11 Audit & Risk Management

11.1 Audit and Financial Governance Framework

The NSW Health System operates within a range of Whole of Government policies issued through NSW Treasury and adopted by NSW Health policy. These require public health organisations to maintain effective, independent audit framework and corporate governance practice, as described in this compendium, that is consistent with the "best practice" attributes for the NSW public sector.

Specifically, the audit framework of public health organisations is established within a suite of legislative, policies, procedures, reporting and review requirements. There are several governance mechanisms that oversee the responsible use of government resources and the efficiency and effectiveness of health services delivery in NSW. The legislative basis includes:

Key legislation oversighting financial management, reporting and audit responsibilities

- *Charitable Fundraising Act 1991*;
- *Charitable Trusts Act 1993*;
- *Dormant Funds Act 1942*;
- *Health Administration Act 1982*;
- *Health Services Act 1997*;
- *Independent Commission Against Corruption Act 1988*;
- *Local Health District and Speciality Health Network By-Laws*;
- *Statutory Health Corporation By-Laws*;
- *Public Finance & Audit Act 1983*;
- *Government Sector Finance Legislation (Repeal and Amendment) Act 2018*;
- *Public Health Act 2010*;
- *Ombudsman Act 1974*;
- *Trustee Act 1925*.

In addition, there are several State and Commonwealth Government administrations that are involved in overseeing the audit and governance framework of public health organisations within NSW. Some of the key NSW administrations are NSW Treasury, Department of Premier and Cabinet and the Audit Office of NSW.

11.2 Audit Requirements

11.2.1 Internal audit unit

The chief executive must establish and maintain an effective internal audit function. This function is directly responsible to the chief executive for:

- regular appraisal of the adequacy and effectiveness of the organisation's:
  - systems of internal control; and confirmation of compliance with those systems;
  - risk management program; and
  - governance processes.
- review of operations or programs, to ascertain if results are consistent with established or appropriate goals and objectives and if the operations or programs are being carried out as planned;
- reporting directly at regular intervals to the chief executive and board on the result of any audit appraisal, inspection, investigation, examination or review made by the internal audit organisation
- monitoring and confirming implementation of recommendations made following any audit appraisals, inspections, investigations, examinations or reviews.

Internal audit units and internal auditors are to comply with the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

The Manager, Internal Audit or the internal auditor as the case may be is to have direct access to the Chairperson of the Audit and Risk Management Committee and the Chairperson of the board.

11.2.2 Employment of an internal auditor

A public health organisation must notify its intention to advertise for a Chief Audit Executive position, appoint a new Chief Audit Executive, or remove an appointed Chief Audit Executive with the Deputy Secretary, Governance, Workforce & Corporate, NSW Ministry of Health.

Once employed, the Chief Audit Executive term of employment/engagement should not be amended without formally notifying the Deputy Secretary, Governance, Workforce and Corporate, NSW Ministry of Health[6]

11.2.3 External audit

The affairs and operations of a public health organisation as disclosed in its accounts and associated financial and other records shall be audited in respect of each financial year.

The Audit Office of NSW undertakes the external audit function for NSW public health organisations.

6 Section 1.3 Internal Audit Policy Directive PD2016_051

11.3 Audit and Risk Management Committee

11.3.1 Role of the Audit and Risk Management Committee

Health Agencies must complete an Internal Audit and Risk Management Attestation Statement for the financial year by 17 July each year

NSW Health seeks to observe high ethical standards and conduct in commercial engagements. Each public health organisation must establish an Audit and Risk Management Committee.

The Audit and Risk Management Committee plays a key role in assisting the board and the chief executive perform their duties under the *Health Services Act 1997* particularly in relation to the organisation's financial reporting, internal control, risk management and internal and external audit functions. The role of the Audit and Risk Management Committee is separate from that of executive management of the organisation. Its role is to provide advice and it has no decision-making powers or supervisory functions.

The Audit and Risk Management Committee has a duty to provide assurance to the public health organisation that financial information reported to it reasonably portrays the organisation's financial condition, results of operations, plans and long-term commitments and contingencies.

The Audit and Risk Management Committee is responsible for independently reviewing the financial statements and external reporting prior to approval by the public health organisation. If any technical or operational issues arise in relation to the finalisation of such reports, the Committee can act as a useful forum for resolving such issues. A sound understanding of the financial reporting requirements and significant policies and principles that underpin these reports is crucial for Audit and Risk Management Committee members.

The Audit and Risk Management Committee should thoroughly review the financial statements for compliance with all prescribed accounting and other requirements; assess the appropriateness of the public health organisation's accounting policies and performance measures; identify and investigate any unusual financial or operational trends or variations from forecasts; review the impact of any materially adverse findings; ensure that the financial statements provide a true and fair view of the activities of the organisation for the period under review and of its affairs at the balance date. Of particular relevance are the notes and disclosures that complement the statements.

In addition, NSW Health policy (Enterprise-wide Risk Management – PD2015_043) requires the Audit and Risk Management Committee to maintain oversight of risk management within the organisation, to review systems and the control frameworks. It is required to provide reasonable assurance to the chief executive and the board that an enterprise-wide risk management system which addresses both clinical and non-clinical risks has been effectively implemented.

11.3.2 Membership of the Committee

The Audit and Risk Management Committee consists of between 3 and 5 members. The Chair and members are selected from the NSW Government's Audit and Risk Committee Members Prequalification Scheme.

The role and responsibilities of the Audit and Risk Management Committee in a NSW Health organisation's Governance structure, including procedures for the appointment and remuneration of committee members is set out in NSW Health Policy Directive, *Internal Audit* (PD2016_051)

See the NSW Health Model Charter for an Audit & Risk Management Committee.

11.4 Enterprise-wide Risk Management Framework

Requirement to establish an enterprise-wide risk management framework and compliance with State laws.

Risk is the effect of uncertainty on objectives[7]. Risk management involves developing systems to identify and analyse risks with the aim of reducing any harmful consequences and benefiting from any opportunities. Managing risks –identifying, assessing and controlling them- is part of everyday activity throughout NSW Health.

Risk management is a critical component of good management practice and effective corporate governance and is essential to ensure that decisions are made with sufficient information about risks and opportunities.

As public health organisations are exposed to a wide variety of corporate and clinical risks on a daily basis, effective risk management is important and should be promoted as a way of meeting organisational responsibilities and objectives.

Effective enterprise risk management is a key component of strategic planning and monitoring of organisational systems that are fundamental to evidence based decision making, responsible management and good governance. Enterprise wide risks are best managed through a structured enterprise-wide risk management process involving continuous monitoring and risk control (policy, procedures and guidelines) in an integrated and systematic manner.

Health Agencies must report quarterly on the top 10 risks inclusive of all extreme risks

This best practice is reflected in the NSW Health Policy Directive Risk Management –Enterprise-Wide Policy and Framework (PD2015_043) which requires each public health organisation to establish and implement an enterprise-wide risk management framework.

Each public health organisation is required to ensure that it complies with various state laws relating to its operations, especially those that directly impose legal responsibilities for managing risk:

- *Public Finance & Audit Act 1983*;
- *Government Sector Finance Legislation (Repeal and Amendment) Act 2018*;
- *Annual Reports (Departments) Regulation 2015*;
- *Annual Reports (Statutory Bodies) Regulation 2015*;
- *Government Information (Public Access) Act 2009*;
- *Workplace Health & Safety Act 2011*;
- *Protection of the Environment Operations Act 1997.*

Application of an effective enterprise –wide risk management framework requires the examination of all aspects of an organisation's functions and responsibilities in order to identify and manage opportunities and risks.

7 AS/NZS ISO 31000:2009 Risk management – Principles and guidelines

11.4.1 Governance and risk

Effective risk management is built into governance and organisational structures, planning and operational processes in order to minimise the likelihood and impact of potential risks. This systematic and integrated approach enables public health organisations, to deliver on its performance objectives and meet its responsibilities and accountabilities to its stakeholders.

A responsive, open and consultative approach benefits the organisation and its stakeholders through active consultative processes, clear communication and education in risks, effective risk controls and the responsible management of risks at all levels of the organisation.

A key document on governance and risk is the NSW Auditor General's 2011 report Corporate Governance –Strategic Early Warning System

The NSW Auditor General's 2011 report *Corporate Governance – Strategic Early Warning System*, identified sound risk management as essential to good corporate governance.

Governance, risk management and compliance are three highly related but distinct disciplines, being that.

- Governance is performance and conformance and provides the direction and structure required to meet organisational objectives and enables your agency to properly manage your business;
- Risk Management provides the foundation for resilience, the policies and procedures enable your agency to continue to function effectively in a changing environment;
- Compliance is adherence to both external and internal requirements.

See also Clinical Governance section 5 of the Compendium.

11.4.2 Risk Management Framework[8]

Key areas of risk control include identification, assessment, management and integration into strategic and operational risk assessment. In order to achieve this requirement, all public health organisations must:

- have a risk management plan that identifies how the organisation will minimise, manage, record and monitor risk, including procedures for escalating risk reports to the chief executive and board.
- include risk management planning as a part of the strategic, operational and annual business planning activities of the organisation, its facilities and/or networks.
- have a risk register that is used to record, rate, monitor, report risk; and that facilitates the minimisation and management of risk.
- have an established process for monitoring and reviewing risk controls and governance systems.

11.4.3 Responsibilities

Management and all staff of public health organisations have a responsibility to ensure risk management principles are integrated into the organisation's daily operations. Risk identification, assessment and effective risk management is considered to be a core accountability of boards, chief executives and organisational staff and contractors.

Public health organisations have a responsibility to ensure that systems are in place to enable the organisation to deal responsibly and effectively in identifying, managing and mitigating risks through an enterprise –wide risk management plan and risk registers.

8 Risk management framework : "assist the organization in integrating risk management into significant activities and functions" AS/NZS ISO 31000:2018 Risk Management Guidelines Section 5.1

Key responsibilities for Boards, chief executives and Audit & Risk Committees in risk management

Boards

Boards of public health organisations, are responsible for establishing an Audit and Risk Management Committee to oversee, monitor, control, review and report on the implementation of policies, procedures programs and standards relating to organisational governance, services, functions, performance, compliance and risks.

Chief executives

Chief executives of public health organisations are accountable for multiple dimensions of performance – financial, clinical, management, quality, risk, community expectations and health outcomes. Their key risk performance accountabilities will relate primarily to ensuring appropriate robust clinical, organisational and financial management structures are in place within the organisation.

Chief executives need to ensure that there is:

- a robust risk management plan in place within the public health organisation and that this system is consistent with and embraces principles articulated by risk management approaches developed by the Ministry;
- an assessment, communication and reporting of risk that is clearly defined and differentiated;
- a regular review of the performance of the risk management plan and that review results are utilised as a basis for improvement;
- clear definition, allocation and documentation of the responsibility, accountability, authority and clearly defined interrelationships of those within the organisation who perform and verify work affecting risk management to an action plan:
- the identification and provision of adequate resources, particularly trained staff for the management performance of work and verification activities including internal review; and
- appropriate communication with internal and external stakeholders that has regard to their objectives and perceptions, and their needs for appropriate communication about risk management issues.

Audit & Risk Management Committee

The Audit & Risk Management Committee is a key component in the public health organisations corporate governance framework involved in the monitoring, review, oversight and reporting on:

- internal controls;
- enterprise risk management;
- business continuity plans;
- disaster recovery plans;
- corruption and fraud prevention;
- external accountability (including financial statements);
- compliance with applicable laws and regulations;
- internal audit and
- external audit.

The Audit & Risk Management Committee does not have executive powers or delegated financial responsibility, or management functions. The Committee is directly responsible to the governing board, or to the chief executive in a chief executive controlled public health organisation for the exercise of its responsibilities.

The Audit & Risk Management Committee has the ability to seek explanations and additional information concerning financial and risk management matters and to provide reports to the governing board or chief executive. Primary responsibility for the management of the organisation rests with the chief executive or board.

11.4.4 Risk Management Process, Methods and Resources[9]

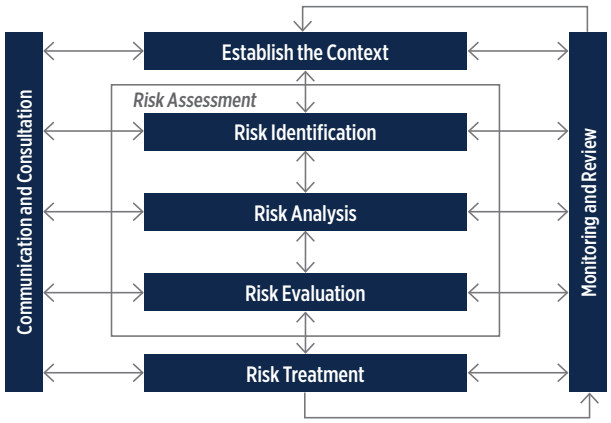
Key documents
NSW Health Policy Directive Risk Management Enterprise-wide Policy & Framework
NSW Policy Directive PD 2015_043 & AS/NZS ISO 31000:2018 Risk Management Principles & Guidelines

Policies, procedures, systems and internal controls for risk management should be clearly defined and communicated throughout the public health organisation. Appropriate resources should be in place to support risk management policy and practice.

To implement risk management across the organisation, boards and chief executives should:

- champion risk management within the organisation.
- ensure appropriate resources are allocated to managing and monitoring risk and to implementing risk minimisation and mitigation strategies which have been identified through risk planning activities.
- implement and keep current a risk management plan for the organisation.
- include risk assessments in strategic planning and decision making.
- ensure communication of risk management requirements to management and staff.
- establish and monitor the risk register for the organisation that provides for the recording, monitoring and management of risk.
- ensure that there is a formal delegation of authority from the chief executive to various levels of management within the entity to accept risks or take–up opportunities.
- review and action risks escalated from within the organisation.

Elements in the enterprise risk management processes framework[10] p11.



Source: NSW Treasury

9 See NSW Health Policy Directive Risk Management –Enterprise-Wide Policy and Framework NSW Health PD2015-043
10 See diagram in PD2015_043 page 14

Risk Management Process

Establishing the context

An important first step is to consider the strategic, organisational and risk management context in which risks will be identified, managed and evaluated within organisational structures and the processes.

Risk identification

Identify what may happen, compile a comprehensive list of events (both risks and opportunities) that may affect the organisation, the sources of the risk and the areas of impact., Some of the examples of key risk categories identified in relation to health service delivery include the following:

- clinical care & patient safety;
- health of the population;
- workforce;
- communication & information;
- facilities and assets;
- security;
- emergency & management;
- legal;
- finance;
- work, health & safety;
- environmental;
- leadership and management;
- community expectations.

Risk analysis

Risks are then analysed to understand the nature of the risks, to identify the potential likelihood of occurrence, the consequences and impacts.

Risk assessment

Risk assessment then involves the comparison with the level of risk identified in the risk analysis stage against pre-determined criteria to determine whether the risk is acceptable within tolerable limits, or, if not then how it should be treated, controlled and prioritised.

Risk treatment & controls

Risks may be treated in several approaches ranging from rejection and risk avoidance, reducing the likelihood of the risk occurring, reducing the potential consequences, transferring the risks or retaining the risk within a specified strategy.

For public health organisations there are several key areas of risk control which require the rigorous application of risk identification, assessment, management and integration into strategic and operational risk assessment. Some examples include:

- fraud prevention and control plans;
- internal audit charters or plans;
- budget management strategies and plans;
- clinical services plans;
- asset (capital) management plans;
- workforce and human resource management plans;
- information technology plans;
- community engagement plans;
- safe practice environment plans;
- leadership and management plans.

Monitoring and review of risks

Identified risks need to be continually monitored and reviewed to ensure that risk management plans are appropriate and risk control processes are effective and the overall risk management approach remains relevant.

Communication and consultation within the organisation and with stakeholders throughout the risk management cycle is critical to achieving an effective risk management process.

Audit and Risk Management – Resources & References

NSW Health Policy Directive, Risk Management – Enterprise-Wide Policy and Framework – NSW Health (PD2015_043):
https://www1.health.nsw.gov.au/pds/Pages/doc.aspx?dn=PD2015_043

NSW Health Policy Directive, Internal Audit – NSW Health (PD2016_051):
https://www1.health.nsw.gov.au/pds/Pages/doc.aspx?dn=PD2016_051

NSW Treasury, Internal Audit and Risk Management Policy for the NSW Public Sector, available at:
https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management

Audit Office of NSW website:
http://www.audit.nsw.gov.au/

SAI Global AS/NZS ISO 31000:2018 Risk Management Guidelines

The following documents are available on the NSW Health intranet only:

NSW Health Risk Matrix:
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/1_risk_matrix.pdf

NSW Health Risk Report Form
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/2_risk_report_form.pdf

Guidance Sheet for NSW Health Risk Report Form
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/3_guidance_sheet_risk_report_form.pdf

NSW Health Risk Management Self Assessment Checklist
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/4_self_assessment_checklist.pdf

NSW Health Risk Management Staged Implementation Plan
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/5_implementation_plan.pdf

Facilitating Risk Workshops
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/6_facilitating_risk_workshops.pdf

Identifying and Categorising Risks within NSW Health's priorities
http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/7_identifying_categorising_risks.pdf

Risk Management Glossary

http://internal.health.nsw.gov.au/cgrm/rmra/risk_management/8_glossary.pdf

Local Documentation

The enterprise-wide risk management plan, developed using the NSW Health policy directive framework

Risk register with both clinical and non-clinical risks

Documentation with clearly identified responsibilities for the management of clinical and non-clinical risk

The Audit and Risk Management Committee Terms of Reference; and minutes of meetings.

Disaster Management plan

Audit reports and any documentation which demonstrates the implementation of recommendations and system improvements, following audit appraisals, investigations, and reviews

Risk assessments which have been conducted to facilitate a safe environment

OHS and risk management training records

Records of OHS consultation