SA Health

Policy

Risk Management, Integrated Compliance, and Internal Audit

Version 2.0

Approval date: 26 September 2024

PDS Reference No: D0508

Government of South Australia

SA Health

1. Name of Policy

Risk Management, Integrated Compliance, and Internal Audit

2. Policy statement

This policy provides the mandatory requirements that apply across SA Health to effectively govern and manage risk, compliance with applicable obligations and internal audit functions.

3. Applicability

This policy applies to all employees and contracted staff of SA Health; that is all employees and contracted staff of the Department for Health and Wellbeing (DHW), Local Health Networks (LHNs) including state-wide services aligned with those Networks and SA Ambulance Service (SAAS).

4. Policy principles

SA Health's approach to risk management, integrated compliance, and internal audit is underpinned by the following principles:

- We support a culture where risk management, integrity, and continuous improvement practices are integral to the achievement of SA Health's objectives.
- We apply effective risk management practices to support the achievement of our objectives, consistent with the agency's risk appetite and tolerance levels.
- We establish and maintain systems and processes to:
    - Ensure risks are identified, assessed, managed, reported, and acted upon in a timely manner.
    - Deliver risk-based compliance and assurance activities that are designed to provide insightful improvement recommendations to assist in meeting the agency's objectives.
    - Facilitate, monitor, and report on compliance with relevant obligations, and internal audit findings and recommendations.
- We integrate risk management in all organisational activities, including integrated compliance and internal audit, to ensure an effective and coordinated risk response.
- We demonstrate integrity, competence, and professional due care in the delivery of risk and compliance functions and internal audits by adhering to relevant professional and ethical standards.
- We involve relevant stakeholders in decision making.

5. Policy requirements

- Each agency must establish an independent Audit and Risk Committee to provide oversight on risk management, integrated compliance, and internal audit activities.

Risk Management

- Each agency is responsible for implementing a process of identifying, assessing, managing, and reporting on risks, controls and treatments and must:
    - Establish an integrated risk management system and maintain those systems and processes to ensure risks are adequately managed, in line with:
        - ISO31000:2018 Risk Management – Guideline
        - SA Government Risk Management Guide
        - SA Health Policies and Frameworks
        - Legislative and regulatory requirements, and Standards or industry guidelines, where applicable
    - Establish a risk appetite statement and risk tolerances.
    - Ensure that:
        - Risk assessments demonstrate that relevant stakeholders have been consulted.
        - The SA Health Risk Matrix has been applied.
        - Risks are managed considering the agency's risk appetite and tolerance.
        - The frequency of a risk's review is considerate with the agency's risk rating.
        - Risk is reassessed as a result of any new information including but not limited to corrective audit and/or compliance actions undertaken.
    - Establish appropriate risk escalation protocols (refer to Appendix 1: Escalation Mandatory Instruction).
    - Provide a six monthly report on the agency's strategic risks to the DHW Risk and Assurance Services unit which enables DHW to monitor and provide feedback on risk trends across the system to agencies and the Health Chief Executive's Council (HCEC).

Integrated Compliance

- Each agency is responsible for implementing a process of identifying, risk assessing, managing, and reporting on compliance obligations and breaches and must:
    - Establish an integrated compliance management system (ICMS) in line with ISO 37301:2021 – Compliance management systems.
    - Implement and maintain a Compliance Obligations Register in line with risk management principles.
    - Establish effective systems for oversight, monitoring and reporting of compliance breaches and related corrective actions.
- Identified findings relating to non-compliance which require action from DHW in the capacity of System Leader must be escalated in accordance with Appendix 1: Escalation Mandatory Instruction.

Internal Audit

- Each agency must:
    - Establish an Internal Audit Charter, with accompanying procedures, that describes the purpose, authority, responsibilities, and activities of the function.
    - Ensure that:
        - The internal audit strategic direction is set by the agency and not by any external internal audit service suppliers.

        - The internal audit function is independent and resourced with appropriately experienced staff who adhere to relevant professional and ethical standards.
        - Internal audit activities operate in accordance with the IIA International Professional Framework (IPPF) and International Standards for the Professional Practice of Internal Auditing (prior to 9 January 2025) or Global Internal Audit Standards (from 9 January 2025).
    - Establish risk based internal audit plans in consultation with key stakeholders including the agency's Audit and Risk Committee.
    - Establish effective systems for oversight, monitoring and reporting of audit related corrective actions.
    - Provide DHW Risk and Assurance Services unit with approved and endorsed local internal audit reports which identify findings over centralised processes for the purposes of establishing and tracking remediation strategies (refer to Appendix 1: Escalation Mandatory Instruction). Instances where findings require DHW's immediate attention following identification, also refer to Appendix 1: Escalation Mandatory Instruction.
- DHW Risk and Assurance Services unit will provide agencies and HCEC with approved and endorsed DHW internal audit reports undertaken on centralised processes for the purposes of informing the system on findings identified and remediation to be undertaken by DHW, to communicate any actions which require remediation locally, and for agencies to consider whether further local risks exist which may warrant a review. Actions required to be remediated locally will be recorded, managed, and followed up by the relevant agency.

6. Mandatory related documents

The following documents must be complied with under this Policy, to the extent that they are relevant:

- Department of Treasury and Finance - *Treasurer's Instructions 2* and *Treasurer's Instructions 28*
- ISO 37301:2021 – Compliance management systems
- ISO 31000:2018 Risk management – Guidelines
- *SA Government Risk Management Guidelines*
- *SA Health Risk Matrix* (Available from the *SA Health intranet)*

7. Supporting information

- *Global Internal Audit Standards*
- Internal Audit Charter (agency level)
- *Institute of Internal Auditors Internal – various resources*
- Institute of Internal Auditors (IIA) *International Professional Practices Framework (IPPF)*
- Integrated Compliance Framework (agency level)
- Local instructions or protocols (agency level implemented procedures)
- *Risk Appetite Statement for the Department for Health and Wellbeing*
- Risk Management Framework (agency level)

8. Definitions

- **Agency:** means an employing authority or any other agency of instrumentality of the Crown.
- **Breach:** means an act of breaking or failing to observe a law, agreement, or code of conduct.

- **Compliance activity:** means individual action or system/process implemented to meet compliance requirements.
- **Compliance focus areas:** means annual selection of key compliance areas based on risk and issue assessments which are approved by an appropriate agency governance oversight committee.
- **Compliance obligation:** means a rule, an act or course of actions defined by legislation, framework, standard, etc that the agency must comply with.
- **Control:** means an ongoing, routine, or regular activity that is designed to modify the likelihood of a risk occurring and/or the consequence should the risk materialise.
- **Integrated compliance:** means the structured approach to support the agency meeting compliance requirements. These requirements may include, but are not limited to legislation, regulations, policies, standards, codes of practice, agreements or contractual arrangements, whole of government directives, Premier's Circulars, Ministerial directions and Treasurer's Instructions.
- **Integrated risk management:** means a structured approach that supports the agency to achieve its objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio, integrating with business planning, performance management and assurance activities of the agency.
- **Internal audit:** means an independent objective assurance function that is designed to improve the effectiveness of the agency's operations.
- **Risk:** means the effect of uncertainty on objectives. It can be described as something that may happen in the future that can have a negative or positive impact on performance of the agency.
- **Risk analysis:** means the process to comprehend the nature of risk and to determine the level of risk. It provides the basis for risk evaluation and decisions about risk treatment.
- **Risk appetite:** means the nature and extent of risk the agency is willing to accept or retain to achieve its objectives.
- **Risk assessment:** means the overall process of risk identification, risk analysis and risk evaluation.
- **Risk assessment criteria:** means the terms of reference against which the significance of risk is evaluated.
- **Risk culture:** means an agency's attitudes and behaviours towards risk management.
- **Risk escalation:** means the formal process to communicate a risk to the Chief Executive, Department for Health and Wellbeing.
- **Risk evaluation:** means the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable, in line with the agency's risk appetite and tolerance.
- **Risk management:** means the coordinated activities to direct and control risks.
- **Risk management process:** means systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
- **Statewide services**: means Statewide Clinical Support Services, Prison Health, SA Dental Service, BreastScreen SA and any other state-wide services that fall under the governance of the Local Health Networks.
- **Treatment**: means a further short-term activity designed to modify the likelihood and/or the consequence of a risk. A treatment can include activities to improve an existing control or to develop and implement a new control.

9. Compliance

This policy is binding on those to whom it applies or relates. Implementation at a local level may be subject to audit/assessment. The Domain Custodian must work towards the establishment of systems which demonstrate compliance with this policy, in accordance with the requirements of this policy.

Any instance of non-compliance with this policy must be reported to the Domain Custodian for the Risk, Compliance and Audit Policy Domain.

10. Document ownership

Policy owner: Domain Custodian for the Risk, Compliance and Audit Policy Domain

Title: Risk Management, Integrated Compliance, and Internal Audit Policy

Objective reference number: A5126068

Review date: 30 June 2027

Contact for enquiries and provision of information: health.riskandassuranceservices@sa.gov.au

11. Document history

Version	Date approved	Approved by	Amendment notes
1.0	05/02/2024	Chief Executive, DHW	New policy combining previous System-wide Risk Management Policy, Integrated Compliance Policy, and System-wide Internal Audit Policy
2.0	26/09/2024	Chief Executive, DHW	Revisions to mandatory instruction language and removal of mandatory annual compliance reporting to DHW and requirement for LHNs/SAAS to use the DHW Risk Criteria

12. Appendices

1.Escalation Mandatory Instruction

Appendix 1: Escalation Mandatory Instruction

The following Instruction must be complied with to meet the requirements of this policy.

This mandatory instruction outlines the requirements for SA Health agencies to escalate a risk or compliance/audit finding/s to the Chief Executive, DHW.

1. Escalation of risk by an SA Health agency

- The ownership and management of a risk that has been escalated remains the responsibility of the escalating agency.
- In order to escalate an SA Heath agency risk to the Chief Executive, DHW, the agency Chief Executive Officer must:
    - Provide a written notification to the Chief Executive, DHW and the DHW Risk and Assurance Services unit.
    - The escalation of a risk to DHW must:
        - Provide a description of the risk and any potential system-wide impact/s.
        - Include key controls implemented to manage the risk, an assessment of their effectiveness and any identified control limitations.
        - Include any treatments proposed to create a new, or improve an existing, control.
        - Describe any discussions held with key stakeholders.
        - Provide reason/s for escalation, including specific details of any assistance in the implementation of treatments being requested of DHW and the rationale for such a request.
        - Be endorsed by the agency's Governing Board or Audit and Risk Committee (or equivalent oversight committee) prior to submission.
- DHW Risk and Assurance Services will record the escalation of the risk and ensure the relevant DHW business unit is formally notified of the request.
- The relevant DHW business unit must assess the risk escalation request and brief the Chief Executive, DHW within 30 days advising:
    - That any broader system impacts are noted and referred to HCEC for consideration;
    - If any recommended supporting actions requested will be progressed by DHW; or
    - If no recommended supporting actions are be progressed, the reasons no action will be taken.
- Communication must be sent from the Chief Executive's office to the agency Chief Executive Officer advising of the decision.
- A copy of the briefing and communication to the agency Chief Executive Officer must be provided to DHW Risk and Assurance Services unit for their records.
- To de-escalate a previously escalated risk, the agency Chief Executive Officer must provide a written notification to the Chief Executive, DHW and the DHW Risk and Assurance Services unit notifying them that the risk no longer requires escalation, and an update of the effective or partially effective controls in place.

2. Escalation of compliance or audit report finding by SA Heath agency

- In order to escalate an SA Health agency compliance or audit report finding to the Chief Executive, DHW, the agency Chief Executive Officer must:
    - Provide a written notification to the Chief Executive, DHW and the DHW Risk and Assurance Services unit.
    - The escalation of a finding to DHW must:
        - Provide a copy of the compliance or internal audit report and a description of the finding.
        - Include any proposed actions to remediate the finding.
        - Provide a description of any associated risks to the agency or any potential system-wide impact/s.
        - Provide reason/s for escalation, including specific details any assistance in the implementation of actions being requested of DHW and the rationale for such a request.
        - Be endorsed by the agency's Governing Board or Audit and Risk Committee (or equivalent oversight committee) prior to submission.
- DHW Risk and Assurance Services will record the escalation of the finding and ensure the relevant DHW business unit is formally notified of the request.
- The relevant DHW business unit must assess the finding escalation request and brief the Chief Executive, SA Health within 30 days advising:
    - That any broader system impacts are noted and referred to HCEC for consideration
    - If any recommended supporting actions requested will be progressed by DHW; or
    - If no recommended supporting actions are to be progressed, the reasons no action will be taken.
- Communication must be sent from the Chief Executive's office to the agency Chief Executive Officer advising of the decision.
- A copy of the briefing and communication to the agency Chief Executive Officer must be provided to DHW Risk and Assurance Services unit for their records.
- If DHW is responsible for undertaking actions to remediate, the finding and remediation strategies will be recorded, managed, and followed up by DHW Risk and Assurance Services unit as a part of local Recommendation Improvement Register (RIR) processes. The escalating agency will be kept regularly informed by DHW Risk and Assurance Services unit of the progress of actions taken for their own record.