

# SESLHD PROCEDURE COVER SHEET



**Health**  
South Eastern Sydney  
Local Health District

<b>NAME OF DOCUMENT</b>	Enterprise Risk Management
<b>TYPE OF DOCUMENT</b>	Procedure
<b>DOCUMENT NUMBER</b>	SESLHDPR/304
<b>DATE OF PUBLICATION</b>	July 2025
<b>RISK RATING</b>	Medium
<b>LEVEL OF EVIDENCE</b>	National Safety and Quality Health Service Standards: Standard 1 – Clinical Governance
<b>REVIEW DATE</b>	July 2028
<b>FORMER REFERENCE(S)</b>	N/A
<b>EXECUTIVE SPONSOR</b>	Director, Clinical Governance and Medical Services
<b>AUTHOR</b>	SESLHD Risk Management Lead
<b>POSITION RESPONSIBLE FOR THE DOCUMENT</b>	<a href="mailto:SESLHD-Risk@health.nsw.gov.au">SESLHD-Risk@health.nsw.gov.au</a>
<b>FUNCTIONAL GROUP(S)</b>	Corporate Governance
<b>KEY TERMS</b>	N/A
<b>SUMMARY</b>	<a href="#">NSW Health Policy Directive PD2022_023 - Enterprise-wide Risk Management</a> directs all NSW Health organisations to establish and maintain a risk management framework that is appropriate and fit for purpose for the organisation. This procedure articulates how SESLHD meets the NSW Policy directive requirements.

## **COMPLIANCE WITH THIS DOCUMENT IS MANDATORY**

**This Procedure is intellectual property of South Eastern Sydney Local Health District.  
Procedure content cannot be duplicated.**

Feedback about this document can be sent to [SESLHD-Policy@health.nsw.gov.au](mailto:SESLHD-Policy@health.nsw.gov.au)

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

### 1. POLICY STATEMENT

[NSW Health Policy Directive PD2022\\_023 - Enterprise-wide Risk Management](#) directs all NSW Health organisations to establish and maintain a risk management framework that is appropriate and fit for purpose for the organisation. This procedure articulates how South Eastern Sydney Local Health District (SESLHD) meets the NSW Policy Directive requirements.

### 2. OBJECTIVE

This procedure articulates both the SESLHD Risk Management Framework (RMF) and the SESLHD Risk Management Process. This aligns with the NSW Health Policy to describe the minimum requirements for NSW Health organisations. It is complementary to the [NSW Health Policy Directive PD2022\\_022 - Internal Audit](#) and consistent with AS/NZS ISO 31000:2018 Risk Management – Guidelines.

This document sets out a comprehensive framework to guide SESLHD staff in the systematic identification, management, and escalation of risk. It outlines structured processes and responsibilities that support effective risk management. The aim is to ensure transparency, cultural safety, environmental sustainability, accountability, and informed decision making across the organisation. This is to assure the SESLHD Audit and Risk Committee and SESLHD Board of the adequacy and effectiveness of risk management practices.

The core principles of the Risk Management Framework and Risk Management Process are:

- Risk management is the shared responsibility of all SESLHD staff.
- Effective risk management is based on the thorough evaluation of data.
- Staff should be empowered to manage risks at the appropriate level of delegation.
- Successful risk management relies on collaboration and partnership.
- The four lines of defence help protect the organisation from risks that could prevent it from achieving its strategic objectives.
- The SESLHD Executive and Board have approved a defined risk tolerance and appetite for the organisation, and there is an expectation to manage and mitigate risks within this limit.

This procedure does not include project risk management.

### 2.1 DEFINITIONS

- **Additional Controls:** the additional controls describe what is required to be implemented to control the risk to the target risk rating and the target milestone.
- **Additional Control Approver:** the manager who has delegation to approve the additional controls required to mitigate the risk to the target risk rating.
- **Approving Manager:** the manager who has delegation to accept, reject or escalate the risk once entered in ERMs. The Approving Manager, sponsors

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

and has delegation, to approve and oversee the implementation of the additional controls required to mitigate the risk to the target risk rating.

- **ARC:** refers to SESLHD Audit and Risk Committee (SESLHD Board Committee). SESLHD Audit and Risk Committee have no executive powers, delegated financial responsibility or management functions, but provide independent advice to the Chief Executive and SESLHD Board by monitoring, reviewing and providing advice about the organisation's risk management framework.
- **Board:** in this document, references to "the Board" refer to SESLHD Board. SESLHD 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.
- **Current Controls:** the current controls describe all the mitigation activities that are currently in place to control the risk to its current risk rating.
- **Current risk rating:** the amount of risk at the time of reviewing the risk. This tracks the effectiveness of the implementation of the additional controls. The initial and current risk ratings will be the same when the risk is first entered into ERMs.
- **Delegation:** this refers to the delegations outlined for roles within the SESLHD Delegation of Authority Manual.
- **ERMS:** is the SESLHD Enterprise Risk Management System or 'Risk Register.'
- **Hazard:** anything that has the potential to cause harm, injury, damage, or other undesirable outcomes.
- **Impact:** the actual effect or consequence that occurs when a hazard materialises.
- **Initial (Inherent or residual) Risk Rating:** the amount of risk at the time of the initial risk assessment. Inherent risk is when assessing risk without any controls in place (unlikely scenario in health). Residual risk is the level of risk with the existing or current controls accounted for.
- **Key Risk Indicator:** Key Risk Indicators (KRIs) are measures/data that are used to identify when risk is within or outside risk appetite or tolerance.
- **Milestones:** Milestones describe the quantitative and qualitative outcomes that will be achieved by implementing the additional controls. These will be linked to the data used to establish the key risk indicator and the outcome or target required to bring the risk into tolerance.
- **Risk:** the likelihood and consequence (severity) of harm resulting from exposure to a hazard
- **Risk Appetite:** the amount and type of risk that SESLHD Board is prepared to pursue, retain or take to achieve objectives and strategic goals. Refer to [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#).
- **Risk Category:** risk categories are a systematic way to classify and organise risks. They help SESLHD categorise the impact on business objectives.
- **Risk Category Owner:** a member of SESLHD Executive Leadership Team who has ownership of a District Strategic Risk Category and oversight of additional control and mitigation strategies.
- **Risk Owner:** the role that has delegated responsibility and accountability to minimise the impacts of a documented risk by ensuring the implementation of additional controls.
- **Risk Owner (Delegate):** the role delegated by the risk owner to ensure that

# SESLHD PROCEDURE

## Enterprise Risk Management

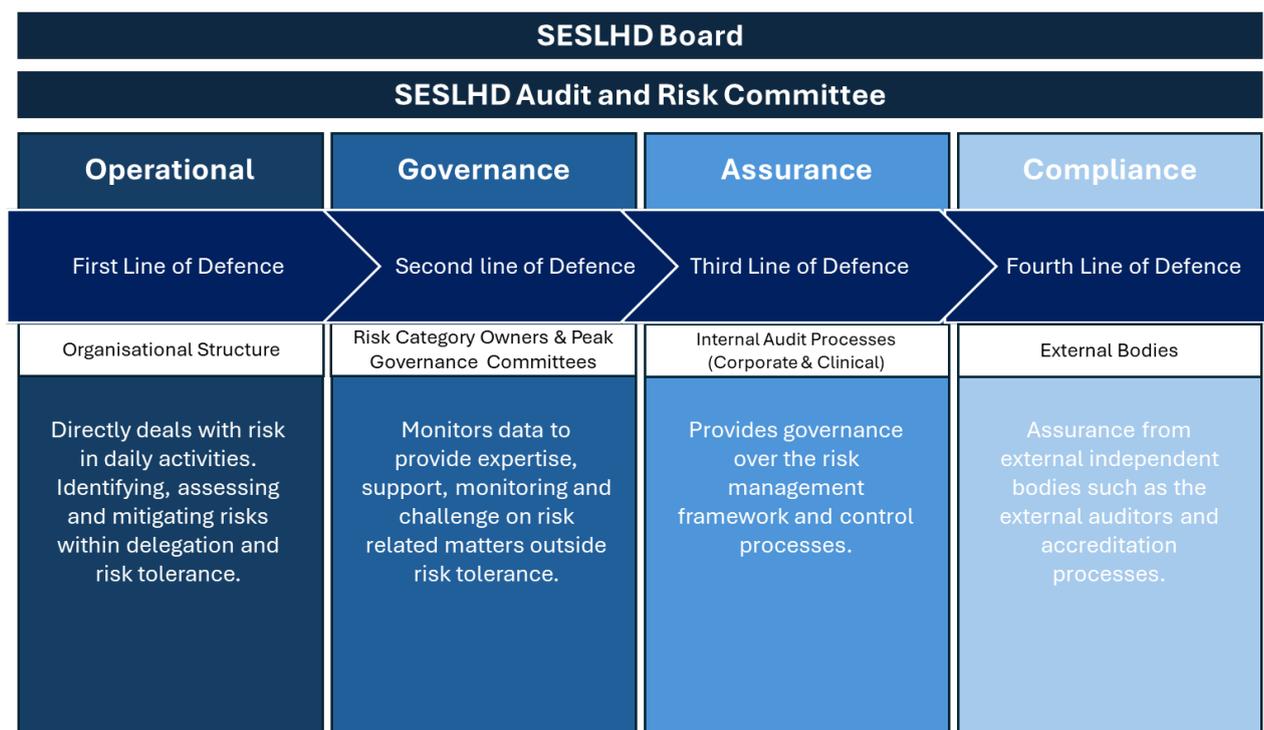
SESLHDPR/304

an identified risk is monitored and reviewed in ERMS within set timeframes, and that current and additional controls are actively implemented.

- **Risk Tolerance:** the assessed and accepted threshold levels of risk exposure that, when exceeded, will trigger a risk assessment and review of current controls.
- **Target Risk Rating:** the desired optimal level of risk, when additional controls have been implemented, and the target milestones have been achieved. This should be within the SESLHD risk appetite and tolerance level for the risk category.

### 3. RESPONSIBILITIES

The SESLHD RMF uses a tiered model known as the Four Lines of Defence to manage risk. This approach provides an integrated and comprehensive safety net to protect the organisation from potential hazards. Various levels and structures within the organisation are responsible for different elements of this framework. See [Appendix B: SESLHD Risk Management – 4 Lines of Defence](#).



#### 3.1 First Line of Defence: Operational risk within line management

The first line of defence is operational line management, running from frontline staff to the Chief Executive. It involves the ability of the operational line to identify, assess, manage or escalate risk during routine operations. This is essential for ensuring high-quality care and is enabled by the operational team’s extensive understanding of the organisation’s culture, processes, and daily challenges to inform decision making and enable prompt corrective actions when needed.

**3.1.1 All staff:**

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

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. Staff have a responsibility to identify hazards, report them to the appropriate level of management, and document them in the appropriate notification system, refer to [Section 5.1 Risk Identification through Notification and Reporting Systems](#).

Risks that are beyond a staff member's delegation of authority to control must be escalated to a higher level of operational management for review, refer [Appendix C: SESLHD Risk Management Process Chart](#).

**3.1.2 Managers:**

Managers and decision makers at all levels in NSW Health organisations are accountable for managing risk within their sphere of authority and delegation. They are responsible for initiating the risk assessment process when a risk is outside of tolerance or when staff and/or data within notification or reporting systems indicates that a potential risk needs further investigation, refer to [Section 5.1 Risk Identification through Notification and Reporting Systems](#) and [Appendix C: SESLHD Risk Management Process Flow Chart](#).

The manager must have the appropriate delegation to accept, reject or escalate the risk, once entered in ERMS.

**3.1.3 General Managers or Directors:**

General Managers and Directors are responsible for managing all risks within their approved delegation and ensure appropriate mitigation strategies are in place. It is the role of the General Manager/Director to review and ratify high or extreme risks escalated to them via ERMS. Where a risk exceeds their delegation or has broader organisational implications, the General Manager/Director must escalate the risk to the Chief Executive for further action, including referral to the relevant SESLHD Peak Committee for acceptance.

**3.1.4 Chief Executive:**

The Chief Executive holds overall responsibility and accountability for risk management in SESLHD and plays a central role in shaping the organisation's risk culture. The Chief Executive is responsible for nominating the SESLHD Chief Risk Officer.

The Chief Executive is accountable for internal controls, including adhering to established policies and the NSW Health Code of Conduct. The Chief Executive is responsible for ensuring necessary controls and treatment plans are in place to effectively manage risk. The Chief Executive also attends the SESLHD Audit and Risk Committee to discuss the current management of risk and internal controls.

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

Where SESLHD is unable to manage a risk within its tolerance levels and is not prepared to accept the level of risk, the Chief Executive is able to escalate the risk to the Ministry, via SESLHD Board, for additional guidance and support. If the risk identified has the potential to be 'system-wide' the Chief Executive should notify the Ministry of Health's Corporate Governance and Risk Management Unit in accordance with [NSW Health Policy Directive PD2022\\_023 - Enterprise-wide Risk Management](#).

### 3.2 Second Line of Defence: Risk category strategic management and governance

The Second Line of Defence provides subject matter expertise and governance within SESLHD Risk Categories. Second Line resources are separate from those responsible for operational delivery and provide additional expertise to control risk that can be utilised by the First (Operational) Line.

#### 3.2.1 SESLHD Chief Risk Officer:

All NSW Health organisations are required to nominate or appoint an appropriately skilled Chief Risk Officer. 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 and resources associated with coordinating, maintaining and embedding the framework in the organisation

#### 3.2.2 SESLHD Risk Category Owners:

Specified members of the SESLHD Senior Executive Team who are responsible for managing delegated strategic risk categories. They are responsible for ensuring necessary controls and treatment plans are in place to effectively manage the over-arching risk category, including the formulation of strategic plans, the provisioning of resources and the reporting of progress to ARC when requested. SESLHD Risk Category Owners advise the Board annually on the key risk indicators, tolerance and appetites for their respective category. Refer to [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#).

#### 3.2.3 SESLHD Peak Governance Committees:

SESLHD Peak Committees for Corporate and Clinical Risk provide an additional level of assurance, independent of the operational line. As per [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#) the peak SESLHD committees for risks within Clinical and Corporate Risk Categories are;

- **SESLHD Clinical and Quality Council** – Clinical Care and Patient Safety Risk Category
- **SESLHD Executive Meeting** – All Corporate Risk Categories

The SESLHD Peak Committees and their respective Charter's ensure that SESLHD operates within defined risk tolerance and appetite levels.

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

If the SESLHD Peak Committees are not adequately assured that out of tolerance corporate and clinical risks are being effectively controlled, they may assign an action to the appropriately delegated operational manager to initiate a risk assessment. Please refer to the [Appendix C: SESLHD Risk Management Process Chart](#).

All Clinical and Corporate risks in ERMS that fall outside of SESLHD's risk tolerance and appetite will be reported to and periodically reviewed by the requisite SESLHD Peak Committee.

### 3.3 Third Line of Defence: Internal Audit

#### 3.3.1 Internal Audit and Clinical Governance Unit:

The third line of defence provides SESLHD with an additional level of assurance regarding the effectiveness of corporate and clinical governance, risk management, and internal controls. This is accomplished through the delivery of independent and objective advice, primarily via audits and reviews that are conducted separately from operational management. This process is implemented as outlined below:

**Internal Audit** is responsible for providing assurance to the Chief Executive, SESLHD Board 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 annual Internal Audit Program is aligned to areas escalated within the Risk Management Framework. The organisation's enterprise-wide risk management framework must be the subject of an internal audit at least once every five years.

**Clinical Governance Unit (CGU)** is responsible for providing assurance to the Chief Executive surrounding compliance to the National Safety and Quality Health Care (NSQHS) Standards. CGU will complete an independent annual Clinical Audit program which is aligned to areas escalated within the Risk Management Framework.

### 3.4 Fourth Line of Defence: External Audit

#### 3.4.1 External auditing agencies and third parties:

The fourth line of defence focuses on external assurances provided by independent assessors, regulators, and other external bodies. While the first, second and third lines of defence focus on risk management within the organisation, the fourth line, when referring to external bodies, provides an independent, external perspective on the effectiveness of those processes.

Their specialised expertise can offer an unbiased evaluation of whether the organisation is meeting compliance standards, regulatory requirements, and industry best practices e.g. Accreditation auditors for NSQHS or NSW Work Health Safety Inspectors. This enhances the organisation's governance by ensuring transparency, providing objective assessments, and reassuring the public that the organisation is effectively managing its risks and complying with regulations.

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

### 4. SESLHD RISK MANAGEMENT FRAMEWORK

The SESLHD Risk Management Framework is in alignment with the ISO 31000:2018 Risk Management Guideline; Principles, Framework and Process. This is the underlying international standards that form the basis of the [TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector](#), [NSW Health Policy Directive PD2022\\_023 - Enterprise-wide Risk Management](#) and [NSW Health Policy Directive PD2022\\_022 - Internal Audit](#).

#### 4.1 Leadership Commitment

SESLHD is committed to strong governance and leadership, with risk management being a key element of operations at all levels. It is essential for enhancing management systems and supporting the successful achievement of objectives and strategic goals. The SESLHD Senior Executive Team and SESLHD Board endorse this procedure, which outlines the SESLHD Risk Management Framework, as well as the Corporate and Clinical Risk Categories, Tolerances, and Appetite Statements.

#### 4.2 Integration

The Risk Management Framework is integrated into SESLHD operations and governance structures as articulated in [Section 3: Responsibilities](#), [Appendix B: SESLHD Risk Management – 4 Lines of Defence](#) and [Appendix C: SESLHD Risk Management Process Chart](#).

#### 4.3 Design

SESLHD Risk Management Framework, Risk Categories, Tolerances and Appetite have been designed by considering both the external and internal context to SESLHD which includes, but is not limited to:

- Social, cultural, political, legal, regulatory, financial, technological, economic and environmental/climate change factors
- Key drivers and trends affecting the objectives of SESLHD
- External stakeholders' relationships, perceptions, values, needs and expectations
- Contractual relationships and commitments
- The complexity of networks and dependencies
- NSW Health CORE values
- Governance, organisational structure, roles and accountabilities
- SESLHD strategy, objectives and policies
- SESLHD's risk culture

#### 4.4 SESLHD Risk Categories, Tolerance and Appetite Statements

The purpose of categorising risk allows a consistent framework to be applied when considering risk in SESLHD. [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#) sets out the following:

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

- Risk Category definition
- The Risk Category Owner of the over-arching risk category
- SESLHD Committees that assures risks within the category are appropriately managed
- Key Risk Indicators (KRI) – The over-arching data used by SESLHD to measure the risk category and its effect on SESLHD meeting its objectives
- Risk Tolerance – The appetite statements show the tolerance that SESLHD has assigned for the data and how the KRI converts to Low, Medium, High or Extreme Risk ratings
- Risk Appetite Statement – these statements give an over-arching statement on the level of risk SESLHD is willing to tolerate within a particular risk category.

The adapted NSW Health Risk Matrix for SESLHD helps staff to use the notification data outlined in [Section 5.1 Risk Identification through Notification and Reporting Systems](#) as a Key Risk Indicator and assign a risk rating to their risks. This provides inter and intra reliability to the SESLHD Risk Management Framework. A Risk Assessment as described in [Section 5.4 Risk Assessment](#) and [Appendix C: SESLHD Risk Management Process Chart](#) must be completed to meet the needs and complexity of the risk identified. Risk assessments must look at risk in the context of [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#) and adapted NSW Health Risk Matrix for SESLHD.

### 4.5 Implementation

Implementation of the Risk Management Framework and Process is mandated across all teams within SESLHD. The Risk Management Team are available to help all staff at all levels of SESLHD to build capability within SESLHD Risk Management Framework in accordance to the delegation and responsibilities assigned to role. Please contact [seslhd-risk@health.nsw.gov.au](mailto:seslhd-risk@health.nsw.gov.au) for assistance.

### 4.6 Evaluation

Periodic evaluation of SESLHD risk maturity will be conducted via the NSW Government Risk Maturity Assessment framework. The SESLHD Board will review and endorse the SESLHD Corporate and Clinical Risk Categories, Tolerances, and Appetite Statements on an annual basis. This ensures that the risk appetite and tolerance are aligned to achieve SESLHD's objectives and strategic direction. Evaluation of the SESLHD Risk Management Framework is described in [Section 7 Audit](#) of this procedure.

### 4.7 Improvement

SESLHD should continually monitor and adapt the risk management framework to address external and internal changes. Improvement can occur from but is not limited to:

- Annual review by the SESLHD Senior Executive Team and SESLHD Board of the SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements
- Annual Internal Audit and Risk Management Attestation
- Feedback from periodic Risk Maturity Assessment
- Feedback from Internal Audit

Once implemented, these improvements should contribute to the enhancement of risk management and achieving SESLHD's objectives and strategic direction.

# SESLHD PROCEDURE

## Enterprise Risk Management

SESLHDPR/304

### 5. SESLHD RISK MANAGEMENT PROCESS

The SESLHD RMF follows the ISO 31000:2018 Risk Management Guideline – Process.

#### 5.1 Risk Identification through Notification and Reporting Systems

As stated in [Section 3.1.1](#) all staff (permanent, temporary or contract) are accountable for identifying and managing risk in their day-to-day roles, including carrying out their roles in accordance with their delegation, policies and procedures.

Quantifiable risk identification is possible through the data available to staff and operational managers, within the notification systems. Refer to [Appendix C: SESLHD Risk Management Process Chart](#).

<b>SESLHD Risk Category</b>	<b>Notification/Reporting System</b>
Clinical Care and Patient Safety	Incident Management System (IMS+) Quality Audit Reporting System (QARS) Quality Improvement Data System (QIDS) Hospital Acquired Complication (HAC) data
Service Delivery (Business Continuity and Emergency Management)	SESLHD Health Services Functional Area Coordinator (HSFAC) notification Incident Management System (IMS+) Code System
Infrastructure – Buildings and Equipment	Asset and Facilities Management Online System (AFMO) Incident Management System (IMS+) Code System
Infrastructure - Digital	SARA Ticket Incident Management System (IMS+)
Governance and Performance	NSW Health SLA Reporting SESLHD OrBiT
Financial Management	PowerBudget PowerFTE
People and Culture	Recruitment and On-Boarding (ROB) Stafflink Health Roster People and Talent (PAT) My Health Learning (MHL) People Matters Employee Survey (PMES)
Work Health and Safety	Incident Management System (IMS+) Quality Audit Reporting System (QARS) Workers Compensation Claim Data

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

### 5.2 Communication and Consultation

Any variations in quantitative data within SESLHD Risk Notification Systems or qualitative staff feedback that may indicate a potential risk should be communicated to the direct line manager in the first instance.

To ensure key stakeholders have been consulted, this should also be communicated at an appropriate forum or meeting.

### 5.3 Scope, Context and Criteria

If a manager determines that a potential risk requires further assessment, they should determine the appropriate scope and context for a risk assessment and assign a Risk Owner.

The Risk Owner should be a manager with the appropriate level of delegation to oversee the assessment of the identified risk, typically a Divisional or Co-Director. They may delegate the task of conducting the risk assessment to another manager within their operational line, referred to as the Risk Owner Delegate. The scope should specify what is included in the risk assessment, what is excluded, which data will be considered as Key Risk Indicators and the target risk level to be achieved.

The risk assessment team leader, which can be the Risk Owner Delegate, must assign an appropriate assessment team (risk partners). The size and scope of the risk assessment team must meet the complexity of the risk assessment.

This aims to:

- Bring different areas of expertise together for each step of the risk management process and ensure cross team collaboration
- Ensure that different views are appropriately considered when defining risk criteria and when evaluating risks
- Provide sufficient information to facilitate risk oversight and decision-making
- Build a sense of inclusiveness and ownership among those affected by risk

### 5.4 Risk Assessment

Risk assessments are to be documented using the [SESLHD Risk Assessment Tool](#) unless otherwise specified by a NSW Health Policy Directive.

A risk assessment involves:

- **Identification:** Identification of hazards caused by an event and its potential impact on SESLHD risk categories.
- **Analysis:** Analysis of the likelihood and consequence of impacts occurring using adapted NSW Health Risk Matrix for SESLHD.
- **Evaluation:** Evaluation of the effectiveness of current controls in mitigating identified impacts occurring.
- **Treatment:** Decision on whether to Tolerate or Treat the assessed risk with additional controls. If treated, the design of Additional Controls to further mitigate the risk of the event occurring to a more tolerable level of consequence and likelihood

### **5.4.1 Identification of Hazards and Analysis of Current Control Effectiveness and Risk Rating**

The risk assessment team is responsible for reviewing key risk indicator data within the relevant notification system to identify hazards within the prescribed scope of the assessment.

For each identified hazard, the team assesses and documents the potential impact the hazard could have. The risk assessment team then needs to determine the consequence and likelihood of the impact occurring. Refer to [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#) for the over-arching SESLHD Key Risk indicators for the relevant risk categories.

The impact of a hazard is the actual effect or consequence that would occur if the hazard materialised e.g. Harm caused due to a safety incident, magnitude of service disruption or asset damage.

The likelihood of the impact of a hazard occurring is determined by analysing the best available data to determine when the impact last occurred and determine how likely it is in occurring again and at what frequency.

The risk assessment team must consider the current controls that are in place to decrease the likelihood and or consequence of the impact occurring. This process requires analysis of relevant data sources and uses the adapted NSW Health Risk Matrix for SESLHD to rate the consequence and likelihood of a risk.

It is very unlikely in health that an inherent risk rating will be assigned, as an inherent risk rating is the consequence and likelihood of an impact occurring without any controls in place. A residual risk rating is the level of risk with the existing or current controls accounted for.

Current controls are usually business as usual processes, resources, credentialling requirements and NSW systems embedded to decrease the consequence and likelihood of a potential hazard occurring and its associated impact.

### **5.4.2 Decision on Whether to Tolerate or Treat the Current Controls**

Once the risk rating has been assigned, the risk assessment team is required to evaluate the effectiveness of current controls. If the assigned risk rating is outside of tolerance the current controls must be treated.

This process will identify which controls will be tolerated and any that require further addressing.

## **5.5 Risk Treatment – Formulation of Additional Controls**

If the Risk Assessment process determines that the current controls do not effectively mitigate the risk, a decision will be made to treat the risk with additional controls.

The risk assessment team should consist of individuals with the necessary expertise to evaluate the current controls and ability to propose suitable additional controls. The required individuals will vary depending on the risk category and scope of the assessment. Developing additional controls requires consultation with subject matter experts within the risk assessment team. Consider that additional controls may be required from teams outside of the immediate operational line management of the Risk Owner.

If a risk assessment relates to Aboriginal and Torres Strait Islander patients, families or staff, it is important to recognise the historical trauma that healthcare systems have placed on Aboriginal people. The Aboriginal Hospital Liaison Officer or Aboriginal Health Directorate should be involved in the risk assessment process and the development of additional controls to provide culturally appropriate strategies.

Proposed additional controls must have an assigned additional control owner and approver. The Additional Control Approver must have the delegation to authorise the implementation of the additional control. They may then delegate this implementation to an Additional Control Owner.

Proposed additional controls must set out additional actions, that when implemented, will achieve the desired target risk rating and desired milestones. The target risk rating should be within the SESLHD risk appetite and tolerance level for the risk category. [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#).

Risks or opportunities which identify one-off and/or recurrent funding requirements are required to be managed and escalated through normal business processes, noting the ERMS number.

For example risk assessments, refer to the resources section on the SESLHD Intranet > [Risk Management](#) or contact SESLHD Risk Management Team [seslhd-risk@health.nsw.gov.au](mailto:seslhd-risk@health.nsw.gov.au) for assistance.

## **5.6 Approval, Escalation and Rejection of a Risk Assessment, Additional Controls and Documentation in ERMS**

### **5.6.1 Approving a Risk Assessment and Documenting in ERMS**

The responsibility of the Approving Manager is to ensure current and target risk ratings have been established based on the most accurate information and data source/s available and considered SESLHD Key Risk Indicators in line with the [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#).

The Approving Manager must review the feasibility of the proposed additional controls and approve them if appropriate. If approved, the risk may then be registered in ERMS by the **Risk Owner** (or delegate). The Approving Manager will be notified via email and can then accept the risk. **If the risk is rated high or extreme**, the Approving Manager must escalate the risk on ERMS to the General Manager or Director, as per [Section 5.6.2](#).

**5.6.2 Escalating High or Extreme Risk Assessments**

Following completion of a risk assessment, any risk rated as high or extreme must be escalated in ERMS by the Approving Manager to the relevant General Manager. If the General Manager ratifies the risk rating, the Risk Management Team is responsible for escalating it to the SESLHD Executive Meeting or Clinical Quality Council for discussion and ratification.

A risk that is unable to be managed to be within its tolerance levels and SESLHD is not prepared to accept the level of risk, or the risk has NSW Health system implications, SESLHD is to escalate the risk to the Ministry of Health via the SESLHD Executive Leadership Team and SESLHD Board for additional guidance and support. Contact SESLHD Risk Management Team [seslhd-risk@health.nsw.gov.au](mailto:seslhd-risk@health.nsw.gov.au) for immediate assistance.

**5.6.3 Rejecting a Risk Assessment**

A risk assessment may be rejected for various reasons, such as insufficient information from the Risk Owner or assessment team, an incomplete/improperly conducted assessment, or if the proposed additional controls are not approved.

Even if a risk is within tolerance, the Approving Manager may still reject it if the proposed additional controls are not accepted at that time. This could be due to factors such as the prioritisation of objectives or the timing of implementation. The decision must be documented and returned to the Risk Owner, who may either resubmit alternate controls or continue to monitor and reassess the risk at a later date. The risk may also be considered in future business or strategic planning.

Any rejection of a risk assessment should be discussed with the Risk Owner.

**5.7 Monitoring and Risk Reviews**

SESLHD has assigned the following review times for ERMS risks with the current risk rating of:

<b>Current Risk Rating</b>	<b>Minimum Timeframe for Review</b>
<b>Extreme (A-E)</b>	30 Days
<b>High (F-K)</b>	30 Days
<b>Medium (L-T)</b>	90 Days
<b>Low (U-Y)</b>	90 Days

Risk reviews should detail the progress made in implementing the additional controls necessary to achieve the target risk rating and milestones. During the review, the current risk rating may be adjusted based on the Key Risk Indicator used in the initial assessment. The current risk rating may increase or decrease depending on data and/or the progress of implementing the additional controls.

When an existing 'accepted' risk is reviewed and the current risk rating deteriorates from medium to high or high to extreme, the Risk Management Team will escalate the risk for re-approval. This gives the Approving Manager the opportunity to re-review the suitability of the additional controls.

Best practice is to review the risk in unison with achieving milestones during implementation of additional controls. Risk Owners are expected to complete their own reviews and updates in ERMS.

All risks entered in ERMS will be reviewed and quality controlled by the Risk Management Team, who will contact the Risk Owner and Approving Manager if there are any questions or concerns about the integrity of the data. The Risk Management Team, under the delegation of the Chief Risk Officer, have authority to amend the risk detail for minor updates or where data changes do not require approval as per the delegations.

Narrative in ERMS is used for Executive and Board Reporting and should be contemporaneous with the implementation of additional controls.

The resources section of the SESLHD Intranet > [Risk Management](#) provides comprehensive guidance on the use of ERMS and its functions or contact SESLHD Risk Management Team [seslhd-risk@health.nsw.gov.au](mailto:seslhd-risk@health.nsw.gov.au) for assistance.

## 5.8 Risk Closure

Risk Owners must receive approval from all risk stakeholders including the Approving Manager and Additional Control Owner, before closing a risk.

A risk can be closed in ERMS when the current risk rating reaches the target risk rating and/or the additional controls in place have been assessed as adequate for ongoing monitoring. It is important to detail this evidence in the 'Reason for Reviewing' risk field at the point of closure.

To close a risk which remains out of tolerance, the Risk Owner should contact the Risk Management Team to ensure sufficient documentation and appropriate approval.

'Closed' risks generate an automated email notification and the risk moves to the 'Completed' risk's view in ERMS. 'Completed' Risks are still part of the SESLHD Risk Register, these risks are within SESLHD risk tolerance and do not have an active implementation plan for additional controls. The current risk rating has reached the target risk rating and no further change in the risk rating is expected and/or no further additional controls are required to be implemented. The current documented controls mitigating the risk are acceptable.

# SESLHD PROCEDURE

## Enterprise Risk Management

**SESLHDPR/304**

### 5.9 Risk Reporting

Risk Reporting is undertaken by the SESLHD Risk Management Team with risk data reported to the appropriate committee, facility, executive or manager for action. Risk Owners are expected to be diligent in the review of risks assigned to them and be thorough with their evidence of:

- What additional controls are being implemented.
- What milestones they expect to achieve the target risk rating.
- That the review narrative and current risk rating reflect the progress against the additional control implementation plan against the target milestones and risk rating. Narrative in ERMS is used for Executive and Board Reporting and should be contemporaneous with the status of implementation of additional controls.

The SESLHD Risk Management Team will download and process data from ERMS for monthly reporting and compliance reporting as required. Notification and reporting is also provided to the NSW Ministry of Health as required and when strategic and operational risks are identified that may have the potential to impact the NSW Health System more broadly.

### 6. DOCUMENTATION

SESLHD Risk Management Framework, resources and information can be accessed on the SESLHD Intranet > [Risk Management](#).

### 7. AUDIT

SESLHD Risk Management Framework must be the subject of an Internal Audit at least once every five years as directed by [NSW Health Policy Directive PD2022\\_023 - Enterprise-wide Risk Management](#). The Internal Audit and Risk Management Attestation Statement is submitted annually to the Secretary, NSW Health regarding SESLHD conformance or otherwise to [NSW Health Policy Directive PD2022\\_032 - Enterprise-wide Risk Management](#) and [NSW Health Policy Directive PD2022\\_022 - Internal Audit](#). The Internal Audit and Risk Management Attestation Statement is then communicated to the SESLHD Audit and Risk Committee and SESLHD Board.

### 8. REFERENCES

- ISO 30001:2018 – ISO 31000:2018 Risk Management Guidelines
- [TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector](#)
- [NSW Health Policy Directive PD2022\\_023 - Enterprise-wide Risk Management](#)
- [NSW Health Policy Directive PD2022\\_022 - Internal Audit](#)
- [SESLHDHB/027 - SESLHD Delegations of Authority Manual](#)

### 9. APPENDIX

- [Appendix A: SESLHD Corporate and Clinical Risk Categories, Tolerances and Appetite Statements](#)
- [Appendix B: SESLHD Risk Management – 4 Lines of Defence](#)
- [Appendix C: SESLHD Risk Management Process Chart](#)

# SESLHD PROCEDURE

## Enterprise Risk Management

SESLHDPR/304

### 10. VERSION AND APPROVAL HISTORY

Date	Version No.	Author and approval notes
September 2011	0	Michael Spence, Manager Enterprise Risk Management
May 2014	1	Approved by DET & Chief Executive
October 2015	2	Revised by Michael Spence, Manager Enterprise Risk Management.
November 2015	2	Re-formatted by District Policy Officer. Submitted to the Deputy Chief Executive for approval.
November 2015	2	Submitted to the DET for information.
November 2015	2	Minor changes to procedure. Executive Sponsor endorsed to publish.
January 2021	3	Major review commenced. Substantial revision following system and framework updates.
February 2021	3	Draft for comment period.
June 2021	3	Final version approved by Executive Sponsor. To be tabled at Corporate Executive Council for approval.
July 2021	3	Approved at Corporate Executive Council.
October 2022	4	Review commenced. Chief Risk Officer – Revision following implementation of <a href="#">NSW Health Enterprise-wide Risk Management Policy PD2022_023</a>
December 2022	4	Draft for comment period.
February 2023	4.1	Approved by Executive Sponsor.
March 2023	4.1	Approved by SESLHD Executive Council and published by SESLHD Policy team.
10 July 2025	5.0	Major review commenced following 2024 Risk Maturity Assessment and associated program of works. Approved at SESLHD Executive Meeting and SESLHD Board as per PD2022_023.