# Enterprise-wide Risk Management

**Summary** This Policy Directive describes the requirements for NSW Health organisations to establish, maintain and monitor risk management practices in accord with the Australian/New Zealand Standard ISO 31000:2018, consistent with whole of Government policies.

**Document type** Policy Directive

**Document number** PD2022_023

**Publication date** 01 July 2022

**Author branch** Corporate Governance & Risk Management Unit

**Branch contact** (02) 9391 9654

**Replaces** PD2015_043

**Review date** 01 July 2027

**Policy manual** Not applicable

**File number** H22/33301

**Status** Active

**Functional group** Corporate Administration - Governance

**Applies to** Ministry of Health, Public Health Units, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, Affiliated Health Organisations, NSW Health Pathology, Public Health System Support Division, Cancer Institute, NSW Ambulance Service, Dental Schools and Clinics, Public Hospitals

**Distributed to** Ministry of Health, Public Health System, NSW Ambulance Service

**Audience** Boards;All Chief Executives;Directors;Health Service Managers;Audit and Risk Committees

Secretary, NSW Health

NSW Health

POLICY DIRECTIVE

# Enterprise-wide Risk Management

## POLICY STATEMENT

All NSW Health organisations must establish and maintain a risk management framework that is appropriate, fit for purpose, and tailored to the needs of the organisation.

## SUMMARY OF POLICY REQUIREMENTS

All staff (permanent, temporary or contract) are accountable for managing risk in their day-to-day roles, including carrying out their roles in accordance with policies and procedures, identifying risks and inefficient or ineffective controls and reporting these to the appropriate level of management.

Managers and decision makers at all levels in NSW Health organisations are accountable for managing risk within their sphere of authority and in relation to the decisions they take.

In addition to the responsibilities above, senior executives are responsible for managing specific strategic risks as the risk owner and are responsible for ensuring necessary controls and treatment plans are in place to effectively manage that risk, including providing adequate resources.

The Chief Executive officer has ultimate responsibility and accountability for risk management in their organisation.

All staff are to contribute to a positive risk culture that encourages desirable risk management behaviours such as open and regular discussion of risk, with concerns about business practices raised and acted upon promptly.

NSW Health organisations are to nominate or appoint an appropriately skilled Chief Risk Officer who is responsible for the oversight and promotion of risk management; for designing the risk management framework; and for the oversight of activities associated with coordinating, maintaining and embedding the framework.

All NSW Health organisations must have an enterprise-wide risk management procedure in place that outlines how the organisation will identify, assess, manage and monitor risks. It must include processes for escalating risks and for providing risk reports to the senior executive team, the Chief Executive, the Audit and Risk Committee and Board.

The organisation's risk appetite and risk tolerance are to be documented, communicated and regularly reviewed.

Risk owners must reduce a risk to an acceptable level through implementing additional controls or improving existing controls. Where the current level of a risk is outside the organisation's risk tolerance, it is to be escalated to more senior levels of management.

Where a NSW Health organisation is unable to manage a risk to be within its tolerance levels, the risk is to be escalated to the Ministry of Health for further advice or support. The

ownership and management of a risk that has been escalated remains the responsibility of the health organisation.

All NSW Health organisations are to maintain a risk register which provides an accurate and complete record of risk assessment and management activities. The risk register is to be subject to regular review and update as risks are addressed and new risks identified.

The NSW Health risk matrix must be used by all NSW Health organisations when assessing risk.

Where a new or emerging risk that has the potential to be system-wide is identified, the organisation is to complete a Potential System-wide Risk Notification Form, have it approved by the Chief Executive, and forward it to the Ministry of Health's Corporate Governance and Risk Management Unit.

Risk management and reporting is to be a standing agenda item for senior executive team meetings, for Audit and Risk Committee meetings, and for Board meetings.

Reporting is to be appropriate for the size and complexity of the organisation and must periodically include the number of risks that are operating outside the organisation's risk tolerance and the number of risks that are overdue for review.

The organisation's risk management framework must be the subject of an internal audit at least once every five years.

An Internal Audit and Risk Management Attestation Statement is to be submitted to the Ministry of Health by 17 July each year, stating whether the NSW Health organisation has complied with this Policy Directive and the NSW Health Policy Directive *Internal Audit* (PD2022_022).

## REVISION HISTORY

| Version | Approved By | Amendment Notes |
|---|---|---|
| PD2022_023<br>July - 2022 | Secretary, NSW Health | Updated to support development and implementation of organisation-appropriate risk management frameworks. |
| PD2015_043<br>(October 2015) | Deputy Secretary, Governance, Workforce and Corporate | Updated policy directive |
| PD2009_003<br>(June 2009) | Director General | New policy directive |

# CONTENTS

# 1 BACKGROUND

Risk is the effect of uncertainty on objectives. Risk management involves identifying the types of risk exposure within an organisation, measuring those potential risks and proposing means to mitigate or exploit them.

Risk management is essential to good management practice and effective corporate governance and ensures decisions are made with sufficient information about risks and opportunities. While it is impossible to remove all risk, the overall goal is to identify, understand, manage and reduce risk to an acceptable level, to ensure effective operation, service provision and resource utilisation across an organisation.

Risk is different from an issue, which is an event that has already occurred, or is currently occurring, and is impacting, or has had an impact, on objectives.

Effective policies and systems combined with a sound risk culture help to promote desirable risk management behaviour. These behaviours are reflected in the open and regular discussion of risk which incorporates genuine risk concerns about business practices and the timeliness of responses. Collectively, these behaviours help organisations stay within an organisation's risk appetite and achieve performance aspirations in a sustainable way.[1]

NSW Health is committed to developing a positive risk management culture, where risk is seen as integral to the achievement of our aims at all levels of the organisation and where all staff are alert to risks, capable of an appropriate level of risk assessment and confident to report risk or opportunities perceived to be important in relation to each Health organisation's priorities.

## 1.1 About this document

This Policy describes the minimum requirements for NSW Heath organisations in implementing and maintaining an enterprise-wide risk management framework. It is complementary to the NSW Health Internal Audit Policy Directive (PD2022_022) and consistent with AS/NZS ISO 31000:2018 *Risk Management – Guidelines*.

While NSW Treasury's *Internal Audit and Risk Management Policy for the General Government Sector* (TPP20-08) is only applicable to the Ministry of Health, the Mental Health Commission, Health Professional Councils and the Health Care Complaints Commission, this Policy Directive has been developed to align with the Core Principles and Core Requirements outlined in TPP20-08.

[1] [1] Arzadon, E., Du Preez, R. and Sheedy, E., 2021. *Auditing Risk Culture: A practical guide*. [ebook] Sydney: Institute of Internal Auditors - Australia. Available at https://www.iia.org.au/technical-resources/publications/auditing-risk-culture---a-practical-guide.

## 1.2 Key definitions

| | |
|---|---|
| **Risk** | The effect of uncertainty on objectives, noting that effect is a deviation from the expected and may be positive and/or negative. |
| **Board** | In this document, references to "the Board" includes the Board of any local health district, specialty health network, or Board-governed statutory health corporation, the Cancer Institute of NSW Board, Ambulance Services Advisory Board, Health Infrastructure Board, HealthShare NSW Board, and NSW Health Pathology Board. |
| **Current risk** | The current amount of risk, after all existing controls are accounted for. |
| **NSW Health organisation** | A local health district, specialty health network, statutory health corporation, units of the Health Administration Corporation (including the NSW Ambulance Service, HealthShare NSW, eHealth NSW, Health Infrastructure and NSW Health Pathology), and health bodies established under their own statute, including the Cancer Institute of NSW. |
| **Risk appetite** | The amount and type of risk that an organisation is prepared to pursue, retain or take to achieve goals and objectives. |
| **Risk owner** | The manager responsible for ensuring that an identified risk is monitored and reviewed within set timeframes, and that appropriate controls are implemented and maintained. |
| **Risk tolerance** | The assessed and accepted threshold levels of risk exposure that, when exceeded, will trigger a risk response. |
| **Senior executive** | A senior member of the organisation who has management accountability for a core component of the health organisation. Senior executives generally report directly to the chief executive or to another senior executive within the health organisation. |

## 1.3 Legal and legislative framework

- *Government Sector Finance Act 2018*
- *Health Services Act 1997*
- *Accounts and Audit Determination for Public Health Entities in NSW*

# 2 RISK MANAGEMENT RESPONSIBILITIES

## 2.1 Responsibilities of staff

All staff (permanent, temporary or contract) are accountable for managing risk in their day-to-day roles, including carrying out their roles in accordance with policies and procedures, identifying risks and inefficient or ineffective controls and reporting these to the appropriate level of management.

Risks that are beyond a staff member's capacity or delegation of authority must be escalated to a higher level of management for review, with subsequent mitigations communicated back to the staff member who identified the risk.

## 2.2 Managers and decision makers

Managers and decision makers at all levels in each NSW Health organisation are accountable for managing risk within their sphere of authority and in relation to the decisions they take. Risks that are beyond a manager's or a decision maker's capacity or delegation of authority must be escalated to a higher level of management for review.

Responsibilities also include supporting a positive risk culture, managing risks within the levels the organisation is willing to accept or tolerate, and supporting the implementation of the organisation's risk management framework as appropriate for their role.

## 2.3 Senior executives

In addition to the responsibilities above, senior executives are responsible for managing specific strategic risks as the risk owner and are responsible for ensuring necessary controls and treatment plans are in place to effectively manage that risk, including providing adequate resources.

Senior executives must attend Audit and Risk Committee meetings, when requested, to discuss the current management of specific risks.

## 2.4 The Chief Risk Officer

All NSW Health organisations are to nominate or appoint an appropriately skilled Chief Risk Officer. This role may be a dedicated role or incorporated as a function of an existing role.

The Chief Risk Officer supports the Chief Executive and is responsible for:

- the oversight and promotion of risk management within the organisation
- designing the organisation's enterprise-wide risk management framework
- the oversight of activities associated with coordinating, maintaining and embedding the framework in the organisation.

The Chief Risk Officer role (or function) is to be considered a senior role within the organisation and be either a member of the organisation's senior executive, or directly report to a member of the senior executive team.

## 2.5 Internal Audit

Internal Audit is responsible for providing assurance to the Chief Executive and to the organisation's Audit and Risk Committee on the effectiveness of the risk management framework, including the design and operational effectiveness of internal controls.

The organisation's enterprise-wide risk management framework must be the subject of an internal audit at least once every five years.

## 2.6 The Chief Executive

The Chief Executive has ultimate responsibility and accountability for risk management in their organisation. Risk management-related responsibilities also include promoting a positive risk culture, determining and articulating the level of risk the organisation is willing to accept or tolerate, approving the organisation's enterprise-wide risk management framework and plans, and ensuring these are communicated, implemented and kept current.

## 2.7 Audit and Risk Committee

Audit and Risk Committees across NSW Health have no executive powers, delegated financial responsibility or management functions, but provide independent advice to the Chief Executive and Board by monitoring, reviewing and providing advice about the organisation's risk management framework.

## 2.8 The Board

The Board is responsible for approving the organisation's enterprise-wide risk management framework, including the levels of risk appetite and tolerance, and for seeking appropriate assurance on the effectiveness of the framework.

# 3 ENTERPRISE-WIDE RISK MANAGEMENT FRAMEWORK

All NSW Health organisations must establish, implement and maintain an enterprise-wide risk management framework that is tailored to achieving their strategic and operational plans, support the delivery of performance objectives, meet business needs and be integrated with its systems and processes. It must also recognise the organisation's contribution to broader state-wide health strategies and objectives, such as the *NSW State Health Plan* and *NSW Health Strategic Priorities*.

The Framework is to be consistent with *AS ISO 31000:2018 Risk Management Guidelines* and:

- be structured and comprehensive
- be customised – the framework and process are customised and proportionate to the NSW Health organisation's external and internal context related to its objectives
- be inclusive – appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered, resulting in improved awareness and informed risk management

- be dynamic – effective risk management anticipates, detects, acknowledges and responds to internal and external changes in a timely manner
- be based on the best available information - inputs to risk management are based on historical and current information, future expectations and any associated limitations and uncertainties
- take human and cultural factors into account
- involve continual improvement – through learning and experience.

NSW Health organisations must also ensure that the identification and assessment of the impacts of climate change is integrated into its enterprise-wide risk management framework, and that the projected impact on assets and services is actively managed and mitigated.

## 3.1 Risk culture

Risk culture is a crucial element within the framework. Together with effective policies and systems, sound risk culture encourages desirable risk management behaviours such as open and regular discussion of risk, with concerns about business practices raised and acted upon promptly.

All management and staff must support a positive risk culture, where, as a minimum:

- Staff are thoughtfully engaged, and risk management is seen as an enabler, rather than a barrier, for achieving business objectives.
- Leaders and managers have a good understanding of the business environment, the risks that are present, and how they may be changing.
- Managers and leaders in the business are good role models of risk management behaviour, e.g. reporting and resolving risk issues, complying with policies.
- People who speak up about risk issues/concerns are valued by managers, their concerns are taken seriously, and managers respond to their concerns appropriately.
- Leaders and managers regularly communicate about risk management, in both formal and informal ways.[2]

## 3.2 Risk appetite and risk tolerance

All NSW Health organisations are to ensure risk appetite and risk tolerances are documented, communicated and regularly reviewed. The risk appetite statement must be linked to the organisation's strategic goals, performance agreement and operational plans, and have consideration of the organisation's contribution to broader state-wide health strategies and objectives, such as the *NSW State Health Plan* and *NSW Health Strategic Priorities*.

In developing or updating risk appetite, NSW Health organisations are to consider the level of risk appetite, as outlined in Table 1.

[2] Arzadon, E., Du Preez, R. and Sheedy, E., 2021. *Auditing Risk Culture: A practical guide*. [ebook] Sydney: Institute of Internal Auditors - Australia. Available at https://www.iia.org.au/technical-resources/publications/auditing-risk-culture---a-practical-guide.

*Table 1: Levels of risk appetite*

| Level | This means there is… |
|---|---|
| Zero | **No willingness to take on any risk**<br>The organisation **will not** operate in this area. |
| Low | **A willingness to take on a limited level of risk necessary to achieve goals and objectives**<br>The organisation may operate in this area, or in this way, where the value is assessed as worthwhile, after risks have been effectively mitigated or uncertainty minimised. |
| Moderate | **A willingness to take on a moderate level of risk for benefits linked to goals and objectives**<br>The organisation may operate in this area, or in this way, after risks have been effectively mitigated to pursue benefits that enhance strategic outcomes or operational objectives. |
| High | **A willingness to take on higher levels of risk to maximise gains**<br>The organisation may operate in this area, or in this way, after all options are considered and the most appropriate option selected to maximise strategic or operational gains. |

In developing the risk appetite statement, organisations may articulate the level of appetite for individual risk categories, so long as the approach establishes boundaries for sound decision making and risk taking.

The organisation's risk appetite is to be approved by the Chief Executive and by the Board, on advice from the Audit and Risk Committee.

# 4 RISK MANAGEMENT METHODOLOGY

All NSW Health organisations must develop and maintain an enterprise-wide risk management procedure that outlines how the organisation will identify, assess, manage and monitor risks. It must include a process for escalating risks and for reporting risks to the Chief Executive and Audit and Risk Committee, and to the Board.

Risk is to be considered and assessed at different levels, across many functions and activities, as appropriate for the size and complexity of the organisation.

All risk assessments, including their identification, controls, likelihood, consequence, and risk rating are to be documented consistently across the organisation. Controls embedded within the organisation's current business processes are to be identified as part of the risk evaluation process.

In developing risk management procedures, NSW Health organisations are to ensure an identified risk can be assessed and rated in the context of the environment in which the risk was initially identified (i.e., project, ward, unit, service, or facility level), and managed accordingly.

## 4.1 Risk identification

NSW Health organisations are to ensure risks are identified by examining sources of risk, areas of impact, causes and potential consequences of events and scanning the environment.

Organisations must ensure there is formal consideration and documentation of risk and opportunities during:

- Strategic, business, service and workforce planning
- Budget planning and monitoring
- Planning, development and implementation of new service delivery methods, programs, clinics or projects
- Planning, development, implementation and maintenance of new and existing information technology hardware and software systems
- Development and implementation of new or revised policies, procedures and guidelines
- Changes to service delivery, projects or agreed levels of activity
- Planning and implementing capital projects and programs
- Scoping of, and reporting of findings from, internal audits
- Procurement and acquisitions processes.

Risks may also be identified by the risks associated with not pursuing an opportunity.

### 4.1.1 Risk categories

As part of the risk identification process, all risks must be categorised. Categorising risks supports identification of risks across the key aspects of a health organisation's business. NSW Health organisations may set their own risk categories, use risk categories documented in earlier policy directives, adopt the recommended risk categories outlined in Appendix 7.1, or use a mix of all these options.

The risk management categories must be described in the organisation's enterprise-wide risk management procedures and included as a field in the risk register.

### 4.1.2 Risk register

All NSW Health organisations are to maintain a risk register which provides an accurate and complete record of risk assessment and management activities. The risk register is to be a 'living document', subject to regular review and update as risks are addressed and new risks identified, and as strategies and controls for existing risks are updated. Recommended fields for inclusion in an organisation's risk register are included in Appendix 7.2.

### 4.1.3 Identification of potential system-wide risks

Where an organisation identifies a new or emerging risk that has the potential to be system-wide, the organisation is to complete a 'Potential System-wide Risk Notification Form', have it approved by the Chief Executive, and forward it to the Ministry of Health's Corporate Governance and Risk Management Unit via email MOH-CGRM@health.nsw.gov.au.

Forms are available from the NSW Health intranet page.

In notifying the Ministry, the notification must include a:

- Clear and concise description of the risk and its potential system-wide impacts
- Clear description of why this has been identified as an emerging or potentially significant risk for the NSW Health system
- Description of the organisation's main controls and their limitations
- Summary of any outcomes from discussions with leads within the organisation, as well as any advice from the organisation's Audit and Risk Committee.
- Summary of any outcomes from discussions with stakeholders internal to the NSW Health system, including any feedback from the relevant units within the Ministry of Health.

System-wide risks that are generally known, or that have controls that are largely effective, do not need to be reported to the Ministry.

### 4.1.4 Notification of risks to other NSW Health organisations

Where there are significant risks arising from strategic and operational activities of the organisation that affect, or are likely to affect, other NSW Health organisations, the Chief Executive is to formally communicate the risk, and any risk treatment that has been undertaken to manage the risk, to those affected organisations.

In communicating the risk and risk treatments, the Chief Executive must have regard for the benefits of sharing information to enable affected health organisations to understand the risk and mitigations, against increasing the level of risk by sharing certain information.

## 4.2 Risk assessment

NSW Health organisations must develop and implement a process for assessing identified risks. The process must reference the use of Table 2 and 3, below, and include:

- identifying the causes and sources of the risk
- identifying and assessing the effectiveness of existing controls to mitigate the risk
- determining the potential consequences and likelihood of the consequences being experienced.

Through this process, the level of risk is to be determined and compared with the organisation's risk tolerance to determine if further controls are needed.

*Table 2: Consequences from a risk occurring*

| Consequence | Context |
|---|---|
| **Catastrophic** | Unexpected, or potentially preventable, death of multiple persons from the same event or cause; or<br>Substantial reprioritisation of resources to salvage key strategic, operational or performance objectives |
| **Major** | Unexpected, or potentially preventable, death of a person; or<br>Reprioritisation of resources to ensure delivery of key strategic, operational or performance objectives |
| **Moderate** | Major harm to a person (or persons); or<br>Modest reprioritisation of resources to support strategic, operational and/or performance objectives |
| **Minor** | Minor harm to a person (or persons); or<br>Reprioritisation of resources to support delivery of key objectives at a unit- or service-level |
| **Minimal** | Minor harm, not requiring medical treatment, to a person (or persons); or<br>Short-term diversion of resources to achieve business unit or service objectives |

*Table 3: Likelihood of a consequence being experienced*

| Likelihood | Time scale | OR | Probability |
|---|---|---|---|
| **Almost certain** | Several times a month | | Greater than 97% |
| **Likely** | Monthly, or several times a year | | At least 70% but less than 97% |
| **Possible** | Yearly, or several times over a three-year period | | At least 30% but less than 70% |
| **Unlikely** | Once every three years | | At least 3% but less than 30% |
| **Rare** | Less frequent than once every three years | | Less than 3% |

### 4.2.1 NSW Health risk matrix

The NSW Health risk matrix, below, must be used by all NSW Health organisations when assessing both strategic and operational risks.

| | | Consequence Rating | | | | |
|---|---|---|---|---|---|---|
| | | **Catastrophic** | **Major** | **Moderate** | **Minor** | **Minimal** |
| **Likelihood Rating** | **Almost certain** | A | D | J | P | S |
| | **Likely** | B | E | K | Q | T |
| | **Possible** | C | H | M | R | W |
| | **Unlikely** | F | I | N | U | X |
| | **Rare** | G | L | O | V | Y |

**Risk matrix key:** Extreme (A – E) | High (F – K) | Medium (L – T) | Low (U – Y)

## 4.3 Risk treatment and escalation

Risk owners must reduce a risk to an acceptable level through implementing additional controls or improving existing controls. Options for treating risk include:

- avoiding the risk by stopping the activity or choosing an alternative activity
- reducing the risk by removing the source of the risk or implementing further mitigation strategies to change the likelihood and consequences of the risk
- sharing the risk with another party
- accepting the risk to pursue an opportunity but may include implementing further mitigation strategies or strengthening existing controls.

As part of their risk management framework, all NSW Health organisations must have documented processes in place that enable staff to escalate risk to more senior levels of management when the current level of risk is outside the organisation's risk tolerance.

### 4.3.1 Escalation of organisation-level risks to the Ministry of Health

Where a NSW Health organisation is unable to manage a risk to be within its tolerance levels and is not prepared to accept the level of risk, the organisation is to escalate the risk to the Ministry of Health for additional guidance and support. The organisation is to complete an 'Escalation of Organisation-level Risk' form, have it approved by the Chief Executive, and forward it to the Ministry of Health's Corporate Governance and Risk Management Unit via email MOH-CGRM@health.nsw.gov.au.

In escalating to the Ministry, the notification must include:

- A clear and concise description of the risk and its potential impacts on the organisation
- The reason/s for the escalation
- Details of the support needed, or an outline of the requested actions, and a rationale for the support or actions.

The ownership and management of a risk that has been escalated remains the responsibility of the health organisation. Forms are available from the NSW Health intranet.

## 4.4 Monitor and review

### 4.4.1 Monitoring and reviewing individual risks

Organisations must include the period for review of individual risks as part of their risk management framework and ensure risk owners review individual risks within the required time. Risks are to be reviewed at least every:

| Risk Rating | Extreme (A – E) | High (F – K) | Medium (L – T) | Low (U – Y) |
|---|---|---|---|---|
| Review period | 28 days | 91 days | 182 days | 364 days |

### 4.4.2 Executive monitoring and reporting

All NSW Health organisations must ensure that risk management and reporting is a standing agenda item for senior executive team meetings, for audit and risk committee meetings, and for Board meetings.

Reporting to the senior executive team, and to the Audit and Risk Committee, is to be appropriate for the size and complexity of the organisation. As an indicator of risk culture, reporting is to periodically include the number of risks that are operating outside the organisation's risk appetite and the number of risks that are overdue for review.

# 5 ATTESTATION STATEMENT

## 5.1 Annual attestation of compliance

The Internal Audit and Risk Management Attestation Statement is an annual statement to the Secretary, NSW Health about the NSW Health organisation's conformance or otherwise to this Policy Directive, and to the NSW Health Policy Directive *Internal Audit* (PD2022_022). Advice, opinion or feedback may be sought from the Audit and Risk Committee in relation to the organisation's compliance.

The Chief Executive is to submit the Attestation Statement, along with the Internal Audit and Risk Management compliance self-assessment for the financial year (available from the NSW Health intranet), to the Ministry of Health (via email MOH-CGRM@health.nsw.gov.au) by 17 July each year, stating whether the NSW Health organisation complied with these Policy Directives during the financial year immediately prior.

A copy of the final completed Internal Audit and Risk Management Attestation Statement must be communicated to the Audit and Risk Committee and to the Board.

## 5.2 Requesting an exception to policy requirements

Where a NSW Health organisation is not able to comply with any of the requirements of this Policy Directive, or with the NSW Health Policy Directive *Internal Audit* (PD2022_022), the Chief Executive may apply in writing to the Secretary, NSW Health for an exception from the relevant policy requirement(s) prior to 31 March of the financial year for which the exemption is sought. The request must include an outline of why the organisation has not been able to comply with the policy requirement/s.

A determination with respect to an exception will be for the reporting period only and, even if circumstances for the initial exception are ongoing, further exceptions must be renewed annually. Where an exception is granted, the exception must be indicated on the Attestation Statement.

The organisation's Audit and Risk Committee and Board must be notified of the request for exception.

## 6 GLOSSARY OF TERMS

| | |
|---|---|
| **Current (or residual) risk** | The amount of risk, now, after all existing controls are accounted for. |
| **Effect** | The deviation from the expected outcome or norm. |
| **Inherent risk** | The amount of risk in the absence of controls. |
| **Issue** | An event that has already occurred, or is currently incurring, and is impacting, or has had an impact, on objectives. |
| **Risk owner** | The manager responsible for ensuring actions to address a particular risk are designed, implemented and regularly reviewed. |
| **Target risk** | The desired optimal level of risk. |

# 7 APPENDICES

## 7.1 Recommended risk categories and areas of risk to consider within the categories

### 7.1.1 Clinical care and patient safety

Access appropriate to needs and prioritised according to clinical need

Care evaluation, clinical handover, clinical pathways and variance analysis

Clinical quality improvement and clinical practice improvement

Complaints and concerns about clinicians

Decision making at end of life and mortality management

Discharge and transfer of care

Hospital-acquired complications

Informed consent

Patient safety, including incident management and near miss or incident trends

Protection of people unable to care for themselves while accessing health services

### 7.1.2 Financial management

Administration, such as accommodation, payroll, transport and travel

Commercial income

Fraud prevention and control

Operational budgets and financial performance

Public liability

Procurement of goods and services, maintenance and contracts management

Treasury Managed Fund and other insurance arrangements

### 7.1.3 Governance and performance

Accreditation

Climate adaptation

Credentialing and delineation of clinical privileges

External and internal auditing

Governance structures and delegations

Legislative compliance

Resource accountability

Performance Agreement requirements

Project and program management

Strategic and operational planning

Sustainability

### 7.1.4 Health of the population

Alignment of strategic clinical direction, planning, monitoring and performance of population health services

Community health

Disease prevention and control

Human behaviour and demographics

Health protection and surveillance

### 7.1.5 Infrastructure

Air quality, heating, noise, lighting, and radiation

Access and controls

Asset management
(including buildings, equipment, land, plant, vehicles, supplies and utilities)

Climate resilience

Hazardous substances and dangerous goods management

ICT Hardware infrastructure

Information and data management systems

Internal and external communication platforms

Minor & capital works

Security management and security monitoring

Software

### 7.1.6 Legal

Commercial and legal management

Contract management

Intellectual property

Litigation

Regulatory compliance

### 7.1.7 People and culture

Continuing education, learning and professional development

Human resources performance management

Organisational and workplace culture

Professional development and mentoring

Recruitment selection, credentialing, retention and appointment

Succession planning

Workplace relations, including grievances

Visiting medical officers, contracts and volunteers

### 7.1.8 Reputation

Access to, and quality of, services

Climate impact and environmental sustainability

Compliments and complaints management

Consumer engagement and empowerment, and stakeholders' expectations

Patient experience

Privacy and confidentiality

Release of information

The right care and services, including the protection of children and vulnerable populations, provided in the right setting within appropriate timeframes

### 7.1.9 Service delivery

Business continuity management and disaster recovery planning

Catering and food hygiene

Chemicals, radiation and hazardous material management

Cleaning services

Disaster response

Electronic information security management and cyber security

Environmental sustainability

Infection control

Procurement

Records management

Waste management

### 7.1.10 Work health & safety

Workplace health and safety

Workers' compensation and injury management

Contractor non-compliance

## 7.2 Recommended risk register data fields

| | |
|---|---|
| **Organisation name** | Name of the NSW Health organisation |
| **Risk ID** | Unique identifier which identifies the risk |
| **Date risk created** | Date risk was created |
| **Risk category** | Relevant to the risk, using the risk categories listed in the organisation's enterprise-wide risk management procedures, each risk is to be categorised. |
| **Risk description** | A description of the risk, possible causes and impacts. |
| **Risk owner** | Risk owner by position, not name (only one risk owner for each risk) |
| **Inherent risk rating** | The risk rating, as per risk matrix, at the time of risk identification. |
| **Current controls** | Description of the controls that are in place |
| **Control type** | Type of control is either proactive or reactive |
| **Control effectiveness** | Level of effectiveness of current controls is either substantial, partial, or ineffective |
| **Current risk rating** | Risk rating after controls |

**Additional controls / action items to mitigate risks:**

| | |
|---|---|
| **Additional control description** | Identify and capture any further actions that need to be carried out to further reduce risk from "residual risk rating" in order to manage the risk to an acceptable level. |
| **Due date** | Stipulate when the actions are due to be completed. |
| **Responsible position** | Position (not name) responsible for implementation |
| **Target risk rating** | Proposed risk rating after the implementation of mitigating actions |
| **Trend** | Trend for the risk (e.g., decreasing; increasing; no change) |
| **Risk status** | Active; Inactive. |