Enterprise Risk Management Standard

1. Brief description

This Standard is designed to ensure a consistent understanding and application of Risk Management at Western Power, and to support the identification and management of Risk on an ongoing basis within the Risk Appetite set by the Board.

1.1 Related Documents

This Standard is made under and supports the Assurance and Risk Policy.

Figure 1: Assurance and Risk suite document hierarchy

1.2 Scope

This Standard applies to all Western Power Personnel. For the purposes of this Standard, Personnel means:

(i) every employee, officer and director of Western Power; and

(ii) every contractor of Western Power when performing activities on behalf of Western Power.

1.3 Objectives

This Standard provides an overview of the Enterprise Risk Management (**ERM**) Processes to be applied by all Personnel across Western Power in order to ensure that Risk Management is adequately integrated and appropriately undertaken throughout the organisation. Further, this Standard is intended to:

(i) provide the mechanism for a truly integrated Risk Management approach for all Western Power Personnel, where Risk Management is incorporated into relevant organisational processes and Risk information is used as a key input to inform decision making

(ii) provide the Board, Executive Management, leadership groups and wider stakeholders with confidence that appropriate processes are in place to enable Strategic, Functional, Operational and Project Risks to be effectively managed throughout Western Power

(iii) encourage a "Risk-aware" culture that promotes the recognition and management of Risk, allowing for innovation and responsible Risk-taking while ensuring appropriate measures are taken to protect the organisation (i.e. mitigate against intolerable risk exposure)

(iv) define the approach and key roles and responsibilities for managing Risk across the organisation.

1.4 Principles

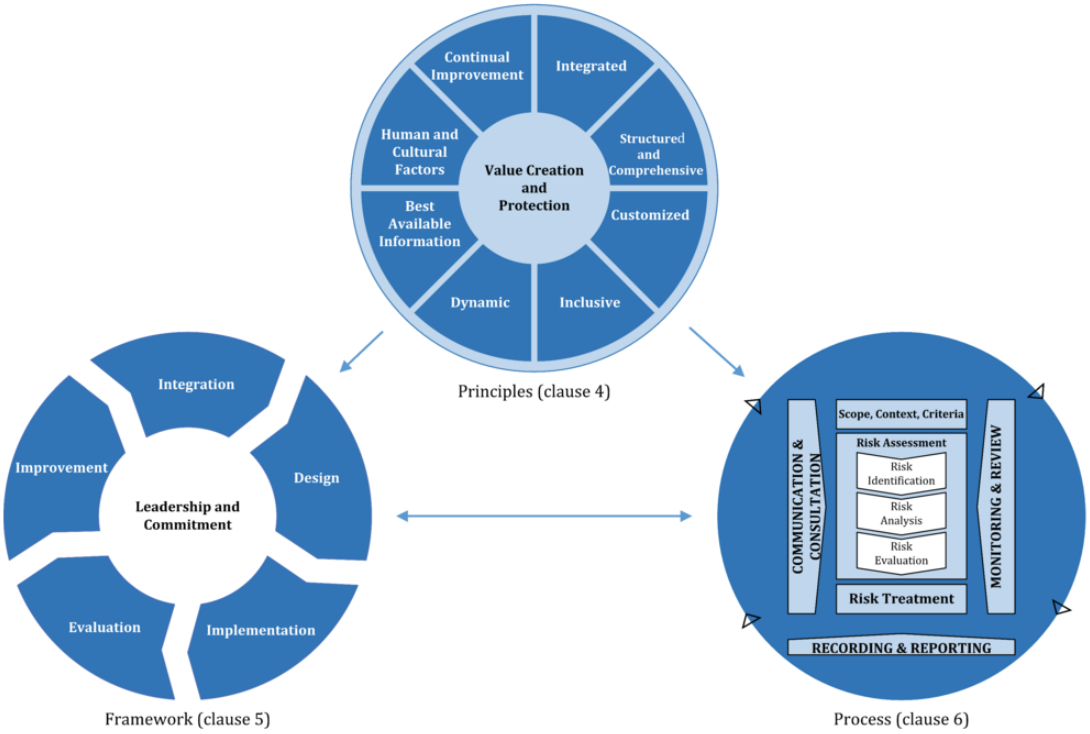
Risk is the effect of uncertainty on objectives[1]. It is an uncertain event or condition that, if it occurs, will affect Western Power's ability to successfully execute and achieve its strategic, functional and/or operational objectives.

Risk Management refers to the activities undertaken to control and direct an organisation's processes, systems and culture towards the effective management of Risk.

Western Power provides a structured, uniform and systematic approach to managing Risk through the application of the Risk Management principles, framework and processes found within *ISO 31000:2018 Risk Management – Principles and Guidelines* (**ISO 31000**), as depicted in Figure 2 below.

In managing Risk, Western Power endeavours to ensure that all Risks are managed within Risk Appetite set by the Board, and are managed to a reasonable and tolerable level, with Safety risks being managed to As Low As Reasonably Practicable (ALARP).

Figure 2: Risk Management principles, framework and processes



At Western Power, Risk Management is intended to create and protect enterprise value by being:

[1] As defined within ISO 31000:2018 Risk Management - Guidelines

(i) integrated into organisational processes and decision making

(ii) structured, timely and comprehensive

(iii) customised to suit the business context

(iv) transparent and inclusive

(v) dynamic, iterative and responsive to change

(vi) based on best available information

(vii) aware of human and cultural factors

(viii) focused on continual improvement.

2. Risk Appetite

The Board sets the nature and extent of the Risk Western Power may take in carrying out its operations and achieving its strategic objectives. This risk appetite is articulated by the Board through a:

(i) Risk vision

(ii) Risk Appetite Statement

(iii) Enterprise Risk Assessment Criteria.

2.1 Risk vision

Western Power has a Board approved Risk Vision Statement (EDM #43397084), which articulates the organisation's risk management goals and risk management objectives.

2.2 Risk Appetite Statement

Western Power has a Board-approved Risk Appetite Statement (EDM #43397084), which articulates what Risks the organisation are and are not willing to accept in pursuit of its strategic objectives.

2.3 Enterprise Risk Assessment Criteria

Western Power's Risk Appetite is also embodied through the Enterprise Risk Assessment Criteria (EDM #34037272) approved by the Board. It is applied across all Strategic, Functional and Operational Risk assessments. These provide terms of reference by which the significance of Risk is evaluated.

3. Integrated Risk Management

It is essential that Risk Management is integrated within existing business processes for it to be effective and to support its ongoing benefit to the organisation. Effectively integrated Risk Management enhances an organisation's ability to:

(i) consider efficacy / cost of Controls

(ii) understand the interrelated impacts of Risk across the organisation

(iii) effectively assess and allocate resources for the management of Risk.

In committing to make Risk Management an activity that is straightforward, value adding and that forms a part of "the way we do things around here", the requirements of this Standard have been integrated with a number of existing business processes, including:

(i) business continuity, crisis management and emergency management

(ii) compliance management

(iii) work health and safety and environmental management

(iv) investment decision making

(v) project management

(vi) contract management

(vii) asset management

(viii) protective security – cyber, physical, personnel and information

(ix) strategic planning

(x) function planning.

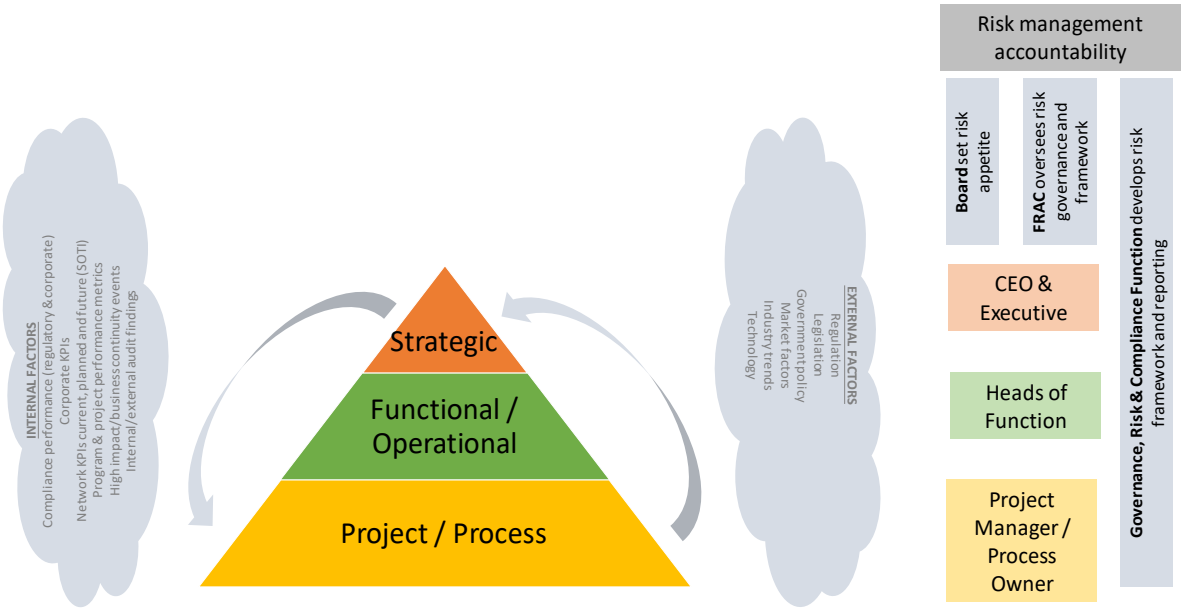
4. Enterprise Risk Management Processes

A suite of ERM Processes exists to support the implementation of this Standard. In enabling this process, Risk Systems are available at each level (strategic, functional, operational and project) to facilitate the identification, analysis, evaluation, treatment, monitoring, reviewing and reporting of Risks in a consistent manner across the organisation (see Figure 2 above). The following sections (including Figure 3 below) provide an overview of these processes.

For more detailed guidance on ERM processes, refer to the Enterprise Risk Management Guideline (EDM #41492839).

In addition to the general concepts surrounding ERM processes, the Enterprise Risk Management Guideline, along with the Assurance Standard (EDM #54729231), provides further requirements surrounding the identification and management of Critical Risks (which have an Inherent Consequence risk rating of catastrophic) and Critical Controls.

Figure 3: Enterprise Risk Management Hierarchy (on-a-page)



4.1 Strategic Risk Management Process

Consistent with the ERM process described above, Western Power's Strategic Risk Management Process involves the identification, analysis, evaluation, treatment, monitoring, reviewing and reporting of Risks that can impact on the achievement of strategic objectives or affect its long-term position and performance. Detailed guidance on ERM processes (which applies to Strategic Risks) are found within the Enterprise Risk Management Guideline.

The process of setting Western Power's Strategic Risks is accomplished by the Board and Executive Management undertaking facilitated workshops where existing Strategic Risks are reviewed, new / emerging Risks are identified, and accountabilities allocated for management action. These workshops are held concurrent with, and as part of, the broader strategic review of the business.

External parties may be involved in these workshops to provide wider perspectives on Risk issues. The workshops are informed using Risk System information, key performance metrics, assurance reports (e.g. internal audits, external reviews) and surveys on emerging external factors such as political, economic, societal, technological, market and environmental drivers.

Strategic Risks are recorded in a Strategic Risk System and reviewed quarterly for changes in the internal or external factors surrounding the risk, with reporting to the Finance, Risk Audit Committee (**FRAC**). On a quarterly basis a deep dive on a strategic risk is held with the FRAC, with the schedule of deep dives determined by the FRAC. On an annual basis a detailed review of the Strategic Risks is held with the Board and/or Executive to ensure ongoing currency and relevance.

4.2 Functional Risk Management Process

Western Power's Functional Risk Management Process involves the identification, analysis, evaluation, treatment, monitoring, reviewing and reporting of Risks that can impact on the achievement of functional objectives developed as part of the annual function planning process. Detailed guidance on ERM processes (which applies to Functional Risks) are found within the Enterprise Risk Management Guideline.

These Risks are owned by the relevant Head of Functions (i.e. Risk Owners) who are accountable and responsible for ensuring identified risks are appropriately managed. Responsibilities may be formally delegated to appointed personnel where appropriate.

Functional Risks are recorded within Functional Risk Systems and reviewed on a quarterly basis (at a minimum). Outside of this quarterly process, existing and emerging Risks should be monitored on an ongoing basis and where required, Functional Risk Systems should be updated to reflect any changes.

Functional Risks are assessed using the Enterprise Risk Assessment Criteria.

4.3 Operational Risk Management Process

Western Power's Operational Risk Management Process involves the identification, analysis, evaluation, treatment, monitoring, reviewing and reporting of Risks that can impact on the achievement of operational objectives. Operational Risks may be specific to a function, or cross-functional, and are owned by the relevant member of the management team (i.e. Risk Owners) such as the Head of Function, Area Manager or Team Leader. Detailed guidance on ERM processes (which applies to Operational Risks) are found within the Enterprise Risk Management Guideline.

Operational Risks are identified on an ongoing basis with all Western Power personnel being responsible for the identification and escalation of Risks as part of performing day to day operations and decision making. These Risks are recorded within Operational Risk Systems and reviewed on a frequency determined by the Risk Owner (at least annually).

Operational Risks are assessed using the Enterprise Risk Assessment Criteria. However, within certain Risk Contexts, an adapted version of the Enterprise Risk Assessment Criteria that is more fit-for-purpose may be used, but still align with the Enterprise Risk Assessment Criteria. Examples of such Risk Contexts include:

4.3.1 Network Risk Management

Network Risks relate to gaps existing (or forecast to exist) between the condition or performance of the network and Western Power's network objectives as defined in the Network Investment Strategy. These Risks arise through Western Power's stewardship of the network and the provision of covered services, including the application of statutory obligations.

Given the specific Risk Contexts surrounding such Risks, an adapted version of the Enterprise Risk Assessment Criteria with tailored Consequence Measures may be used.

Network Risks are routinely reviewed for changes, and formally refreshed / updated at a minimum on an annual basis, although this can occur more frequently on an ad-hoc basis if required.

4.3.2 Occupational, Health & Safety Risk Management

Occupational, Health & Safety Risk Management relates to the need to eliminate Risks to health and safety or, if elimination is not reasonably practicable, minimise so far as is reasonably practicable, as required under Health and Safety laws.

Occupational, Health & Safety Risks are to be assessed using the Enterprise Risk Assessment Criteria.

4.3.3 Cyber Risk Management

To promote consistency in the manner cyber risks are identified and evaluated, a *Cyber Threat, Vulnerability and Risk Guideline* (EDM #50791013) has been developed, with risk assessment criteria specific to Cyber Security. The Guideline describes the process for identifying cyber risks, the stages at which cyber risks require Treatment, and how the cyber risks should be managed, reported and monitored. It also describes how external Threats and Vulnerabilities associated with Cyber Security should be managed.

4.4 Project Risk Management Process

Western Power's Project Risk Management Process involves the identification, analysis, evaluation, treatment, monitoring, reviewing and reporting of Risks that can impact on the achievement of project objectives. These should consider the context of Risks to the achievement of expected business value / benefit, and not just be restricted to delivering on cost, quality, scope and schedule.

Project Risks tend to be more dynamic in nature (i.e. subject to constant changes) than other Risk types, have a limited planning period and generally only exist during the project lifecycle. This is due to projects having an agreed start and end date and not business as usual activities. Project Risks are owned by the relevant Project Manager and should be documented within a project specific Risk System or equivalent. Project Risks should be reviewed (e.g. via a project risk workshop) and updated at every relevant "gate" of the project's lifecycle.

Given the specific Risk Contexts surrounding project Risks, an adapted version of the Enterprise Risk Assessment Criteria with tailored Consequence and Likelihood measures has been developed and can be found within the Delivery Risk Management Guideline (EDM #43041786).

5. Roles and responsibilities

All Western Power Personnel are responsible for the identification and management of Risks across the organisation, however, the overarching responsibility for ensuring that Risk Management is integrated into all aspects of Western Power's organisational activities sits with the Board and Executive Management.

The following sections provide additional details on specific roles and responsibilities across three areas:

(i) Organisational (see section 5.1)

(ii) Enterprise Risk & Resilience Area (see section 5.2)

(iii) Risk-specific (see section 5.3)

5.1 Organisational roles and responsibilities

5.1.1 Board

The Board is responsible for:

(i) defining Western Power's Risk Appetite

(ii) identifying, reviewing and monitoring Western Power's Strategic Risks

(iii) overseeing the Finance, Risk and Audit Committee with regards to Risk Management

(iv) integrating Risk Management into the organisation's governance, activities and decision making.

5.1.2 Finance, Risk and Audit Committee (FRAC)

The FRAC is responsible for:

(i) reviewing the adequacy and robustness of implemented Risk Management Processes, including the manner in which risks are to be identified, managed and reported

(ii) ensuring that key Risk Profiles, material changes to the profiles, trends, emerging Risks, and the Risk Management programme are reported at least annually to the Board

(iii) review reports from the Auditor General and Internal Audit on:

- the effectiveness of the internal controls, compliance and risk management systems
- any changes to Critical Risks faced by Western Power.

5.1.3 Executive Managers

The Executive Managers are responsible for:

(i) providing leadership and direction through the continuous reinforcement of the vision for, and the organisation's commitment to Risk Management

(ii) ensuring Risks taken in the achievement of business objectives are within the Risk Appetite set by the Board

(iii) identifying and reporting Risks to the Board that may exceed the Risk Appetite

(iv) actively supporting the Risk Management Process and championing appropriate Risk Management practices across the organisation

(v) identifying, evaluating, monitoring and taking ownership of Western Power's Strategic Risks, including the escalation of any new and emerging Risks identified at the strategic level

(vi) ensuring that Critical Risks are appropriately identified and managed in accordance with the Assurance Standard

(vii) identifying and directing implementation of Strategic Risk Treatments to avoid any duplication, inefficiencies or potential inconsistencies that could otherwise exist between similar Functional or Operational Risk Treatments

(viii) asking challenging questions of the business in relation to current Risk exposure, including the Treatments that are being implemented to manage the exposure

(ix) integrating Risk Management into the organisation's governance, activities and decision making

(x) overseeing the adequacy and capability of resources available to execute and implement required Risk Treatments.

5.1.4 Heads of Functions

The Heads of Functions (HoFs) are responsible for:

(i) ensuring Risks taken in the achievement of their functional and operational objectives are within the Risk Appetite set by the Board

(ii) actively supporting the Risk Management Process and championing appropriate Risk Management practices across the organisation

(iii) identifying and reporting Functional and Operational Risks to Executive Managers and the Enterprise Risk & Resilience Area that may exceed the Risk Appetite, or where significant changes to the Risk Profiles of these risks are identified

Note: Where such activities have been delegated, ensuring appropriate team members are available to undertake required responsibilities

(iv) ensuring adequate Controls and Treatments for managing Strategic, Functional and Operational Risks are in place and monitored for continued operating effectiveness

(v) ensuring that Risks, Controls and Treatments are captured within relevant Risk Systems in a manner that is accurate, consistent and timely.

(vi) ensuring that Critical Risks are appropriately identified and managed in accordance with the Assurance Standard

(vii) incorporating any initiatives and Treatments associated with Functional and Operational Risks within their respective function plans

(viii) ensuring the adequacy and capability of resources available to execute and implement required Risk Treatments

(ix) consulting the Enterprise Risk & Resilience Area and other subject matter experts, as required, in enabling the above responsibilities to be effectively executed.

5.1.5 Area Managers / Formal Leaders

All Formal Leaders are responsible for:

(i) regularly discussing Risks with their teams, including identifying new and emerging Risks

(ii) escalating and providing information on new and emerging Risks to their function's Risk Champions, Risk Owners and/or HoFs, to ensure Risks, Controls and Treatments can be captured within relevant Risk Systems and reported in a manner that is accurate, consistent and timely

(iii) ensuring that Personnel who report to them incorporate Risk Management into their planning and decision-making processes

(iv) consulting the Enterprise Risk & Resilience Area and other subject matter experts, as required, in enabling the above responsibilities to be effectively executed.

5.1.6 Other Personnel

All Personnel are responsible for identifying and managing Risk within their day to day operations and escalating Risks to management where these Risks cannot be managed within their authority.

5.2 Enterprise Risk & Resilience Area roles and responsibilities

The Enterprise & Resilience Risk Area is responsible for:

(i) providing Risk Management subject matter expertise to the organisation

(ii) developing and maintaining this Standard to support its continued alignment to Western Power's business as it changes over time

(iii) facilitating Risk workshops and delivering training to Personnel as required by the organisation

(iv) attending planning and decision-making forums / meetings to provide Risk input into those discussions, where appropriate

(v) supporting Executive Management with the development and monitoring of the organisation's Strategic Risks

(vi) supporting the Board to develop and maintain the organisation's Risk Appetite Statement

(vii) providing the Executive Team and FRAC with the required level of Risk reporting.

5.3 Risk-specific roles and responsibilities

These responsibilities relate to Risk-specific roles that exists to support the effective management and coordination of Risks, Controls and Treatments for which they are responsible for (e.g. via delegation, appointment etc.). For roles and responsibilities specific to certain Risk Contexts as highlighted within section 4.3, refer to the respective guidelines referenced throughout this Standard.

5.3.1 Risk Champions

Risk Champions act as delegates to action the responsibilities of Heads of Function and are supported by the Enterprise Risk & Resilience Area to deliver Risk-related activities. The Risk Champions are responsible for:

(i) maintaining their Function's Risk System (e.g. ensuring completeness, accuracy and consistency of information captured)

(ii) escalating any relevant changes in their Function's Risk Profile to the HoF and/or Enterprise Risk & Resilience Area

(iii) acting as a liaison with the Enterprise Risk & Resilience Area on behalf of their Function

(iv) attending any Risk training provided by the Enterprise Risk & Resilience Area

(v) assisting with any Risk activities relevant to their function as a part of other business initiatives.

5.3.2 Risk Owners

Risk Owners have the accountability and authority to manage particular Risks and are typically the individuals most impacted by the Risk if it were to eventuate. Where appropriate, Risk Owners may also have accountability over the Controls in place to manage respective Risks.

Risk Owners are responsible for:

(i) coordinating with Risk Champions in ensuring any identified Risks are appropriately and consistently captured within relevant Risk Systems

(ii) coordinating with assigned Control Owners in ensuring adequate Controls are in place and working effectively to manage Risks to tolerable levels

(iii) monitoring Treatment implementation progress to ensure Treatments are completed within agreed timeframes

(iv) conducting Risk reviews and reporting on the status of any new and existing Risks via the appropriate governance structure (e.g. to HoFs or Project Steering and other Committees) and to the Enterprise Risk & Resilience Area

(v) assessing and monitoring Risk Ratings as controls are introduced or Treatments implemented.

(vi) Escalation of 'extreme' residually rated Risks or Risks associated with a long running issue / threat to an Active Management Forum.

5.3.3 Control Owners

Control Owners have accountability and authority in ensuring the ongoing effectiveness of Controls in place to manage Risks.

Control owners are responsible for:

(i) ensuring existing Controls and planned Treatments are appropriately and consistently captured within relevant Risk Systems

(ii) developing and monitoring the continued operating effectiveness of implemented Controls

(iii) establishing and undertaking appropriate levels of Assurance activities in a timely and consistent manner where Critical Controls have been identified against Critical Risks (see section 6.3 for further details surrounding Critical Controls and Assurance activities)

(iv) providing input into the Risk assessment process for those Risks that are managed through their Controls

(v) providing regular updates to the relevant Risk Owner and Risk Champion where there are changes to the design or operating effectiveness of their Controls

5.3.4 Treatment owners

Where a Risk is considered intolerable, a Treatment must be identified, and a responsible owner assigned for implementation of that Treatment. The Treatment Owner has the authority and accountability to ensure the Treatment is implemented within the agreed timeframe.

Treatment Owners should also coordinate with the Risk / Control Owner in ensuring the status of all planned and ongoing Treatments are adequately captured within relevant Risk Systems.

6. Monitoring, reporting and assurance

The effectiveness of this Standard is assessed in the following ways:

(i) regular formal review

(ii) quarterly reporting to the FRAC

(iii) Risk Management assurance.

6.1 Regular formal review

This Standard will be reviewed at least once every there-year period, or when a major shift in the organisation's Risk Appetite or Risk Profile occurs due to changes in the Organisation's Strategy, or internal / external operating environment.

Regular formal reviews are important in ensuring this Standard remains fit-for-purpose.

6.2 Quarterly reporting to the FRAC

The Enterprise Risk & Resilience Area reports quarterly to the FRAC on the performance of Risk Management. The report includes (amongst other information):

(i) the status of Risk Management governance activities

(ii) the status of and any changes surrounding Strategic Risks (incl. emerging themes)

(iii) results from select Assurance activities conducted

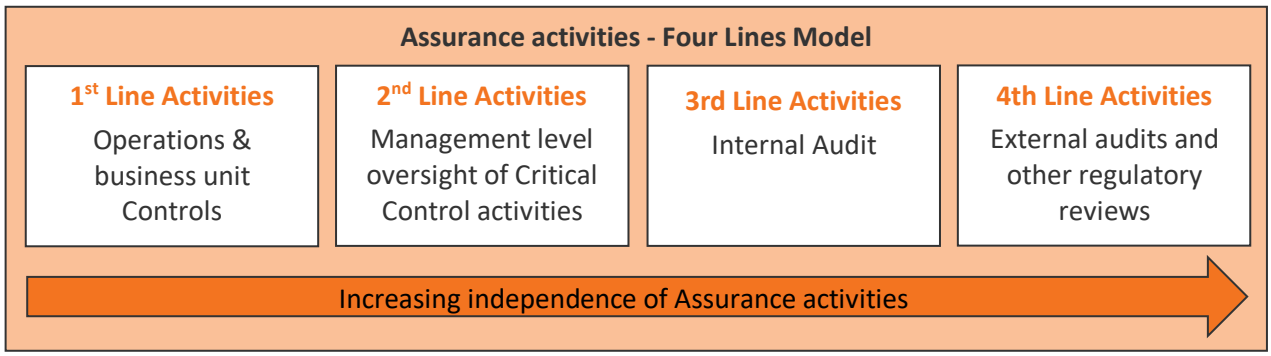
(iv) escalation of any Functional or Operational Risks rated residually as 'extreme'.

(v) escalation of any emerging Functional or Operational Risk themes

6.3 Risk Management Assurance

In providing the Board and Executive Management with confidence on the overall effectiveness of Western Power's Risk Management Processes, the organisation adopts the Four Lines Model (see Figure 4) in providing different levels of Assurance over the effectiveness of processes and Controls across the Business. The Assurance Standard provides an overview and highlights the distinction between each of these lines with an emphasis on Second Line Activities in relation to the undertaking of Critical Control Assurance activities.

Figure 4: Four Lines Model



7. Dictionary

Words in the first column of the following table are defined terms and have the corresponding meaning shown in the second column of the table. Defined terms appear in this document as capitalised.

Defined term	Meaning
As Low As Reasonably Practicable (ALARP)	The residual risk as been reduced to as low as reasonably practicable, demonstrating that the cost involved in reducing the Risk further would be grossly disproportionate to the benefit gained.
Assurance	A structured and systematic approach to providing key stakeholders with confidence that Controls relied on in managing identified Risks are being monitored for continued operating effectiveness.
Control	Controls are any existing measures or actions (manual or system dependent) applied to modify or manage (through prevention, detection or mitigation) Risk exposures associated with processes or activities undertaken.
Control Owner	Accountable and responsible for ensuring the ongoing effectiveness of Controls in place to manage an existing Risk. Control Owners may not necessarily perform the Control activity; however, these owners are required to maintain a level of oversight of the control's performance.
Consequence	Reflects the most realistic / plausible outcome (i.e. Consequence) that would occur at the highest severity if the risk event were to eventuate. Refer to the Enterprise Risk Assessment Criteria for further definition.
Critical Controls	A Control or group of Controls that is believed to be maintaining an otherwise intolerable risk at a tolerable level.
Critical Risk	Critical Risks are risks which contain an Inherent consequence risk rating of catastrophic, based on the most realistic / plausible scenario. Refer to the Assurance Standard (EDM #54729231 for further definition on Critical Risks, and the Enterprise Risk Assessment Criteria for details surrounding Western Power's consequence risk ratings.
Cyber Security	Cyber Security refers to the body of technologies, processes, Controls and practices designed to protect an organisation's networks, devices, programs, and data from attack, damage, or unauthorized access.
Functional Risk	Risks that prevents or hinders achievement of a Western Power function's performance objectives as reflected within a respective function's business plan.

Inherent Risk	The level of risk exposure where no Controls are in place, or if all Controls in place were to fail (i.e. be ineffective) at the same time.
Likelihood	The probability of a Risk event occurring at the type and level of Consequence severity identified.
Operational Risk	Risk that can occur while undertaking operational activities that may adversely impact on the achievement of Western Power's operational objectives.
Risk	The "effect of uncertainty on Objectives" (cl. 3.1 AS/NZS ISO 31000:2018). An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and Threats.
Risk Appetite Statement	The statement approved by the Board in setting the Risk Appetite for Western Power. The level of Risk the organisation is willing to take in carrying out its operations and achieving its strategic objectives.
Risk Assessment Criteria	Terms of reference by which the significance of Risk is evaluated. Provides the mechanism to determine whether a specified level of Risk is within the parameters of Western Powers' Risk Appetite, provides consistency to compare and prioritise Risks, and assists in decision making and appropriate allocation of resources. Refer to EDM 34037272.
Risk Context	Risk Context refers to the unique circumstances surrounding an activity, taking into consideration the external and internal parameters that influence how we identify and manage a specific Risk. Establishing the Risk Context sets the scope / direction for the rest of the Risk Management Process.
Risk Management	The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.
Risk Management Process	The systematic application of management policies, procedures and practices for identifying, analysing, evaluating, treating, monitoring, reviewing, recording, reporting and communicating Risks in a consistent manner across the organisation.
Risk Owner	Risk Owners have the accountability and authority to manage particular Risks and are typically the individuals most impacted by the Risk if it were to eventuate.
Risk Profile	The Risk Profile is a collection point for information about Risks in an area of operational work. The information collected clearly describes the Risks, lists Controls, and measures the Risk against the appropriate criteria. Risk profiles will evolve over time, for example, to show the current level of Risk and, where necessary, the target Risk to be achieved following the implementation of additional or alternate Control measures.
Risk Rating	The measure of Risk exposure calculated as a function of Likelihood and Consequence as per Western Power's Enterprise Risk Assessment Criteria (EDM #34037272).
Risk System	A tool (e.g. spreadsheet or system), used to capture the Risk information outputs from the Risk Management Process.
Strategic Risk	Strategic risks reflect the internal and external forces capable of threatening Western Power's ability to achieve its business strategies or strategic objectives or affect its long-term positioning and performance.
Threats	Threats refer to the potential incidents that could occur as a result of a vulnerability being exploited, intentionally or accidentally, to obtain, damage or destroy an organisation's asset (e.g. information assets).
Treatment	A Risk modification process. Involves selecting a course of action for addressing the Residual Risk, either by implementing or improving Controls that reduce the Likelihood of the Risk and/or the Impact of the Consequences. Treatments include the tasks/action to be performed and the set start and finish dates.

Vulnerabilities	Vulnerabilities are the gaps or weaknesses across systems and processes that can be exploited by individuals or parties intending to cause harm or loss (e.g. through cyber-attacks).

8. Further information

If you have any questions in relation to this Standard, please contact the Head of Governance, Risk and Compliance or the Executive Manager Governance and Assurance.

9. Content owner

Head of Governance, Risk and Compliance.

10. Accountabilities

Executive Manager Governance and Assurance	Accountable for approving the content of this Standard and publishing the approved version in Western Power's corporate policies register.
Head of Governance, Risk and Compliance	Accountable for: (i) developing the content and ensuring its accuracy (ii) implementing this Standard (iii) ensuring Personnel affected by this Standard, and its related documents, are aware of their responsibilities (iv) ongoing education (as necessary) (v) monitoring compliance with the requirements of the Standard and its related documents (vi) ensuring that appropriate remedial actions are taken if there are compliance breaches.

11. Review

This Standard will be reviewed and evaluated by the content owner at least once in every three-year period taking into account the purpose of the Standard and the outcome of the compliance review.

12. Related documents

Title	EDM reference
Assurance & Risk Policy	EDM 32565084
Assurance Standard	EDM 54729231

Cyber Threat, Vulnerability and Risk Guideline	EDM 50791013
Delivery Risk Management Guideline	EDM 43041786
Enterprise Risk Assessment Criteria	EDM 34037272
Finance, Risk & Audit Committee Terms of Reference	EDM 3068969
Internal Audit Charter	EDM 31064221
Risk and Resilience Framework	EDM 41489002
Risk Appetite Statement	EDM 43397084
Enterprise Risk Management Guideline	EDM 41492839

13. Approval history

Version	Approved by	Date of approval	Resolution no.	Notes.
1.	Board	24/03/2006	BD/19/2006	
2.	FRAC	19/07/2007	FRC/14/2007	
3.	FRAC	30/07/2009	053/2009/FRC	
4.	FRAC	29/06/2011	029/2011/FRC	
5.	General Counsel	16/07/2014	070/2014/BD	Under authority delegated by Board on 04/03/2014
6.	Board	05/08/2014	015/2015/BD	
7.	General Counsel	24/04/2015	004/2015/BD	Under authority delegated from the Board on 01/07/2014
8.	General Counsel	15/05/2015	004/2015/BD	Amendments sought by F&RC at its meeting on 4 May 2015 made under authority delegated from the Board on 01/07/2014
9.	General Counsel	15/05/2015	004/2015/BD	Amendments sought by the Board at its meeting on 2 June 2015 made under authority delegated from the Board on 01/07/2014
10.	FRAC	07/02/2017	066/2017/BD	
11.	Executive Manager Governance & Assurance	09/12/2020	004/2015/BD	

……Andrew Cook, A/Executive Manager Governance & Assurance