Policy Name	Risk Management Policy Framework
Policy Type	Human Resources
Policy Number	HR19
Version	2
Approval Date	January 2019
Renewal Date	January 2022

WEST DALY
Regional Council

Policy Number	**HR19**
Policy Name	**Risk Management Policy Framework**

SUMMARY

The following policy and associated appendices provide an overview and broad framework for the management of risk at West Daly Regional Council (WDRC).

Risk arises in all aspects of WDRC's operations and at all stages within the cycles of those operations. It offers both opportunities and threats and must therefore be managed appropriately. Risk management involves establishing appropriate risk management practices and culture, and applying logical and systematic risk management processes to all stages in the life cycle of any activity, function or operation. By minimising possible losses and maximising potential opportunities, risk management enables WDRC to best meet its overall objectives, as set out in Council's Regional Plan.

This policy confirms WDRC's commitment to a strategic and structured approach to risk management in order to achieve an appropriate balance between opportunities, losses, efficiencies and effectiveness.

Specifically:

- This policy provides instructions to staff for the implementation of consistent risk management practices throughout Council's offices and operations.
- Council's risk management process is cyclical and will link to Council's corporate planning cycles.
- Risk management is a tool which identifies strategic and operational threats to corporate objectives and enables the development of strategies to mitigate adverse consequences.
- This policy contains the requirements for establishing and maintaining the Risk Management Framework for Council.
- This policy sets a common approach and outlines the responsibilities of staff to systematically manage risk consistent with Australian Standard on Risk Management (AS/NZS ISO 31000:2009).

1.1 Scope

This policy applies to all staff, elected members and the Audit and Risk Management Committee of West Daly Regional Council.

1.2 Policy Objectives

The objectives of this policy are:

- To establish a risk management framework to assist in the effective discharge of WDRC's stewardship and leadership responsibilities, to strengthen WDRC's control environment including the control of its resources in accordance with its legislative responsibilities.

- To outline WDRC's commitment to an open and accountable system of governance and the embedding of continuous improvement processes across WDRC to support achievement of its strategic and operational objectives. The implementation of an effective risk management framework is fundamental to these principles.

- To provide an umbrella framework to enable the consistent and consolidated management of all of WDRC's risk management obligations.

2. DEFINITIONS

2.1 Definitions (ISO 31000)

- **Risk:** the effect of uncertainty on objectives.

- **Risk owner:** the person or entity with the accountability and authority to manage a risk (i.e. is responsible for managing the identified risk including implementing and monitoring the effectiveness of mitigation strategies, and reporting as needed on the status of the risk to the Corporate Governance section).

- **Risk analysis:** process to comprehend the nature of risk and to determine the level of risk.

- **Risk treatment:** process to modify risk (Note: risk treatments that deal with negative consequences are sometimes referred to as risk mitigation strategies, risk elimination strategies, risk reduction strategies, risk prevention strategies and/or risk control).

- **Likelihood:** chance of something happening.

- **Consequence:** outcome of an event affecting objectives.

- **Inherent risk:** a subjective measure of the level of a risk without considering the effectiveness of controls.

- **Residual risk:** a subjective measure of the risk remaining after risk treatment.

3. ROLES AND RESPONSIBILITIES

3.1 Overview of Responsibilities within Risk Management

WDRC's Risk Management Approach is based on a three lines of Defence model (as illustrated in Figure 1 below) to demonstrate and structure roles, responsibilities, linkages and accountabilities for decision making, risk and control purposes to achieve effective governance and assurance. Each line of Defence provides higher levels of independence and objectivity, thereby delivering greater assurance to key stakeholders.

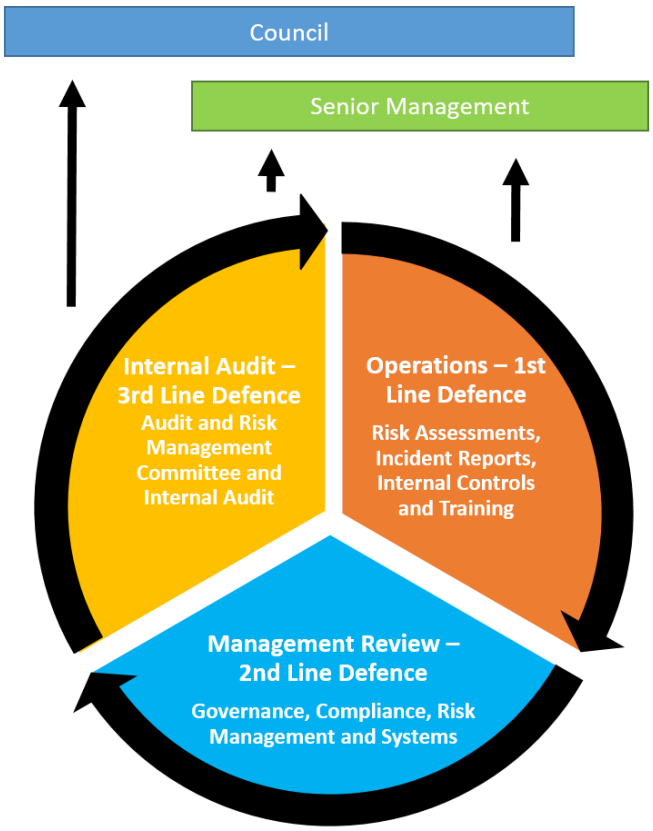
1) First line of defence is 'Operations' - line management is responsible for operationalising risk management and internal controls and implementing business improvement

reviews and outcomes.

2) Second line of defence is ‘Management Review‘ - senior management are responsible for establishing and monitoring WDRC’s policies and standards.

3) Third line of defence is 'Internal Audit' - internal audit and assurance mechanisms are responsible for providing independent and objective assurance and advice on governance, risk and compliance matters and includes Internal Audit, Audit and Risk Management Committee and Council.

Figure 1. WDRC Risk Management Approach



*Adapted from The Institute of Internal Auditors: The Three Lines Of Defence In Effective Risk Management And Control.

3.2 First Line of Defence - Operations

As the first line of defence, operational managers have ownership, responsibility and accountability for directly assessing, controlling and mitigating risks. This includes responsibility for implementing corrective actions to address process and control deficiencies.

Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives. Through a cascading responsibility structure, managers and supervisors design and implement detailed procedures that serve as controls and supervise execution of those procedures by their employees.

Operational management naturally serves as the first line of defence because controls are designed into systems and processes under their guidance of operational management. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events.

3.3 Second Line of Defence - Management Review

Senior management establishes various risk management functions to help build and/or monitor the first line of defence controls. The functions in this second line of defence include:

- Risk management that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout WDRC.
- Monitoring of various specific types of risk such as work health and safety or quality monitoring.
- Providing risk management frameworks that assist in identifying known and emerging issues, shifts in WDRC's implicit risk appetite.
- The development of processes and controls to manage risks and issues.

Senior management establishes these functions to ensure the first line of defence is properly designed, in place, and operating as intended. Each of these functions has some degree of independence from the first line of defence, but they are by nature management functions. The second line of defence serves a vital purpose but cannot offer truly independent analyses to governing bodies regarding risk management and internal controls.

3.4 Third Line of Defence - Internal Audit

3.4.1 Internal Audit

WDRC is committed to maintaining an efficient, effective and economical internal audit function as required by the *Local Government Act*, and will ensure that all internal audit activities remain free of influence by organisational elements.

Internal Audit's role may include, but is not limited to, the review of WDRC risk, internal controls, efficiency, effectiveness, governance, performance and compliance matters including work health and safety.

The primary purpose of Internal Audit is to add value to WDRC's operations by providing an independent appraisal and advisory function for Council, the Audit and Risk Management Committee and senior management thereby assisting Council in realising its objectives. This is achieved by examining and evaluating the adequacy, effectiveness and efficiency of risk management, systems of internal controls and the quality of management systems in an independent and professional manner.

A review or appraisal by Internal Audit does not in any way relieve WDRC staff of their individual

responsibilities and accountabilities. Nor does it any way diminish the responsibilities of Council and senior management for the implementation and maintenance of effective systems of internal controls and prevention and detection of fraud.

3.4.2 Audit and Risk Management Committee

WDRC is committed to maintaining an Audit and Risk Management Committee in accordance with the *Local Government Act* and the Local Government (Accounting) Regulations.

The primary functions of the Audit and Risk Management Committee are to:

a) Monitor strategic and operational risk management and the adequacy of the internal control policies, practices and procedures established to manage identified risk.

b) Oversee the internal audit function including development of audit programs with reference to the Council's risk assessment, the conduct of internal audits by appropriately qualified personnel, the monitoring of audit outcomes and the implementation of recommendations.

c) Review quality of annual financial statements and other public accountability documents (such as annual reports) prior to their adoption by the Council.

d) Review management's responses to external audit recommendations and monitor implementation of the agreed recommendations.

e) Meet with the external and relevant internal auditors at least once each year to receive direct feedback about any key risk and compliance issues, and to provide feedback about the auditor's performance.

f) Advise the Council about the appointment of external auditors.

g) Assess the adequacy of audit scope and coverage.

4. POLICY STATEMENT

Council will work within its Risk Management Framework to minimise the effect of uncertainty on its corporate and business objectives. Risk is inherent in all its activities. The management of risk is good business practice, creates value, is integral to sound corporate governance and in some instances, a mandatory legal requirement. Effective risk management can lead to better decision making and planning as well as better identification of opportunities and threats.

4.1 Risk Appetite

Council's risk appetite is articulated through its descriptions of consequence and likelihood, its matrix for rating risk and its risk registers.

4.2 Risk Management

Risk Management is a structured, consistent and continuous process used across Council at the executive level and the operational level. It is used for identifying, assessing, deciding on, responding to and reporting on opportunities and threats that affect the achievement of the Council's corporate and business objectives.

Strategic Level

Council must identify key strategic risks through strategic risk assessment. These strategic risks provide a framework for identifying other risks, i.e. risks at all levels and activities of Council that should be linked to, or cascade from, the strategic risks. This is consistent with Council's Risk Management approach, which is structured to ensure that all risks in Council, particularly those ranked as high or above, are

identified and effectively managed.

This level relates to the strategic risks associated with Council carrying out its business objectives as articulated in Council's Regional Plan. The high level risks are recorded in the **Strategic Risk Register**. These strategic risks provide a framework for identifying risks at a functional and work group level, for cascading down to operational risks at all levels of Council.

The rationale used for the identification of strategic risks is three-fold:

i. first, the risks have been identified as 'strategic' because if Council does not manage them it will not achieve its corporate objectives;

ii. second, some of the identified risks are global and apply to different degrees, to all parts of Council; and

iii. third, some of the risks are of such a magnitude that not managing them effectively could impact on the operations of several areas of Council.

Operational Level

This level relates to the management of risks associated with work areas meeting their objectives. It includes major operational projects and contracts that may cross over different work groups. These risks are identified, documented and managed through each work area's **Operational Risk Register**.

4.3 Reporting

Strategic and Operational risk registers, including progress of mitigation strategies, will be assessed and reported against to the Audit and Risk Management Committee.

4.4 Monitoring and Review

Council's risk management framework will be reviewed on an annual basis as part of the continual improvement process set out in AS/NZS ISO 31000.

4.5 Documentation, Communication and Evaluation

Documentation of each step of the risk management process must be undertaken. Appropriate documentation demonstrates accountability and provides a record against which it can be determined that the process has been carried out correctly and enables decisions and/or processes to be reviewed.

4.6 Linkages

The outcomes and outputs of the risk management processes will form inputs to Council's internal audit, compliance and assurance activities and vice versa.

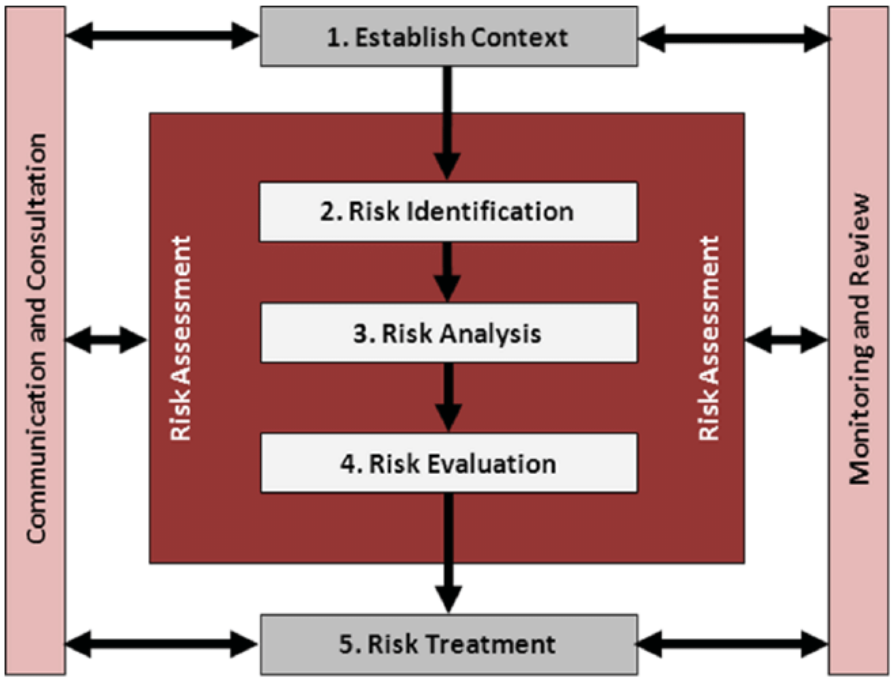
4.7 Risk Management Integration

The approach to managing risk is to be included in Council's planning processes, decision-making structures and operational procedures.

5. USING THE RISK MANAGEMENT FRAMEWORK

The steps outlined below are based on the Australian/New Zealand ISO Standard - Risk Management AS/NZ ISO 31000:2009 (See Figure 2). Work areas are to follow this process in completing the Operational Risk Register, and the same process can also be applied for projects and contracts.

Figure 2: The Risk Management Process (AS/NZS/ISO 31000:2009)



5.1 Stage 1: Establish the Context

i. This step involves establishing the context in which the rest of the process will take place. The objectives, strategies and scope of the activity, or part of Council to which the risk management process is being applied, should be established.

ii. A key step in Council's risk process is the need to identify and evaluate risks in relation to how they affect Council's ability to deliver the strategies identified in Council's Regional Plan.

5.2 Stage 2: Identify Risks and Risk Owner

i. This step seeks to identify the risks that need to be managed. The aim is to generate a list of risks that might have an impact on the achievement of work group outcomes. These risks might prevent, degrade, delay or enhance the achievement of those objectives.

ii. It is intended that risks are identified and measured using data where it is available. Only when objective data is not available are judgements based on experience and existing risk registers allowed.

iii. Descriptions of identified risks consider source and impact, what the risk is, whom it impacts upon and what the impact is.

iv. Identifying the risk and risk owner involves the following steps:

- describe the nature of the risk (Risk Description);
- link the risk to the most relevant strategic risk (Risk Number);

- allocate a risk number (Risk Number);
- identify a risk owner (Risk Owner);
- identify the causes of the risk (Risk Factors/Cause); and
- provide a brief description of the impact/consequence of the risk (Risk Effect). In assessing the impact/consequences, consideration may be given to a range of issues including business management, political, commercial and legal, finance and human resources.

5.3 Stage 3: Analyse Risks

Analysing risks involves the following steps to determine the inherent risk rating and residual risk rating.

Inherent Risk Rating

i Rate the consequence of the risk should it occur, and the likelihood of the risk occurring using the descriptors provided in Tables 1 and 2 below. To determine the inherent risk rating, it is important that the consequence and likelihood of each risk is rated without considering the existing controls and mitigation strategies. This produces a score that indicates worse-case exposure in the event that there are no controls in place, or the controls fail to take effect during a risk event.

ii Now consider the matrix for assessing risks (see Tables 2 and 3 below). Using this matrix, identify the risk rating as Critical, High, Medium or Low.

Residual Risk Rating

i. Consider what is currently being done to mitigate/manage the risk, i.e. what controls are in place? Are there already some mitigation strategies in place to manage the risk? Briefly list the controls and mitigation strategies.

ii. Rate the consequence of the risk should it occur, and the likelihood of the risk occurring using the descriptors provided in Tables 1 and 2 below.

iii. It is important that the consequence and likelihood of each risk is rated in the context of existing controls and mitigation strategies.

iv. Now consider the matrix for assessing risks (see Tables 2 and 3 below). Using this matrix, identify the risk rating as Critical, High, Medium or Low.

Table 1 - Consequence of Risk

In rating the consequence of the risk occurring, the table below also provides some further qualitative descriptors of consequence to be considered when determining which consequence is the most appropriate.

Level	Strategic Delivery	Service Delivery	Human Resources	Finance and Legal	Reputation/ Stakeholder
5.Catastrophic	Community outrage; Major adverse quality problem; Major milestone missed by > 1 year.	Complete and indefinite disruption to services >6 months; Intervention by Minister.	A large number of key employees or directors leave; Death or significant permanent disability to one or more persons.	Large scale class action; Material breach of legislation with very significant financial or reputational consequences; Direct loss >$lm.	Extended Territory wide adverse media coverage; Intervention by Minister.
4.Major	Failure to achieve some performance targets; Major milestone missed by 6 -12 months.	Long term disruption to services with extended resources required to remedy >1 to <6 months.	Some key employees leave; High staff turnover; Poor reputation as an employer; Hospital admission (inpatient); Minor or reversible disability.	Regulatory breach with material consequences but which cannot be readily rectified; Direct loss of $250,000 to $1 million.	Ongoing local, or Territory- wide adverse media coverage.
3.Moderate	Some reduction in performance; Major milestone or deadline missed by 1 - 6 months.	Service restored within expected timeframes <1 week.	Some short term staff morale problems; First aid administered by Site First Aid Officer or possible professional medical treatment required resulting in lost time through injury.	Regulatory breach with minimal consequences but which cannot be readily rectified; Direct loss of $50,000 to $250,000.	Individual complaints; Local temporary adverse media.
2.Minor	Milestone missed by <1 month.	Issues rectified with corrective action.	First aid not required, no lost time or medical expenses.	Direct loss of $0 to $50,000.	Individual complaints Immediately addressed.
1.Insignificant	Negligible performance reduction.	No loss of service.	Routine HR issues.	Regulatory breach with minimal consequences and readily rectified.	Negligible activity.

Table 2 - Risk Assessment Matrix - inc Likelihood of Risk

Likelihood		Consequence				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5	Almost certain to occur in most circumstances	Medium	High	Critical	Critical	Critical
4	Likely to occur frequently	Low	Medium	High	Critical	Critical
3	Possible and likely to occur at sometime	Low	Low	Medium	High	Critical
2	Unlikely to occur but could happen	Low	Low	Low	Medium	High
1	May occur but only in rare and exceptional circumstances	Low	Low	Low	Low	Medium

Table 3 – Overall Risk Assessment

Critical = a score of 8-10

High = a score of 7

Medium = a score of 6

Low = a score of 2-5

6	7	8	9	10
5	6	7	8	9
4	5	6	7	8
3	4	5	6	7
2	3	4	5	6

5.4 Stage 4: Evaluate and Treat Risks

Based on the analysis of the risks, it is necessary to decide whether any further actions are necessary and appropriate to further mitigate the risk. This will require consideration of the following:

i Can additional controls and/or mitigation strategies be identified that can help with better management of the risk? If that is the case, provide a brief description. Note: A key priority for identifying additional controls and mitigation strategies should be reducing the likelihood and/or consequences of each *'Critical'* or *'High'* risk. For other lower ranked risks the option may be simply ongoing monitoring and reporting on the status of the risk. The selected option should be the most appropriate and practicable, with the objective of reducing the level of risk to a tolerable level.

ii Options may include the following:

- *Likelihood Reduction* - eliminating sources of risk or substantially reducing the likelihood of their occurrence.
- *Risk Avoidance* - a particular case of likelihood reduction, where undesired events are avoided by undertaking a different course of action.
- *Impact Mitigation* - minimising the consequences of the risk.
- *Risk Transfer* - shifting responsibility of the risk to another party (also called *risk sharing* because risks can rarely be transferred or shed entirely).

iii On the other hand there may be sufficient controls and mitigation strategies in place. For instance it may be impractical and/or inappropriate to consider further controls to mitigate the risk. If this is the case, place *No further action* in the Mitigation Strategy column. This option is referred to as *risk retention,* i.e. risks cannot be further reduced or avoided, or the costs of doing so would be too high. Risks can also be regarded as opportunities if they are retained and dealt with appropriately.

iv Finally, consider whether it would be beneficial to include this area of risk on Council's internal audit program. For example, an audit of the area may provide confidence that the controls and mitigation strategies in place are working adequately; an audit may also help by suggesting additional controls and mitigation actions that may not have been considered. By giving the Audit function consideration, it will assist Governance and the Audit Committee in developing the Internal Audit Plan for the Council. The Audit Committee will consider recommendations; however its decision to include/exclude certain areas from the program will be guided by a number of other priorities as well.

Table 4 - Risk Treatment Summary

RISK TREATMENT

Level of Risk	Response
Critical Risk	Must be managed by senior management with a detailed plan
High Risk	Detailed research and management planning required at senior levels - management responsibility must be specified
Medium Risk	Manage by specific monitoring or response procedures
Low Risk	Manage by routine procedures - unlikely to need specific application of resources

5.5 Stage 5: Monitor and Review

i Governance will meet with the Audit Committee regularly. This allows Council to assess the effectiveness of the risk management process on an ongoing basis. It also allows for a thorough review of the risk register and, in particular assists in identifying and monitoring risks of a cross- divisional nature. The identified risks and the effectiveness of mitigation strategies will be reviewed to reflect changing circumstances and priorities.

ii A report will be prepared on the progress in achieving risk treatment objectives for presentation to the Audit Committee twice a year.

5.6 Stage 6: Communicate and Consult

The premise underlying this Policy is that Council will consistently consult and communicate with stakeholders and all relevant parties involved. This is to be undertaken at all times in a fair, timely and transparent manner.

6. COMPLIANCE AND CONTINUOUS IMPROVEMENT

6.1 The steps outlined below are based on the Australian/New Zealand Standard - Risk Management AS/NZ ISO 31000:2009 (See Figure 3).

6.2 Council will ensure that its processes follow the requirements of ISO 31000:2009 as follows:

i. mandate and commitment is evidenced by this policy;

ii. the framework and implementation processes are as described in this policy;

iii. monitoring and reviewing of this policy will be undertaken annually; and

iv. annual reviews will evidence continual improvement.

Figure 3: The Risk Management Framework (AS/NZS/ISO 31000:2009)

7. REVIEW

This Policy and the attached Audit and Risk Management Committee Terms of Reference will be reviewed by the Committee every two years or as deemed necessary by either Council or the Chief Executive Officer. All amendments to this Policy, and Terms of Reference require the Audit and Risk Management Committee's endorsement, prior to submission to Council for discussion and approval.

TERMINOLOGY AND REFERENCES

REFERENCES

Audit and Risk Management Committee Terms of Reference

Risk Register Template

Internal Audit Plan

FURTHER INFORMATION:

Chief Executive Officer