probability as most applicable.
Note: The system risk likelihood table is identical to the Department of Health risk likelihood table.

3.2.4 Current risk rating
Refer to the risk matrix (Attachment 1: Risk analysis matrix – Part 3 risk matrix).
Locate where the highest consequence rating and the likelihood rating intersect on the risk matrix. This provides the current risk rating. The rating consists of a word and numeric value. The numeric value assists with prioritising the treatment of risks rated in the same word category.
Note: The health system risk matrix is identical to the Department of Health risk matrix.

3.2.5 Risk Response
Refer to the response to risk table (Attachment 1: Risk analysis matrix - Part 4 response to risk).
Use the current level of risk to determine the management, communication, reporting and review requirements in response to the risk. Programs and projects may have additional governance requirements for risk response and monitoring.
Note: The response to health system risk table is identical to the Department of Health response to risk table.

3.3 Risk Treatment
Refer to Risk treatment planning sheet.
Undertake risk treatment planning. Consider all viable treatment options and select risk treatments based on effectiveness and cost/benefit. If needed seek financial and procurement approval prior to recording as an approved risk treatment.
Risk treatments must have an owner assigned for treatment implementation. Record target dates for treatments which are realistic and achievable within business priorities.
Remember to include key stakeholders when identifying risk treatment options. Improving existing controls may reduce the risk more efficiently than establishing a new control. Also look for treatment options that will effectively reduce multiple risks. Work with multiple risk owners for cost efficiency and effectiveness.
The risk treatment planning sheet provides advice on information needed to document risks and evaluate treatment options and can be used to communicate risks to responsible executives to ensure awareness or endorse proposed treatments.

3.4 Projected risk rating
Refer to the risk analysis matrix and rerate the risk to get the projected risk rating. The projected risk rating is determined by the consequence and likelihood ratings that are expected following implementation of the risk treatments. Remember to consider the effectiveness of both current controls and treatments.

3.5 QHRisk and recording the risk
Risk owners and risk coordinators shall ensure that all risk information is recorded in QHRisk with the exception of project risks where they are recorded in project management software. When identifying potential project risks please refer to the guide for assessing project risk.
3.6 Monitor and review

Timely and appropriate communication and reporting of risks is essential to an effective risk management system and the responsibility of all Department staff.

The Department of Health Executive risk decision map and communication guide and Health system risk decision map and communication guide will assist decision making. The decision maps also show pathways for risk escalation or delegation.

A risk may necessarily be escalated or delegated where the risk requires further or reduced level of oversight. Escalation may occur if the risk has significant consequences and/or where the risk rating sits outside of the department’s identified risk appetite. Refer to the Department of Health Risk appetite statement.

Delegation may occur where a risk has been managed as low as reasonably practicable and there is no further benefit perceived at the identified reporting level i.e. Oversight at the executive committee is no longer required – risk is delegated to operational unit for management.

4. Supporting documents

- Risk Management Policy (QH-POL-070)
- Implementation Standard for Risk Management (QH-IMP-070-1)
- Department of Health Risk appetite statement
- Risk analysis matrix (attached)
- Department of Health Executive risk decision map and communication guide
- Health System Risk Management Framework (Including the System risk assessment tools and response guide and Health system risk decision map and communication guide)
- Risk treatment planning sheet
- A Guide for assessing project risk
- A/SNZS 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. |
**Consequence**
Outcome of an event affecting objectives. (Sourced from AS/NZS ISO 31000:2009)

The consequence impacts are assessed using the consequence table in the Risk Analysis Matrix. Refer to Risk Assessment and Treatment Guideline.

**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.

**Likelihood**
Chance of something happening. (Sourced from AS/NZS ISO 31000:2009)

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

The likelihood (probabilities) is assessed using the likelihood table in the Risk Analysis Matrix. Refer to Risk Assessment and Treatment Guideline.
**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 of management. This may result in the risk transferring to the corporate risk profile for moderation.

**QHRisk**

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.

All risks must be recorded in the QHRisk with the exception of project risks where they are recorded in project management software.

**Risk**

Effect of uncertainty on objectives. (Sourced from AS/NZS ISO 31000:2009)

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/business unit, 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 Risk Assessment and Treatment Guideline.

**Risk Appetite**

Amount and type of risk that management within an organisation are willing to pursue or retain. (Sourced from ISO 73:2009)

**Risk Coordinator**

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 or business unit

**Risk Owner**

A person 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 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. The term is synonymous with the terms ‘Residual Risk’ and ‘Retained Risk’.
Risk Register

A record of risk information is to be recorded and maintained in an active risk register.

All risks must be recorded in the QHRisk with the exception of project risks where they are recorded in project management software.

Strategic risks

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.

System risks

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.

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>14 November 2014</td>
<td>New policy developed.</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>22 July 2014</td>
<td>Update risk matrix link for new QHEPS page</td>
</tr>
<tr>
<td>Version 1.2</td>
<td>6 November 2014</td>
<td>Post Implementation Review</td>
</tr>
<tr>
<td>Version 1.4</td>
<td>24 February 2017</td>
<td>Review post risk maturity evaluation</td>
</tr>
</tbody>
</table>