level higher than a low rating using the Likelihood and Consequence matrix, a treatment plan is required.

The risk appetite for risks related to Human Resources, Organisational and Financial is Moderate. This means for these impact categories if risks are assessed at a controlled level higher than a moderate rating using the Likelihood and Consequence matrix, a treatment plan is required.

If after the assessment of a treatment plan, risks at a treated level remain high or extreme, they should be referred to senior management for consideration.

4.4.6 Risk Treatment

The purpose of risk treatment is to select and implement an action plan to address a risk. Developing a risk treatment is an iterative process of:

- Formulating and selecting treatment options
- Planning and implementing an action plan;
- Assessing the effectiveness of that action plan; and
- Deciding whether the remaining level of risk is acceptable.

Selecting the most appropriate risk treatment option (action plan) involves balancing the potential benefits against the costs, effort or disadvantages of implementation. Options for treating risk may involve one or more of the following options:

- Avoid the risk by deciding not to start or continue with an activity (often not an option for a government department);
- Taking or increasing the risk in order to pursue an opportunity;
- Removing the risk source;
- Changing the likelihood or consequence;
- Sharing the risk (outsourcing, buying insurance); or
- Retaining the risk by informed decision.

The selection of treatment options should be made in accordance with DHS objectives, risk appetite and available resources.

Care needs to be taken when selecting a treatment option as it may produce unintended consequences or expose DHS to other risks. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the treatment becomes and remains effective. The information provided in a treatment plan should include:

- Name of the treatment;
- Details of the proposed action;
- Nominate a person responsible for the treatment – a treatment owner;
- Start and completion dates
- Status reports to ensure follow up.

DHS has decided that:

- Any risk where controls are partially effective or ineffective require a treatment plan.
- Risks that are rated at the controlled level of risk as extreme or high must have the control effectiveness rated as partially effective or ineffective and therefore a treatment plan is required.
- Risks that are rated at the controlled level of risk as either moderate or low can be accepted and monitored, if the control effectiveness has been assessed as effective.

4.4.7 Monitoring and Review

As few risks remain static, they need to be regularly reviewed for currency and accuracy. During the DHS quarterly reporting process, management must review risks within their area and follow up on controls and treatments / action plans that are mitigating the risks. Any action that is out of date and requires further attention can thus be identified. As well, completed treatment could be converted to controls; level of risk confirmed, and risks may be retired or escalated.

Monitoring and reviewing risks, controls and treatments also apply to any actions / treatments from Internal Audit. The audit report provides recommendations that effectively are treatments for controls and risks that have been tested during an internal review.

4.4.8 Recording and Reporting

Risk reporting involves a structured process to record information at each stage of the risk management process. DHS maintains an electronic risk register tool (RiskConsole) which enables monitoring, review and prioritisation of risks. The risk register is based on the Departmental structure and incorporates the DHS strategic objectives.

The currency of the risk register is the responsibility of the Risk Management team which continuously support RAFs through formal training sessions, specific risk assessments, RAF Forums, workshops and as requested by the RAF or senior personnel.

The risk register provides evidence of risks having been systematically identified, analysed and treated on a continual basis by division/business units. Risks may change so the registers should be maintained to accurately record the risk management process, the effectiveness of internal controls and progress of risk treatments.

Reports are submitted on a quarterly basis and are subject to a quality review process before being reported to senior management and the RMAC.

4. Roles and Responsibilities

Role	Authority/Accountability
Chief Executive	• Establishing and maintaining a culture of risk awareness and intelligence; • Development and implementation of a risk management framework specific to the Department's business and needs; • Establishing and maintaining a Risk Management and Audit Committee; • Ensuring governance mechanisms effectively monitor risks and the way they are managed; • Ensuring employees receive support in fulfilling their responsibilities; • Setting standards of best practice for risk management, based on the ISO 31000:2018; and • Contributing to the attainment of whole-of-Government economic, social and environmental objectives in South Australia's Strategic Plan.
Risk Management and Audit Committee	• Assists the Chief Executive in the identification of risks, determining priorities for action, and advise on developing and implementing strategies for effective risk management and ensuring that accountabilities are met; • Provides governance of the risk management function of DHS; • Reviews and monitors the development and implementation of risk management principles across DHS; • Receives quarterly risk management reports.
Executive Director Director/Manager	• Demonstrate a commitment to an integrated risk management system; • Nominate influential and motivated team members to undertake the role of RAF; • Support the RAF's professional development in risk management; • Evaluate risks on a quarterly basis, including relevance of each risk, level of risk, effectiveness of existing controls and treatments and endorse as part of the quarterly reporting process; and • Undertake annual risk reviews as part of business planning process, incorporating fraud risk assessments. • Ensure compliance with the WHS Act 2012 refer DHS Officer responsibilities guide
Risk Management team	• Developing, implementing and monitoring risk management policies and strategies; • Providing expert advice, consultancy and recommendations on risk management; • Reviewing the Department's risk management framework and

	monitoring its implementation; • Implementation of risk management policy and framework; and • Training and support of RAFs and managers.
Key Risk Assessment Facilitators	• Assists with the quarterly requirements at a strategic level; • Supports Executive on nominations for new RAFs; • Encourages and supports other RAFs in learning opportunities.
Risk Assessment Facilitators	• Promote local risk management awareness activities; • Undertake competency-based training and other risk management professional development; • Facilitate quarterly reporting within their area; and • Facilitate annual risk reviews.
Internal Audit	• Providing assurance to the Chief Executive and RMAC regarding the adequacy and effectiveness of risk controls; • Developing and implementing a “risk-based” annual audit plan; • Collaborating with the Risk Management team to ensure risks and controls reviewed during audits are updated on the DHS Risk Register; • Utilising the Risk Register to inform relevant internal audit assignments; and • Promote awareness of the Risk Management Policy and Framework during the course of their reviews.
All Staff	• Employees actively support, report and contribute to the risk management process. Employees also maintain awareness of risks that relate to their work group and discuss risk management with RAFs, Managers and the Risk Management team.

6. Monitor, evaluate and review

See 4.4.8

7. Definitions

Term	Meaning
Control	A measure that maintains or modifies risk. This may come in three types, preventative, mitigating (minimize impact of loss of control) and monitoring (eg audits, inspections, testing)
Control Owners	The owners of a control process that mitigate an identified risk. Where controls are evaluated as partially effective or ‘ineffective, the control owner will participate in developing a treatment to ensure the effectiveness of the control.
Corporate Governance	Set of activities and policies that control the way in which an organization is directed, administered and/or controlled.
Hazard	A reasonably foreseeable source of potential loss of control that

	could cause harm, or damage or disruption.
Incident	An unplanned and unexpected event (including a near miss). A risk made manifest.
Internal and external Context	The environment in which the organisation seeks to achieve its objectives.
Levels or Risk (LoR)	Combination of the likelihood and consequence of the risk, as established during the risk rating stage of the risk assessment and can be determined at either inherent or controlled level.
Inherent LoR	The level of risk before existing controls are considered or if existing controls fail.
Controlled LoR	The current level of risk with controls in place.
Targeted LoR	The projected level of risk whilst treatments are being implemented. The controlled level of risk should be revised as treatments are completed.
Quarterly declarations	Quarterly review of strategic and operational risks with declaration statement attached to maintain a historical record of risk registers by respective divisions/business units that may be subject to future audits.
Resilience	Capacity of an organisation or individual to resist being affected by an event/ incident.
Reasonably Practicable	The term 'reasonably practicable' means whatever is, or was at a particular time, reasonably able to be done in relation to ensuring health or safety
Risk	An incident or event that were it to occur would impact on DHS' capacity to fulfil its objectives'. Under the WHS Act a risk is a hazard that has not been eliminated. The hazard becomes a risk and must be managed to minimize the impact on persons so far as is reasonable practicable
Risk acceptance	Form of risk treatment when there is an informed decision to take a particular risk.
Risk analysis	Process used to understand the nature of risk and to determine the level of risk.
Risk assessment	Process of risk identification, risk analysis and risk evaluation.
Risk appetite	The amount and type of risk that an organisation is prepared to pursue, retain or accept. WHS Act would define this as an ALARP - getting the risk to As Low As Reasonably Practicable
Risk avoidance	Form of risk treatment where there is a decision not to be involved in, or to withdraw from, an activity based on the level of risk.
Risk criteria	Terms or reference against which the significance of a risk is evaluated.
Risk description	A short statement describing a particular risk.

Risk evaluation	Process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable.
Risk financing	Form of risk treatments involving budgetary arrangements to meet the financial costs should a risk occur.
Risk identification	Process of finding, recognising and describing risks.
Risk management	Coordinated activities to direct and control an organisation regarding risk.
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.
Risk management process	Systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk.
Risk mitigation	Measures taken to reduce/treat an undesired consequence.
Risk owner	Person or entity with the accountability and authority for managing the risk and any associated risk treatments.
Risk Profile	One of the four pillars of the Building Safety Excellence in the Public Sector (BSEPS)
Risk register	A documented set of identified risks, controls and treatments (also known as Risk Profile).
Risk retention	Form of risk treatment where there is acceptance of the benefit of gain, or burden of loss, from a particular risk.
Risk sharing	Form of risk treatment involving the agreed distribution of risk with other parties.
Risk source	Anything which alone or in combination has the intrinsic potential to give rise to risk.
Risk tolerance	An individual's or organisation's readiness to bear the risk, after risk treatments, in order to achieve it's objectives.
Risk transfer	Move the liability for the risk to another party or share the risk (contracting, outsourcing, insuring).
Risk treatment / action	Process of selection and implementation of measures to modify the risk.
Stakeholder	Any person or organisation (internal or external) that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Risk Treatment/ Action owners	Treatment owners are responsible for the implementation of treatments. Treatment owners should agree on the treatment design, resourcing and agree timeframes for implementation with directors, risk owners and, possibly, control owners.

8. Reference documents

8.1 Directive documents

ISO31000:2018

The international risk management standard states that the success or risk management will depend on the effectiveness of the risk management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels. The framework:

- Assists in managing risks;
- Ensures the information about risks is accurately reported; and
- Ensures the information is used as a basis for decision making and accountability throughout the organisation.

SA Government Risk Management Policy Statement

The SA Government Risk Management Policy Statement states:

'The South Australian Government recognises that commitment to risk management contributes to sound management practice and increasing community confidence in government performance'.

DHS Risk Management Policy

The DHS Risk Management Policy confirms the Department's commitment to identify, assess and manage risks which may prevent the achievement of strategic goals and objectives.

The Policy directs the Department to integrate risk management into its culture, decision making, programs, practices, business planning and performance reporting and will establish a safe working environment for its staff.

The DHS Risk Management Policy is applicable to the whole of the organisation.

9. Approval

Author: Jim Phillips Principal Risk Management Consultant Quality Assurance, Risk and Business Improvement (QARBI) Phone: 8415 4342 Date: 8/07/ 2019	..... Jonathan Boyd Director QARBI / / 20	..... Daniel Green A/Chief Financial Officer Finance and Business Services / / 20
Comments:	**APPROVED / NOTED** --- **Tony Harrison, Chief Executive** / / 20	

10. Attachment 1 – Risk Categories and Potential Sources of Risk

Best practice in risk identification requires the categorisation of risks. Each risk / opportunity identified will be classified into one of the risk categories that define business activity.

Risk Category	Potential Sources of Risk	
Leadership & Strategic Planning	• Political environment • Leadership and management processes • Government involvement and directions • Ministerial processes • Parliamentary processes and requirements	• Strategic, divisional & business unit planning & reporting • Corporate practices • Protective security • Business continuity and disaster response • Financial requirements and conditions
Knowledge Management / Information Technology	• Procurement • Legal compliance • Protective security	• Records management • Business continuity and disaster response • Advancement in technology
Partnerships / Stakeholder (Working Together)	• Client and stakeholder relationships • Organisational relations (internal & external) • Government collaborations	• Peak bodies and various groups • Communications
Customer Service	• Specific client needs • Promulgation of information to clients	• Evaluation and feedback • Economic value of service
Asset & Facility Management	• Policies & procedures • Legal and financial requirements • Assets, development and maintenance	• Business continuity and disaster response • Protective Security
Legal Compliance	• Legislative requirements • Legal and governance obstructions • Industry regulations and standards	• Legal liabilities • Work Health & Safety • Departmental guidelines
Procurement & Contract Management	• Policies and procedures • Financial management • Contractual agreements • Contract specifications	• External, outsourced functions • Asset management • Resource availability • Transparency & dispute resolution
Human Resource Management	• Managerial responsibilities • Policies & Procedures • Legislative requirement • Recruitment and allocation of resources	• Workforce and succession planning • Staff recognition & dispute resolution • Ethical and Professional conduct
Work Health and Safety	• Governance and legal requirements • Policies and procedures	• Injury management & response • Incident management and documentation
Finance	• Policies and procedures • Financial management	• Legislative & industry requirements • Legal costs
Project Management	• Project Management Framework compliance • Project Management Office requirements	• Skilled resources
Clinical	• Policies & procedures • Safety & quality • Direct client care • Informed consent • Adverse events	• Privacy & confidentiality • Resource allocation • Training & credentialing of clinicians /practitioners • Documentation
Fraud & Corruption	• Policies & procedures • Control breakdown • Protective security	• Procurement & contract management • Illegal activity

11. Attachment 2 – Risk Management Escalation Flowchart