Company Procedure: Corporate Risk Management procedure CEOP0002.21

For questions regarding or permission to release this Policy, please contact Essential Energy's Chief Risk and Compliance Officer.

If working from a printed copy of this document, check Policy Alerts and the Policy Library regularly for updates.

6 July 2022 –Issue 4
Approved By: Chief Risk and Compliance Officer
Next review date: July 2025
COMMERCIAL-IN-CONFIDENCE

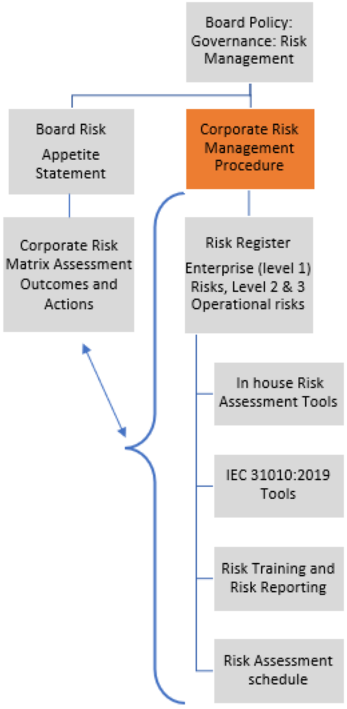
CONTENTS

1.0 PURPOSE

To articulate the company's risk management process, assessment methodology and reporting requirements for the Corporate Risk Management Framework (CRMF).

This procedure has direct application to assist with the management of Enterprise risks at a Corporate level and also applies to divisional risk management as listed in Figure 2 – CRMF (based on ISO 31000: 2018 Risk management—Guidelines).

Figure 1 below illustrates the hierarchy of Corporate risk policy, procedure, register, tools and templates in the CRMF.


Board Policy: Governance: Risk Management
Board Risk Appetite Statement
Corporate Risk Management Procedure
Corporate Risk Matrix Assessment Outcomes and Actions
Risk Register Enterprise (level 1) Risks, Level 2 & 3 Operational risks
In house Risk Assessment Tools
IEC 31010:2019 Tools
Risk Training and Risk Reporting
Risk Assessment schedule

Board Policy: Governance: Risk Management (CECP0002.03) including Risk Appetite Statement
Overarching policy and Risk Appetite Statement including requirements for Risk Management.

Corporate Risk Matrix Assessment Outcomes and Actions (CECG0002.21a)
Risk Framework document that provides guidance on risk consequence and probability. This is used in the Risk Framework to determine impact severity and requirements in risk assessments.

Corporate Risk Management Procedure (this document; CEOP002.21)
This document contains a description of the Risk Management Framework and provides the "how to" templates to assist Division and Function Owners build risk assessments:

- Corporate Risk Assessment Tools.
- IEC31010:2019 Risk Tools.
- Risk training and reporting; and
- Risk assessment schedule.

Figure 1 – Hierarchy of CRMF policies, procedures and templates

This procedure applies to the entire organisation.

2.0 ACTIONS

2.1 Understanding the CRMF

Essential Energy's approach to risk management is aligned to ISO 31000:2018 and IEC 31010:2019 - Risk Management – Risk Assessment Techniques. Effective risk management is embedded into business operations through a three-tiered approach comprising:

- An organisational Risk Management Policy approved by the Board.
- Organisational Risk Management Practices approved by the Chief Executive Officer and Chief Risk and Compliance Officer outlining a consistent approach to risk identification, assessment, control and reporting across business activities and risks; and
- Supporting plans, structures, policies, procedures, and controls to embed effective risk management into operations.

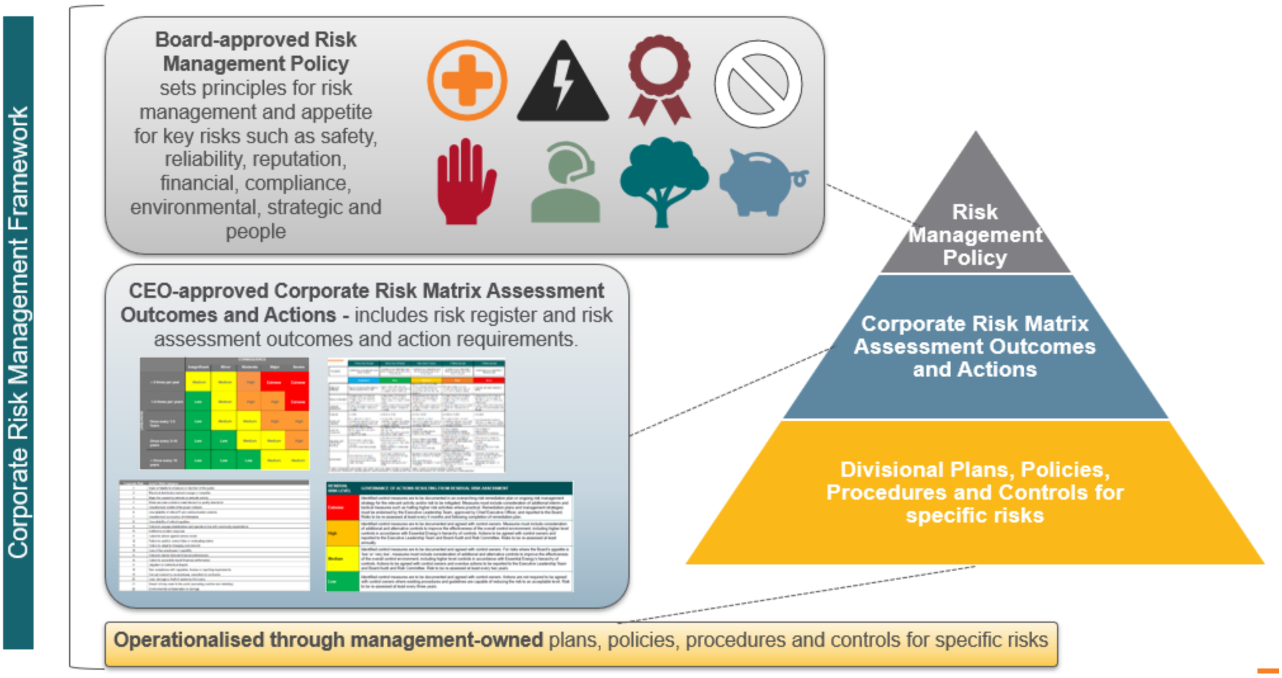

Corporate Risk Management Framework
Board-approved Risk Management Policy sets principles for risk management and appetite for key risks such as safety, reliability, reputation, financial, compliance, environmental, strategic and people
CEO-approved Corporate Risk Matrix Assessment Outcomes and Actions - includes risk register and risk assessment outcomes and action requirements.
Operationalised through management-owned plans, policies, procedures and controls for specific risks
Risk Management Policy
Corporate Risk Matrix Assessment Outcomes and Actions
Divisional Plans, Policies, Procedures and Controls for specific risks

Figure 2 – CRMF (based on ISO 31000: 2018 Risk management—Guidelines)

2.2 Implementing the CRMF

The framework is intended to supplement other organisational management systems (e.g. safety, asset management, compliance) by assisting the organisation to integrate risk management into these systems where possible. Risk management is closely integrated into business strategy and planning, including risks to the achievement of business objectives and plans to address specific high-risk hazards based on the environment and context within which the organisation operates.

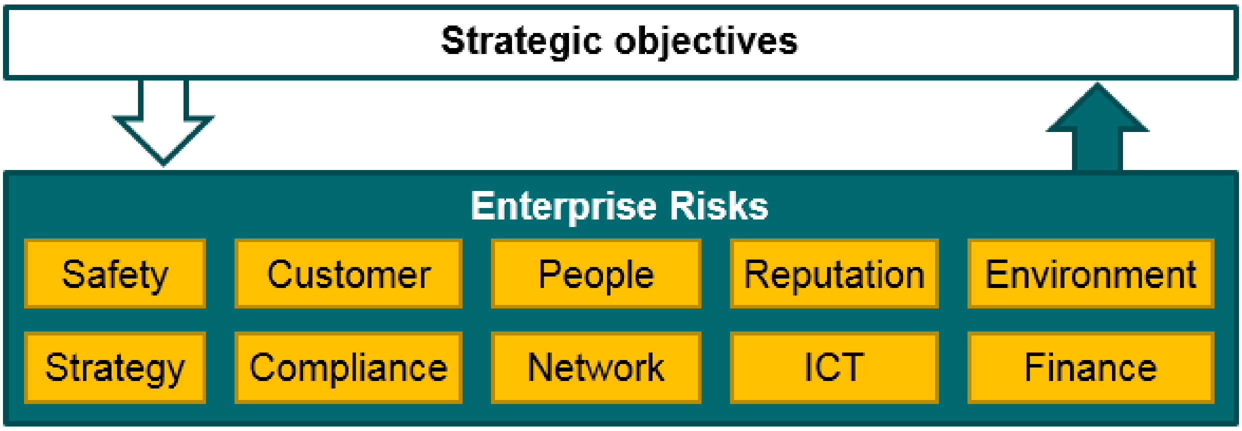


Figure 3 – Relationship between Strategic objectives and Enterprise risk

Enterprise risk categories (**Table 1 below)** assist in linking company level responsibilities and strategic objectives to assessments of Enterprise risks (**Figure 3 above)**.

ER Number	Enterprise Risk Category	Hazard/Threat Event Type
ER 1	Safety	Fatality/serious injury of employee or member of public
ER 2	Network	Major Fire or electrical network outage
ER 3	Customer	Significant customer impact related to the Network
ER 4	Finance	Significant unbudgeted financial loss
ER 5	Compliance	Liability associated with a dispute or material breach of legislation, licence
ER 6	Community Standing	Sustained public criticism of Essential Energy
ER 7	Environment	Significant environmental incident
ER 8	People	Failure to deliver performance due to lack/loss of key employees / skills
ER 9	Strategy	Strategic objectives are not delivered and business opportunities are lost
ER 10	ICT	Significant ICT & OT system failure

Table 1 – Enterprise Risk Categories

To ensure that organisational culture supports effective risk management, Essential Energy establishes and maintains:

- clear principles to guide informed, transparent and evidence-based decision making, including in setting strategic and organisational objectives.

- open communication channels to ensure employees understand what is expected of them, including in their capacity as leaders and role models of appropriate behaviour, and that employees feel safe to escalate concerns and confident that concerns will be addressed appropriately.

- a sufficient level of skills, training, and tools for employees consistent with their accountabilities, responsibilities, and authorities.

- effective identification, assessment, control, monitoring, reporting and escalation processes to integrate risk management into business processes.

- processes and systems that link risk appetite to strategic planning and investment prioritisation.

- a continuous learning culture where Essential Energy challenges, develops and improves business practices and its approach to risk management; and

- assurance processes for the ongoing review and reporting of risk control effectiveness, including at Board and Executive level, and consideration of whether controls are prudent and appropriate to manage risk so far as is reasonably practicable.

2.2.1 Mandate, Commitment and Design of the CRMF

The Board approved Risk Management Policy provides the mandate to implement risk management across the company. Implementing the CRMF and its ongoing effectiveness requires strong and sustained commitment. Section 3 of this procedure outlines the authorities and responsibilities of the Chief Executive Officer (CEO) and the Executive Leadership Team (ELT).

In addition, the following design principles apply (and illustrated in Figure 4 below):

- Understanding of the company and its context is provided through the Strategic Planning process.

- Oversight has been established with Board, Executive and Governance forums to oversee risk management.

- As an electricity distribution network service provider Essential Energy has a unique legislative, regulatory licence context together with standards to comply with.

- Key risk standards are followed such as ISO31000:2018 Risk management – Principles and guidelines and IEC 31010:2019 - Risk management – Risk assessment techniques.

- The CRMF consist of Board approved policies, procedures tools and systems; Essential Energy’s Corporate Risk Matrix is contained in CECG0002.21a Corporate Risk Matrix Assessment Outcomes and Actions and is approved by the CEO.

- Each division is expected to develop risk management practices that allows them to understand the risks that relate to their operational activities; and

- This procedure provides guidance on how to integrate risk management into company processes.

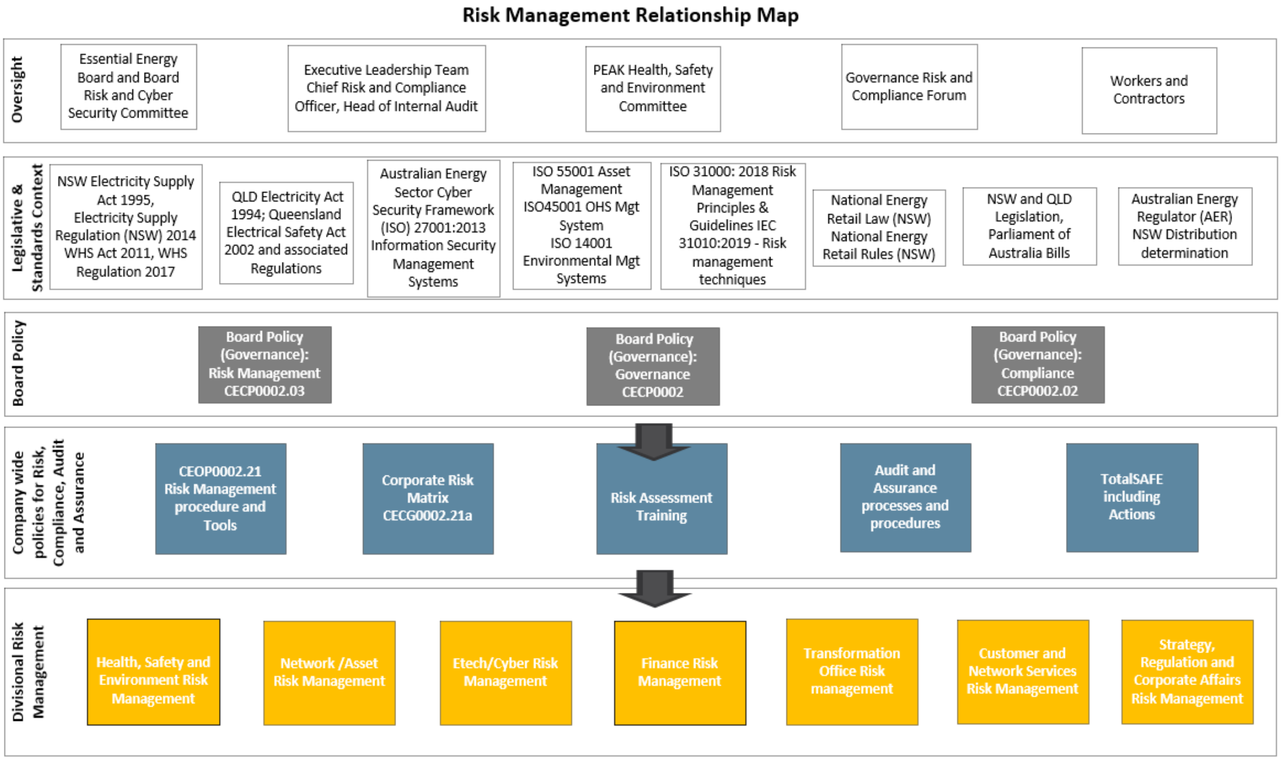

Risk Management Relationship Map
Oversight
Essential Energy Board and Board Risk and Cyber Security Committee
Executive Leadership Team Chief Risk and Compliance Officer, Head of Internal Audit
PEAK Health, Safety and Environment Committee
Governance Risk and Compliance Forum
Workers and Contractors
Legislative & Standards Context
NSW Electricity Supply Act 1995, Electricity Supply Regulation (NSW) 2014 WHS Act 2011, WHS Regulation 2017
QLD Electricity Act 1994; Queensland Electrical Safety Act 2002 and associated Regulations
Australian Energy Sector Cyber Security Framework (ISO) 27001:2013 Information Security Management Systems
ISO 55001 Asset Management ISO45001 OHS Mgt System ISO 14001 Environmental Mgt Systems
ISO 31000: 2018 Risk Management Principles & Guidelines IEC 31010:2019 - Risk management techniques
National Energy Retail Law (NSW) National Energy Retail Rules (NSW)
NSW and QLD Legislation, Parliament of Australia Bills
Australian Energy Regulator (AER) NSW Distribution determination
Board Policy
Board Policy (Governance): Risk Management CECP0002.03
Board Policy (Governance): Governance CECP0002
Board Policy (Governance): Compliance CECP0002.02
Company wide policies for Risk, Compliance, Audit and Assurance
CEOP0002.21 Risk Management procedure and Tools
Corporate Risk Matrix CECG0002.21a
Risk Assessment Training
Audit and Assurance processes and procedures
TotalSAFE including Actions
Divisional Risk Management
Health, Safety and Environment Risk Management
Network /Asset Risk Management
Etech/Cyber Risk Management
Finance Risk Management
Transformation Office Risk management
Customer and Network Services Risk Management
Strategy, Regulation and Corporate Affairs Risk Management

Figure 4 – Design elements of CRMF

2.2.2 *When to Apply this Procedure*

This procedure is intended to be used to understand and manage risks relating to the Essential Energy's business activities. Specifically, a risk assessment is required when:

- an existing risk changes materially, reaches or review trigger, or a new risk is identified;
- there is a material, unplanned and adverse change in the control environment; or
- introducing a new risk control or departing from an existing risk control including through any pilots or trials.

Risk assessments must always be undertaken before an activity or change commences; they cannot be done retrospectively either after a decision, or a change has already been made.

2.2.3 *Modifications to the Corporate Risk Matrix*

The outcomes and actions from the Corporate Risk Matrix set out minimum requirements for assessments of Enterprise or 'Level 1' Corporate Risks. These can be supplemented where necessary for more granular or detailed risk assessments. Examples include modifications to the likelihood and/or consequence scales, to provide more granularity and/or to extend the standard scales to provide for higher or lower values.

Bespoke matrices can also be created to contextualise the likelihood or consequence categories or scales, or to simplify them. This is allowable, provided any modifications maintain alignment to the Corporate Risk Matrix and the rationale for any modifications is appropriately documented.

2.2.4 *Training in the Application of the CRMF*

The Governance Risk and Compliance Forum is a monthly meeting coordinated by the Corporate Risk team where risk specialists can share risk techniques and coordinate and manage risk across different functional areas. In addition, the Chief Risk and Compliance Officer will provide either risk awareness training or more detailed technical training in the application of this procedure.

2.2.5 Monitoring and Review of the CRMF

Monitoring and review of the effectiveness and performance of the CRMF is be performed by the Chief Risk and Compliance Officer. Reports are provided to the General Counsel & Company Secretary, ELT and Risk and Cyber Security Committee (RCSC). Please see Section 2.4 – Risk reporting for more detail.

Improvement actions identified as part of the monitoring/management reviews/continuous improvement will be recorded in TotalSAFE.

2.3 Risk Management Process

All managers and employees of the company are responsible for managing risk. A risk is defined as the effect of uncertainty on objectives. Essential Energy follows the principles in the below Risk Management flow chart (Figure 5 below) based on ISO 31000:2018 and the following sections provide a description of the requirements to complete each step.

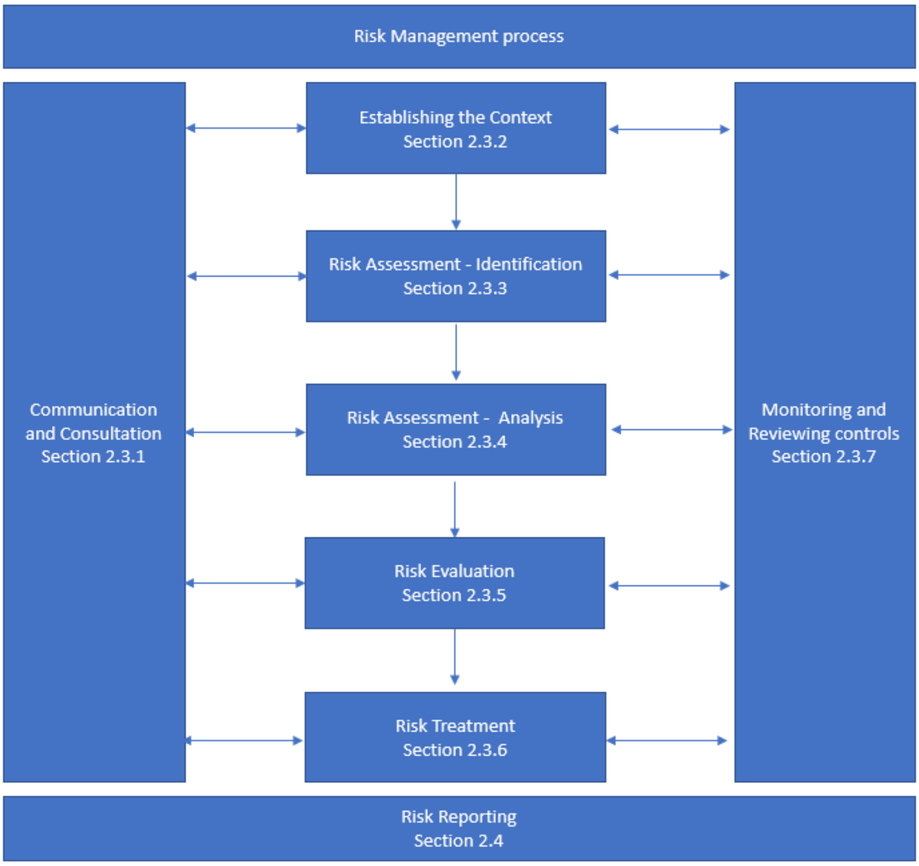

Risk Management process
Establishing the Context Section 2.3.2
Risk Assessment - Identification Section 2.3.3
Risk Assessment - Analysis Section 2.3.4
Risk Evaluation Section 2.3.5
Risk Treatment Section 2.3.6
Communication and Consultation Section 2.3.1
Monitoring and Reviewing controls Section 2.3.7
Risk Reporting Section 2.4

Figure 5 – Risk management process

2.3.1 Communication and Consultation

The first step of the risk management process is Communication and Consultation. Communication and Consultation will be undertaken with internal and external stakeholders as appropriate and will be maintained throughout the risk management process (as indicated in **Figure 5**). Employees and managers should plan the Communication and Consultation process to gain support and input from their colleagues during the earliest stages of the risk management process. It should be noted that the degree of consultation is at the discretion of the person undertaking the risk assessment. The Communication and Consultation process should address information and issues relating to the identified risk, its causes, consequences the existing controls and potential alternative controls. Documentation of the engagement can be maintained using the template provided in Annexure A Internal/External Stakeholder engagement.

Effective Communication and Consultation may involve discussions with experienced and knowledgeable persons, literature reviews including the review of previous risk assessments, incident investigations, audit reports, discussion and survey with stakeholders and the community. In an effective, mature risk assessment, Consultation and Communication will continue throughout the risk assessment process by bringing together stakeholders with differing areas of expertise. This is typically achieved by identifying multi-disciplinary teams of stakeholders in the form of a risk assessment workshop. The consultation process is also important when evaluating risk and for gaining agreement and endorsement for Treatment Action Plans.

Communication and Consultation with stakeholders is important as stakeholders make judgements on risk based on their individual perception. These perceptions can vary due to differences in their risk tolerance, needs, assumptions and concerns; however, it is important that these differences are explored and taken into account during the risk assessment.

Essential Energy technique

- Annexure A - Internal/External Stakeholder engagement; and
- Refer IEC 31010 – 2019 techniques.

2.3.2 Establishing the Context

The context (internal and external) will be established at the commencement of the risk assessment process, describing the objectives and scope of the risk assessment, and the internal and external parameters to be taken into account when managing the risk. Key elements of the context will include:

- **Purpose** – the key objective(s) or outcome(s) e.g., decisions that must be made.
- **Risk appetite** – the level of risk that the organisation is prepared to accept in order to achieve its strategic objectives
- **Scope or Consequence differentiators** – the boundaries of the assessment including specific inclusions and exclusions e.g. an entire asset class population, a subset of an asset class, a specific geographical area or asset, specific causes or failure modes, or the time period over which the risk is to be assessed.
- **Assumptions and Constraints** – any preconditions, or internal / external circumstances in which the assessment is being undertaken including, for example, specific parts of the Asset Management System or Energy network safety management System or network that are under consideration.
- **Methodology** – qualitative, semi quantitative and/or quantitative assessment methods.
- **Stakeholders for risk assessment** – key internal / external stakeholders who need to be involved in the process or be informed of the outcomes, including any pre-existing views.

- **External context** - Key external factors affecting the current network risk environment have been drawn from the Corporate Strategy as follows:

  - **Political** – NSW Electricity Infrastructure Roadmap; Renewable Energy Zones; increasing engagement with local councils.
  - **Economic** – continued pressure for reductions in distribution network charges; competition for emerging distribution services.
  - **Social** – increase expectations around network resilience and control over personal energy supply; changing consumer behaviour, increasing solar penetration; increasing demand for connections; increasing decentralisation**.**
  - **Technological** – rapidly changing technological landscape including batteries (increasing capacity and reducing cost), hydrogen storage, stand-alone power system, microgrids, community batteries, smart technology (meters, asset monitoring), electric vehicles; increasing digitisation.
  - **Environmental** – climate change; increasing focus on decarbonisation; and
  - **Legal/Regulatory** – increasing scrutiny from regulators; increasing regulator focus on cybersecurity; increasing expectations around the sophistication and robustness of risk management practices; increasing complexity as we move towards Distributed Energy Resources (DER) and Distribution System Operators (DSO); National SAPS Framework Australian Energy Market Operator (AEMO).

Establishment of the context will also include defining the risk tolerance for the evaluation of risk. The company's risk tolerance is summarised in **Table 2**. Risk tolerance is a formal term to describe whether additional action needs to be taken to reduce risk.

Risk Tolerance
A risk is tolerable when the risk is reduced to So Far As Is Reasonably Practicable (SFAIRP).
Risks are also tolerable if they are Non-SFAIRP and have a Treatment Action Plan in place to reduce the risk to SFAIRP.
Risks that are Non-SFAIRP, with no Treatment Action Plan in place are considered intolerable unless assessed as within risk appetite (for example, the risk appetite is moderate, and the residual risk level is low).

Table 2 – Risk Tolerance

Statements of risk appetite are included in Board Policy: Governance: Risk Management (CECP0002.03). The table below may be used in risk assessments to link risk appetite to organisational planning, investment and target setting where relevant.

	Risk Appetite				
	Very Low	Low	Moderate	High	Very High
Overall approach / tolerance for uncertainty	Very risk averse	Conservative / cautious	Balanced	Open to increased risk	Actively take or increase risk

	Risk Appetite				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Investment planning and trade offs	Investment directed to improving risk profile	Investments may be redirected to risks with lower appetite	Driven by relative costs and benefits	Investment only if generating significant opex saving or revenue	Actively take risks to improve outcomes in other areas
Performance targets	Significant improvements / towards zero	Typically aim for short-term and long-term improvements	May be willing to trade off performance in different time periods	Willing to accept increase in risk profile	Planned increase in risk profile

Table 3: Risk Appetite and Tolerance trade off

Note: In relation to Very Low/Low appetite risk Owners should use a disproportion factor of > 1.

Key elements of the 'Establish Context' stage include:

- Identify business activity from list of core business functions.
- Identify potential credible threats with consideration to all Enterprise Risk categories.
- Identify and define consequence differentiators within the business function. For example, affected areas, specific regions or scenarios; and
- Identify methodology, stakeholders, external context, risk appetite and tolerance.

Key Techniques include:

- Monitoring of any incidents reported.
- Review of audits and investigations.
- Direct feedback from workers, contractors.
- Public consultation e.g. Customer Advocacy Group and specific industry groups.
- Information provided by industry peers, and regulators throughout Australia; and
- Other – Refer IEC 31010 – 2019 techniques.

2.3.3 Risk Assessment – Risk identification

Risk identification involves the process of systematically identifying the uncertainties to the achievement of objectives. The uncertainty is expressed in the form of a hazard/threat event, i.e. what is the event that will prevent the achievement of the objective? The hazard/threat being any source of harm.

The following factors, and the relationship between these factors, should be considered:

- tangible and intangible sources of risk.
- causes ,controls events.
- threats and opportunities.
- vulnerabilities and capabilities.

- changes in the external and internal context.
- indicators of emerging risks.
- the nature and value of assets and resources.
- consequences and their impact on objectives.
- limitations of knowledge and reliability of information.
- time-related factors; and
- biases, assumptions and beliefs of those involved.

Key elements of the 'Risk identification' stage include:

- Identify causes, controls and events.
- threats and opportunities; and
- consequences and their impact on objectives.

Key Techniques include:

- Annexure C - Bow-Tie/Threat Barrier Tool
- Brainstorming.
- Check lists.
- Root cause analysis
- Review of policies and procedures.
- Monitoring of any incidents reported.
- Review of audits and investigations.
- Direct feedback from workers, contractors.
- Public consultation e.g. Customer Advocacy Group and specific industry groups.
- Information provided by industry peers, and regulators throughout Australia; and
- Other – Refer to IEC 31010 – 2019 techniques.

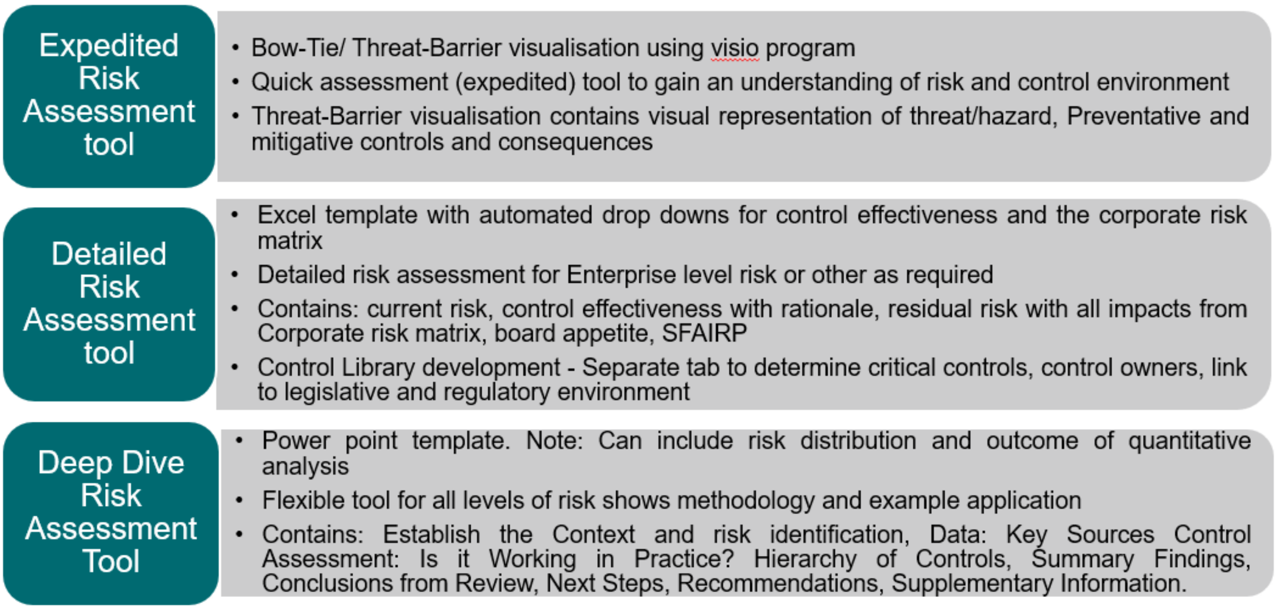
2.3.4 Risk Assessment - Risk Analysis

There are three fundamental techniques to analyse risk. This can involve qualitative, semi-quantitative or quantitative measures.

2.3.4.1 Qualitative Risk Assessment Techniques

Qualitative techniques are based on consequences and likelihoods contained within the Corporate Risk Matrix.

Each division will have approaches to determine qualitative outcomes aligned to the CRMF. Alternatively, Corporate Risk has developed three Corporate Risk Tools (identified in Figure 6 below) with a quick reference guide on when they could be used. Please note these are not mandatory tools but are aligned to the principles contained within the CRMF.



Expedited Risk Assessment tool

- Bow-Tie/ Threat-Barrier visualisation using visio program
- Quick assessment (expedited) tool to gain an understanding of risk and control environment
- Threat-Barrier visualisation contains visual representation of threat/hazard, Preventative and mitigative controls and consequences

Detailed Risk Assessment tool

- Excel template with automated drop downs for control effectiveness and the corporate risk matrix
- Detailed risk assessment for Enterprise level risk or other as required
- Contains: current risk, control effectiveness with rationale, residual risk with all impacts from Corporate risk matrix, board appetite, SFAIRP
- Control Library development - Separate tab to determine critical controls, control owners, link to legislative and regulatory environment

Deep Dive Risk Assessment Tool

- Power point template. Note: Can include risk distribution and outcome of quantitative analysis
- Flexible tool for all levels of risk shows methodology and example application
- Contains: Establish the Context and risk identification, Data: Key Sources Control Assessment: Is it Working in Practice? Hierarchy of Controls, Summary Findings, Conclusions from Review, Next Steps, Recommendations, Supplementary Information.

Figure 6 – Corporate Risk Tools

2.3.4.2 Semi-quantitative Techniques

Semi-quantitative techniques generally include:

- one parameter (usually likelihood) is expressed quantitatively and the other described or expressed on a rating scale.
- scales are divided into discrete bands, the limits of which are expressed quantitatively.
- Points on the scale are often set up to have a logarithmic relationship to fit with data; and
- numeric descriptors are added to scale points, the meanings of which are described qualitatively.

This technique can be completed by monetising the consequence values (as set out in CECG1140 Network Value Framework) and using standard assumptions for converting the qualitative likelihood scales defined in the Network Risk Assessment Criteria into single point estimates.

2.3.4.3 Quantitative Techniques

Quantitative technique is where consequences and likelihoods are expressed on numerical (ratio) scales. Where a risk is analysed in quantitative terms, it should be ensured that appropriate units and dimensions are used and carried over through the assessment.

Within Asset Management and Engineering the value framework is used in conjunction with the Network Risk Management procedure (located on the Policy Library) to monetise capital investment project benefits around safety, reliability, environment (bushfire), environment (other), reputation and community standing, legal and compliance, and financial risk mitigation. The same approach can be taken to analyse benefits in other areas of the business for capital investment projects where these risks are mitigated as a result of the investment.

Generally, for a smaller project with moderate levels of risk and spend a semi-quantitative approach can be taken to monetise these benefits e.g. zone substation building upgrade. For projects with high levels of complexity, spend, societal concern or stakeholder scrutiny the semi-quantitative approach should be used in conjunction with a quantitative approach

2.3.4.4 General Analysis

In general risk analysis should generally consider two alternative risk scenarios:

- The plausible worst case consequence – inherent risk; and
- The most likely foreseeable consequence – residual risk.

Often a risk event will have multiple consequence types associated with it. Each consequence should be assessed using the Corporate Risk Matrix (or developed risk matrix) with a most likely foreseeable likelihood applied. Where multiple consequence categories are assessed, the overall risk rating is taken as the highest from across the range of consequence categories assessed.

An analysis of each identified hazardous/threat event should be undertaken in a consistent manner using control effectiveness rating and rationale as detailed in Annexure B– Understanding controls as part of risk management . Control effectiveness rating and rationale can be used to inform the residual risk ratings

Exemptions for the implementation or removal of a policy or control can be undertaken in the following circumstances:

- obtain approval from the control or policy owner.

- Before approving an exemption, the control owner should be satisfied that the decision is appropriate based on Essential Energy's risk appetite and the relative cost and benefit of alternative options; and

- Exemptions should be in writing, and spell out any timeframe, and conditions such as alternative controls that may be required to manage the risk. See the Board Approved Risk Policy for details.

2.3.4.5 Risk Assessment – Critical Risks and Critical Controls Framework

Critical risks help us identify which events have the biggest potential to cause harm and therefore which controls we should focus our limited resources and effort on. A critical risk is defined as any risk event with a residual risk consequence level of severe. A critical control is a control that plays a significant role in preventing or mitigating a critical risk (see indicators below).

The following are *indicators* that a control may be a critical control. This is not an absolute (yes/no) standard. All items are indicators of criticality, the more present, the higher the indication.

- The control is crucial to preventing or mitigating one or more severe consequence event(s).
- The control's absence or failure would significantly increase the likelihood of one or more severe consequence events occurring, despite the existence of other controls; and
- The control's absence would result in the residual risk rating being outside the Board's risk appetite.

More detail on the Critical Control Framework can be found in Company Manual: HSE Risk Management CECM1000.02, the Critical Risks and Controls Network Risk Management Guide and Annexure B – Understanding controls as part of risk management of this procedure.

Key elements of the 'Risk analysis' stage include:

- Conduct workshops with SMEs.
- Identify the plausible worst case consequence – inherent risk.
- Identify the most likely foreseeable consequence – residual risk.
- Determine control effectiveness supported with evidence on its effectiveness e.g. audits, incidents, documented procedures, SME advice.
- Determine critical risk and critical controls; and
- Determine impacts from Corporate Risk matrix (or approved matrix).

Key Techniques include:

- Annexure C - Bow-Tie/Threat Barrier Tool. –(also contains guidance material) – CEOF0002.21c - Threat Barrier Tool
- Corporate Risk Assessment Tool. (Guidance contained in the first Tab of the Tool) - CEOF0002.21d - Corporate Risk Assessment Tool
- Corporate Deep Dive Risk Assessment (Key notes embedded within the PowerPoint together with example application Tool. – CEOF0002.21e - Deep Dive Risk Assessment Tool
- Quantitative risk assessment using Value Framework – Refer CECG1140 Network Value Framework.
- Critical Risk and Controls Framework – Refer CECM1000.02 HSE Risk Management.
- Check lists.
- Hazard and operability studies (HAZOP).
- Scenario Analysis.
- Root cause analysis.
- Hazard analysis and critical control points (HACCP) Refer CECM1000.02 HSE Risk Management

2.3.5 Risk Evaluation

Each hazardous event will be evaluated against the company's risk appetite and risk tolerance to determine which risks are tolerable based on their existing controls, and which risks require the development of Treatment Action Plans. As detailed in Section 2.3.2, a risk is deemed tolerable if it is considered to be:

- "So Far As Is Reasonably Practicable" (SFAIRP); or
- Non-SFAIRP with treatment action plans in place to move the risk to SFAIRP.
- within the Board approved risk appetite.

Table 4 SFAIRP Test provides guidance for evaluating the risk in order to determine its SFAIRP status.

SFAIRP Test	Yes/No
Have you identified all credible/practicable options to address identified gaps or weaknesses in current controls?	Yes/No
Have you identified additional credible/practicable options to treat risks that are already SFAIRP? (Answers to both these should be 'Yes' to show the risk assessment has at least considered additional controls in line with the requirements of the CRMF, WHS requirements and AS5577 requirements)	**Yes/No**
For safety risks, have you considered options in the context of the Hierarchy of Control?	Yes/No

SFAIRP Test	Yes/No
(Answer should be 'Yes')	
Does the risk assessment demonstrate that the risk(s) is/are managed SFAIRP by reference to appropriate evidence that to do more to manage the risk would: a. Not be necessary (to meet a defined performance objective or target). b. Not be prudent, including by reference to the requirements of relevant legislation, standards or codes, established industry good practice, findings from control monitoring or verification activity, a formal review, investigation or audit, or to satisfy subject matter expert judgement. c. Introduce an unacceptable risk increase or risk transfer. d. Not be strategically aligned or in the long-term interests of customers. e. Be inefficient or grossly disproportionate, as evidenced by appropriate cost-benefit analysis. f. Be unaffordable in a constrained environment.	Yes/No

Table 4 – SFAIRP status test

The responses to the SFAIRP status test questions must be recorded on the relevant risk assessment.

After considering the SFAIRP status in your workshop/meeting, the risk rating and SFAIRP status are to be validated with the relevant Risk Owner and or Control Owner prior to initiating any treatment actions.

To test the rationale of their evaluation Risk Owners or Control Owners are encouraged to ask, "would our stakeholders be surprised if we announced a loss due to this risk?" Where the answer is "yes", the effectiveness of the existing control environment, along with the options to further reduce the risk should be investigated further.

Key elements of the 'Risk evaluation' stage include:

- Summary findings
- Complete SFAIRP test; and
- Compare residual risk outcomes against Board approved risk appetite.

Key Techniques include:

- SFAIRP test contained in this procedure; and
- Board approved risk appetite is contained in the Board Policy: Governance: Risk Management CECP0002.03.

2.3.6 Risk Treatment

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored.

The treatment plan should clearly identify the order in which risk treatment should be implemented. When the results of the risk evaluation determine a risk to be non-SFAIRP, risk treatment options will be identified, and a Treatment Action Plan documented. Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, the treatment action provides additional controls or modifies/improves existing controls. Any business-as-usual activity undertaken to reduce risk is considered an existing control and is not to be included as a treatment action in a risk management plan. Implementation of a treatment action should result in a significantly improved control environment.

Actions within this step include:

- Options identification, including categorisation of treatments using the hierarchy of control. See Annexure B – Understanding controls as part of risk management;
- Understand the benefits and risks associated with each option, to inform forecast residual risk and control effectiveness ratings that would result from each option; and
- Understand the costs of each option.

Once a risk treatment option has been identified, it may be necessary to revisit the risk evaluation in order to determine if it is reasonably practicable to implement. The process of determining if a risk treatment option is reasonably practicable may involve cost-benefit analysis which should be developed on a case-by-case basis.

Specific considerations for demonstrating that safety risks are managed SFAIRP are guided by advice from Safe Work Australia[1]. This states that, "*reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure the health and safety, taking into account and weighing up all relevant matters including:*

a) The likelihood of the hazard or the risk concerned occurring
b) The degree of harm that might result from the hazard or the risk
c) What the person concerned knows, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising the risk
d) The availability and suitability of ways to eliminate or minimise the risk, and
e) After assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is ***grossly disproportionate*** *to the risk."*

All Treatment Action Plans will include a responsible manager and due date for implementation loaded into TotalSAFE. Treatment actions do not necessarily need to have a completion date within the life of the current risk management plan and the treatment action can carry over in the following year's risk management plan.

The Risk Owner or Control Owner is required to endorse any treatment actions and in doing so confirms that the necessary resources will be made available to complete the actions within the designated timeframes.

[1] Safe Work Australia, Interpretive Guideline – Model Work Health and Safety Act, The Meaning of 'Reasonably Practicable'. Available at:

2.3.7 Monitoring and Reviewing Controls

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Key Risk Indicators will be established for Critical risks contained in a risk assessment where the residual risk consequence level is severe. Where Key Risk Indicator performance declines, corrective actions to restore control should be developed and implemented. For options refer to Annexure D: Key Risk Indicators for Risk Management.

The implementation of Treatment Action Plans provides a risk management performance measure. At the completion of all treatment actions, the SFAIRP status does not automatically revert to SFAIRP. A full re-assessment is required to be undertaken to confirm that the hazardous event has moved from Non-SFAIRP to SFAIRP.

Risk Owners and/or Control Owners are responsible for reviewing and monitoring the implementation of Treatment Action Plans and the status of Key Risk Indicators. In certain circumstances, a change control process may be required for Treatment Action Plans e.g., implementation date.

2.4 Risk Reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the organization.
- provide information for decision-making.
- improve risk management activities.
- assist interaction with stakeholders, including those with responsibility and accountability for risk; and
- management activities.

Risk management performance will be measured, monitored and reported using Divisional reports tailored for the risk that is being addressed. The Enterprise (level 1) residual risk outcomes should be noted against Essential Energy's Corporate Risk Matrix, Assessment Outcomes and Actions CECG0002.21a to ensure appropriate governance arrangements. Example risk reporting is identified in Annexure E: Single Page Risk Dashboard.
Monitoring and reporting of performance on the implementation and effectiveness of controls associated with the CRMF should be provided at the respective meetings of key oversight committees.

In addition to the above, the identification and analysis of emerging risks will be conducted in conjunction with the company's strategic planning process.

2.4.1 Emerging Risk Identification

An emerging risk is a risk that is not expected to significantly impact the organisation within a typical risk assessment horizon of 1-3 years, but either:

- Is expected to result in significant impacts over longer time horizons, or
- Has a high velocity – e.g. a potential to cause significant impacts within 1-3 years due to an environment or context that is changing or escalating rapidly

Fundamental to a robust process of emerging risk identification is:

- the risk identification process must challenge the validity and dependability of the core underlying assumptions and business value drivers detailed in the Strategic Plans.

- the ability to draw a relationship between the uncertainty and the objectives and strategic initiatives of the company, in order to test that the uncertainty is not simply a distraction; and
- the process allows for consideration of unexpected, low-probability events with the potential to have a high-impact on the company.

Emerging risks are typically identified and managed through the strategic planning process, but may be identified through other sources, including the examples presented in **Table 5**.

Table 5 – Emerging risk identification sources

Technique	Description
Risk Assessment	Emerging risk identification workshops. Formal risk identification sessions designed to brainstorm uncertainties in the delivery of strategy and the dependability of the underlying business value drivers. This can involve scenario analysis and stress testing of underlying assumptions.
Employee leads	From employees, e.g., Divisional GRC representatives, internal audit or strategic planning. May also be identified at Executive and/or Board planning days.
External sources	External consultants and agencies. The assignment of external experts to conduct consultancy activities that provides information on trends, company performance, contextual developments.
Issues survey	A survey of the company employees designed to identify issues that may impact the operation, strategic execution or reputation of the company.

2.4.2 Emerging Risk Analysis

Due to their nature, many emerging risks material to the company are high-impact, low probability. As a result, the analysis of an emerging risk will not focus so much on the likelihood of the risk, but on the *speed of onset* or Velocity of the risk; that is: how quickly (in terms of time) the impact of the risk will be felt by the company.

Speed of onset or Velocity is an expression of time (as opposed to probability) and is expressed in terms of months.

The analysis of emerging risk will be undertaken on two parameters:

- plausible must likely consequence; and
- speed of onset (velocity).

Table 6 provides a sample of Velocity which can be used in the communication of emerging risks.

Table 6 – Velocity durations

Velocity	Time
Rapid	Less than 3 months
Moderate	Greater than 3 months, but less than 12 months
Slow	Greater than 12 months

The consequence will be assessed using the criteria assigned to the company's Corporate Risk Matrix. The analysis of consequence should be supported with a qualitative statement on the magnitude of the impact. This is important, because in some circumstances the magnitude may well exceed the definition of “Severe” contained on the company Corporate Risk Matrix. In addition, it is good practice to include a narrative of the impact in risk reporting.

2.4.3 Emerging Risk Response

The response to an emerging risk can be one of four actions outlined in **Figure 7** below:

Figure 7 – Matrix for response to emerging risk

Consequence	Velocity: Slow	Velocity: Rapid	Velocity: Very Rapid
Severe	Prepare for	Act upon	Act upon
Major	Prepare for	Prepare for	Act upon
Moderate	Park	Adapt to	Adapt to
Minor	Park	Park	Adapt to

Emerging Risk Response

Act upon	Severe/major consequence, high velocity risks are acted upon. Action is taken to directly respond to the risk - strategy &/or plans changed.
Prepare for	Severe/Major consequence low velocity risks - plans are put in place to prepare the business to manage the risk.
Adapt to	Moderate/minor consequence, high velocity risks are adapted too.
Park	Moderate/minor impact, low velocity risks are parked. Not material in impact and travelling with low velocity hence no need to adapt strategy or plans.

If uncomfortable:......
- Do we know enough?
- Is the impact underestimated?
- Could the risk move faster than estimated?

The initial assessment must be validated with the relevant Risk Category Owner before being finalised, and where emerging risks with severe consequences have been identified, a risk assessment should be undertaken in line with this procedure and Treatment Action Plans developed.
Any Treatment Action Plans should be validated against the Velocity to confirm that the control can be implemented ahead of the expected onset.

2.4.4 Emerging Risk Reporting

Emerging risks will be reported alongside known risks in Divisional risk management Reports. When an emerging risk is identified, it will be assigned to a risk category.

Level 1 Emerging risks will be detailed in the Risk Management Report to the RCSC. In preparing the report, the Risk Manager should consider all identification methods. Typically, this will involve interviews with Risk Category Owners, or their representatives, focusing on issues identified in recent surveys and any other matters that have the potential to impact delivery of Priority Actions.

2.4.5 Opportunity Identification

Where an opportunity is identified while performing any risk management activity it should be referred to the Risk Owner for consideration and prioritisation.

2.5 Governance

Authorities and responsibilities of individuals is described in the AUTHORITIES AND RESPONSIBILITIES section of this procedure. This section outlines the governance in place for Risk Management.

The Board is ultimately accountable for Risk Management. The oversight for this accountability is delegated to the Board Risk and Cyber Committee (RCSC, the Committee), to discharge their oversight responsibilities the Committee receives regular reports from the CEO and the ELT and guides/advises the CEO and the ELT in their assessment of the Risk Management Framework, priorities and measures.

The Executive Leadership Team (ELT) oversee their divisional plans, and as a Committee, note and govern Enterprise Risk, supported by reporting from the General Counsel and Company Secretary and the Chief Risk and Compliance Officer.

The Risk and Control Owners supports the Executives and ELT by undertaking reviews of Risk Assessments. Corporate Risk and Compliance supports Divisions to implement the CRMF

Internal Audit, will, from time to time, independently review the adequacy of the CRMF and effectiveness of the measures taken by the Divisions.

3.0 AUTHORITIES AND RESPONSIBILITIES

Key Authorities and Responsibilities regarding this procedure:

Title	Responsibility
Chief Executive Officer (CEO)	• **What does the CEO do?** • Approves the Essential Energy Corporate Risk Matrix, Assessment Outcomes and Actions - CECG0002.21a. • Overall accountable to the Board for CRMF.
Executives	• **What is an Executive Owner?** A person with accountability or authority to manage enterprise risks. • **What does an Executive Owner do?** • Ensure enterprise risks (level 1) are managed in accordance with the Board approved risk policy. • Decision making authority and support for the key outcomes from risk management activities.
Chief Risk and Compliance Officer (CRCO)	• **What does the CRCO do?** • Responsible for regularly reviewing and updating the CRMF. • Completes reporting to Executive Leadership Team and the Cyber Risk and Security Committee on the Key Risk Indicators and Key Performance Indicators for the CRMF. • Supports General Counsel and Company Secretary in discharging reporting obligations.
L3 Function Owners	• **What is a functional owner?** A person with accountability or authority to manage a function (may also be a Risk Owner). • **What does a functional owner do?** • Ensure strategic and operational risks (level 2 and 3) are managed in accordance with the RM Procedure.

Title	Responsibility
	• Ensure the delivery of processes that the function is responsible for performing. • Review and report key outcomes from risk assessments and control performance monitoring activities to the Executive Owner.
Risk Owner	• **What is a risk owner?** A person with accountability or authority to manage a risk including by delivering the outcome or performing the function or delivering the performance that is impacted by the risk event. • **What does a risk owner do?** • Ensure the risk is managed in accordance with the RM Procedure. • Coordinate / perform risk assessments, including in conjunction with L3 Functional Owner – see above. • Endorse risk ratings, SFAIRP status, control / treatment actions and key risk indicators for the risk events. • Review and report on risk assessments and control performance monitoring activities to the L3 Functional Owner and/or Executive Owner. *Note: where a Risk Owner is also a L3 Functional Owner, Executive review will be required.*
Control Owner (Critical, Control or Interim)	• **What is a control owner?** A person responsible for ensuring that the control is designed and operates effectively to help mitigate the risk and / or deliver the expected performance outcome. • **What does a control owner do?** • Ensure the control is designed, implemented and operated effectively in accordance with Annexure B. • Ensure treatment action plans are implemented. • For critical controls, assign a Verification Owner and ensure this person undertakes Verification activities – see below. • Review assessment provided by Verification Owner and in the event of a discrepancy, see Risk Owner.
Verification Owner	• **What is a verification owner?** A suitably knowledgeable person (other than the Control Owner) responsible for verifying critical controls are performing as expected, plus other controls as required. • **What does a verification owner do?** • Assess design, implementation and operating effectiveness of critical controls (plus other controls as required). • Submit verification summary report to the Control Owner and Risk Owner.

4.0 DEFINITIONS

Where applicable, definitions are consistent with ISO 31000:2018 – Risk Management – Principles and Guidelines.

Bow-Tie Methodology

The Bow-Tie methodology is used to understand the control environment. It provides a graphical means to describe the relationship between hazards, hazardous events (centre), causes (left side) and consequences (right side). Barriers are used to display what measures an organisation has in place to control the risk.

Business Continuity Management (BCM)
Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities (Refer ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements).

Enterprise risk category
Ten enterprise risk categories have been identified for grouping high level risks that have the potential to prevent the company from achieving its objectives. A Risk Category Owner is assigned to monitor the risk management activities undertaken in regard to each enterprise risk category.

Cause
A factor that could lead to the hazardous event occurring. For distinct hazardous events, causes need to have the ability to result in the hazardous event in their own right. Where hazardous events are stated in more general terms, the cause should be expressed in terms of a contributing hazardous event related to an activity.

Corporate Risk Matrix
The 5 x 6 matrix contained in CECG0002.21a Essential Energy Corporate Risk Matrix, Assessment Outcomes and Actions that is used to determine the risk rating for a particular combination of consequence and likelihood. The Corporate Risk Matrix is approved by the CEO and reflects the risk appetite approved by the Board.

Control
Measures that modify risk. Controls may include policies, procedures, processes, devices, practices or actions which modify risk. These may also be described as “barriers”.

Control environment
The combination of a suite of controls, (both prevention and mitigation) identified in a risk assessment to manage a risk.

Control weakening or escalation factor
A condition that leads to increased risk by defeating or reducing the effectiveness of a control. When being considered as part of an incident investigation these may also be described as "contributory factors".
Consequence
The outcome of an event affecting objectives.

Corporate Risk Management Plan
The Corporate Risk Management Plan details the risks to the achievement of the company's strategic and operational objectives. This includes the company risk profile, results of the risk assessments, key risk indicators and the treatment action plans.

Critical Control
The following are indicators that a control may be a critical control. This is not an absolute (yes/no) standard. All items are indicators of criticality, the more present, the higher the indication.

- The control is crucial to preventing or mitigating one or more severe consequence events.
- The control's absence or failure would significantly increase the likelihood of one or more severe consequence events occurring, despite the existence of other controls.
- The control's absence or failure would result in the residual risk rating being outside the Board's risk appetite.

Critical Risk
Any risk event with a severe consequence (residual).

Divisional Governance, Risk & Compliance (GRC) Representatives
The Executive Leadership Team nominated representative(s) that coordinates governance, risk and compliance related initiatives and reporting within each division.

Escalation factor
See control weakening factor.

Executive Leadership Team (ELT)
The Executive Leadership Team comprises the direct reports of the Chief Executive Officer other than the Executive Officer and the Executive Assistant to the CFO.

External context
The external environment in which the company seeks to achieve its objectives. External context may include:

- Political.
- Economic.
- Social.
- Technological.
- Environmental.
- Legal/regulatory.
- natural and competitive environment (whether international, national, regional or local).
- key drivers and trends having impact on the objectives of the company; and
- perceptions and values of external stakeholders.

Hazard
Source of potential harm.

Hazardous event
An event which has the potential to cause harm (i.e. loss or damage).

Hierarchy of controls
Elimination of a hazard is the most effective control and if this is not reasonably practicable to achieve, implementation of additional controls should be considered based upon their degree of effectiveness. This order is referred to as the hierarchy of controls and comprises elimination, substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.

Inherent risk
The inherent risk rating is based on the plausible worst case scenario assuming the absence of company established controls but with the presence of existing external controls such as regulations, road rules etc. and reliance on common sense.

Insurance
A contract in which the insurer agrees to compensate the insured (the company) for any losses or damages caused by risks identified in the contract.

Internal context
The internal environment in which the company seeks to achieve its objectives. Internal context may include:

- governance, organisational structure, roles and responsibilities.
- policies, objectives, and the strategies that are in place to achieve them.
- the capabilities, understood in terms of resources and knowledge e.g. capital, time, people, processes, systems and technologies.
- information systems, information flows and decision-making processes (both formal and informal.
- relationships with, and perceptions and values of internal stakeholders.
- the company's culture.
- standards, guidelines and models adopted by the company; and
- form and extent of contractual relationships.

Key Risk Indicator (KRI)
An indicator used to monitor the effectiveness of the control environment and can be either active (leading) or reactive (lagging). Active indicators measure variables that are believed to be precursors of future risk management performance. Reactive indicators measure historical, after-the-fact performance to show when the desired outcome (in terms of controls) has not been achieved.

Likelihood
Chance of something happening.

Network Fatal Risk
A hazardous event that has the potential to result in a permanent disability or fatality. Network Fatal Risks are those that can be described as low frequency, however high consequence and form a prioritised subset of operational risks.

Operational Risk
A hazardous event linked to day-to-day activities undertaken by the company.

Opportunity
A positive effect of uncertainty on objectives.

Positive risk culture
Is evident in a company when employees are aware of the company's activities, operations, and objectives; consider the opportunities and what can go wrong; and takes action to harness the opportunities and address the consequences.

Project Manager
The employee that leads a particular project and is responsible and accountable for completing the project on time and on budget in a safe and environmentally responsible manner.

Project/Program Sponsor
Manager or individual to whom the Project Manager is accountable.

Recordkeeping
Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information (Source: AS Records classification handbook – HB5031 – 2011).

Residual risk
The risk remaining after risk treatment. Also refers to the current level of risk taking into account the existing controls and their known level of effectiveness.

Risk
The effect of uncertainty on objectives.

Risk analysis
The process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk appetite
The amount and type of risk that the company is willing to pursue, retain, take or turn away from risk. Refer Board Policy: Governance: Risk Management CECP0002.03.

Risk assessment
The overall process of risk identification, risk analysis and risk evaluation.

Risk Category Nominated Lead
Generally, a Divisional GRC Representative or other employee that has been nominated by the Executive Leadership Team member to assist in the implementation of the Risk Management Framework. There may be more than one Risk Category Nominated Lead nominated per division. The Risk Category Nominated Lead supports the Risk Category Owner as required with Enterprise Risk Category reporting and the annual risk assessment refresh.

Risk Category Owner
The Executive Leadership Team member nominated by the Chief Executive Officer to have oversight of all hazardous events contained within an Enterprise Risk Category.

Risk evaluation
The process of comparing the results of the risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision making about the SFAIRP status and risk treatment.

Risk identification
The process for finding, recognising and describing risks.

Risk management
Coordinated activities to direct and control the company with regard to risk.

Risk Management Framework
The set of foundation documents and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the company.

Risk Management Plan
A document that formally collates the results of risk assessments related to a specific set of objectives. This includes the risk ratings, key risk indicators and treatment action plans for the reduction of risk to a tolerable level.

Risk management process
The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Strategic Plan
The Risk Management Strategic Plan details the initiatives aimed at strengthening system weaknesses identified through the monitoring and review of the Risk Management Framework. Implementation of the Risk Management Strategic Plan aims to embed continuous improvement in the Risk Management Framework and its application. Covering a three year period, the Risk Management Strategic Plan is reviewed and revised annually.

Risk Owner
A person with accountability or authority to manage a risk including by delivering the outcome or performing the function or delivering the performance that is impacted by the risk event. (For projects refer to the Project/Program Sponsor.)

Risk profile
The description of the company’s risks.

Risk register
A record of information about related identified hazardous events including descriptions, controls and risk ratings.

Risk treatment
The development and implementation of measures to modify risk. Defined in the Risk Management process as a Treatment Action Plan. Risk treatment measures may include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- taking or increasing risk in order to pursue an opportunity.
- removing the risk source.
- changing the likelihood.
- changing the consequences.
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

Risk tolerance
The company's readiness to accept a residual risk based on the effectiveness of the control environment or the planned risk treatment actions. A risk is deemed tolerable if it is considered to be:

- "So Far As Is Reasonably Practicable" (SFAIRP); or
- Non-SFAIRP with treatment action plans in place to move the risk to SFAIRP.

Risks that are Non-SFAIRP, with no Treatment Action Plan in place are considered intolerable.

Strategic Risk
A hazardous event either related to the development of the Corporate strategy or the delivery of initiatives contained in Strategic Plans.

So Far As is Reasonably Practicable (SFAIRP)
Core to this concept is "reasonably practicable". The objective is to eliminate risk. If it is not reasonably practicable to eliminate a risk, then it should be minimised to so far as is reasonably practicable (in accordance with the hierarchy of controls). SFAIRP is the level of risk that is tolerable and cannot be reduced further without the expenditure of cost, time and/or effort that is disproportionate to the benefit gained or where the solution is impractical to implement.

Subject Matter Expert
An individual with in-depth knowledge of the related business process/es.

Uncertainty
The state, even partial, of deficiency of information related to a future event, consequence or likelihood.

5.0 REFERENCES

Internal
Board Policy (Governance) – Governance – CECP0002
Board Policy (Governance) – Compliance – CECP0002.02
Board Policy (Governance) - Risk Management - CECP0002.03
Corporate Risk Matrix - CECG0002.21a
Company Procedure (Governance) - Risk Management - CEOP0002.21
Internal-External Stakeholder consultation and engagement form - CEOF0002.21b
Threat Barrier Tool - CEOF0002.21c
Corporate Risk Assessment Tool - CEOF0002.21d
Deep Dive Risk Assessment Tool - CEOF0002.21e
Single Page Risk Dashboard report - CEOF0002.21f
Business Resilience procedure - CEOP8078a
Network Value Framework - Quantifying the Cost of Consequence for Network Investments CECG1140
Health Safety and Environmental Manual Risk Management - CECM1000.02
Network Fatal Risk Control Standard CEOP0003.04

Cyber Security CECP2537
Information Security Risk Management CEOP2241

External
NSW Electricity Supply Act 1995; Electricity Supply Regulation (NSW) 2014
Work Health Safety Act 2011, Work Health Safety Regulation 2017
QLD Electricity Act 1994; Queensland Electrical Safety Act 2002 and associated Regulations
Australian Energy Sector Cyber Security Framework (ISO) 27001:2013 Information Security Management Systems
AS Records classification handbook – HB5031 – 2011
NSW Treasury Risk Management Toolkit for the NSW Public Sector (TPP12-03)
ISO 31000: 2018 Risk Management Principles & Guidelines IEC 31010:2019 - Risk management techniques
ISO 55001 Asset Management; ISO45001 OHS Management System ISO 14001 Environmental Management Systems
National Energy Retail Law (NSW); National Energy Retail Rules (NSW)
NSW and QLD Legislation, Parliament of Australia Bills
Australian Energy Regulator (AER) NSW Distribution determination
General Retention and Disposal Authority: Administrative Records GA28

6.0 RECORDKEEPING

The table below identifies the types of records relating to the process, their storage location and retention period.

Type of Record	Storage Location	Retention Period*
Risk Management Strategic Plan	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.14.01
Corporate Risk Management Plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Approved change requests to the Corporate Risk Management Plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Final version of bow-ties Threat-Barriers	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Final version of Risk Assessment spreadsheets	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Risk Management reports submitted to the RCSC	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.17.02

Risk Management reports submitted to the RCSC	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.17.02
Risk management plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Project risk management plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Change management risk assessment	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01

* The following retention periods are subject to change e.g. if the records are required for legal matters or legislative changes. Before disposal, retention periods should be checked and authorised by the 'Records Management Team'.

7.0 REVISIONS

Issue No.	Section	Details of changes in this revision	Change Risk Impact?
2	All	Minor amendment - Roles and responsibilities updated following the separation from Network NSW (NNSW).	Low
3	All	Minor amendment - Document updated due to recent structural changes.	High
4	All	Complete re-write	High

Annexure A – Internal/External Stakeholder consultation and engagement (CEOF0002.21b)

Stakeholder	Means of consultation or engagement	Stage(s) of engagement in Risk Management process	Method of consultation, communication and reporting	Any Specific procedures for statutory reporting obligations
Customer Advocacy Group	*Specific consultation meetings*	*Context, identification and treatment of risks to gain insight into planned public safety initiatives for all groups*	*Presentations Meetings / Consultation during PESAP which aligns with public safety FSA*	*Customer Advocacy Group charter*

Annexure B – Understanding controls as part of risk management

Risk Controls

Essential Energy establishes controls for foreseeable risks. However, Essential Energy recognises that risk controls cannot practically or cost effectively eliminate all possible risks.

Essential Energy strengthens existing controls and establishes additional controls where it is necessary, prudent, efficient and in the long-term interests of the community. Additional controls are considered reasonably practicable where they align to Essential Energy's strategic objectives and can be achieved within its resource constraints.

These decisions are supported by a detailed and robust assessment of alternative risk and control options, including removing or deferring controls that do not provide value for the community.

A consistent approach to risk and control design, planning, prioritisation, and optimisation is underpinned by:

- a common set of probability and financial values for all enterprise risks for use in risk assessment and optimisation; and
- a common set of optimisation tools at a portfolio and asset level and a risk and control level (including consequence differentiators and threat barrier diagrams).

Essential Energy reviews the effectiveness of risk controls based on:

- the mechanism by which the controls are intended to modify risks, both independently and collectively in relation to these risks.
- whether there are shortcomings, gaps or factors that reduce control effectiveness in both the design and operation of controls (both manual or automated).
- compliance with relevant legislation and regulations.
- relevant industry standards, emerging best practices, and established sound practices.
- the availability of alternative controls or insurance to mitigate risk impacts.
- relevant findings from internal and external reviews, risk assessments, reports, or investigations; and
- scenario analysis and organisational resilience to respond to changes in the external environment.

Table 7 – Control ratings - below summarises the aligned rating scale to be applied to each control.

Rating	Description
Effective	The control is designed, implemented and operating effectively
Partially effective	The control is not always and / or fully designed effectively or implemented effectively or operating effectively
Not Effective	The control is not designed effectively or not implemented effectively or not operating effectively.

Control effectiveness rating rationales should be supported by a full examination of applicable data including external data or benchmarking where relevant. For example, applicable data for safety incidents including information such as number of Incidents, Near Misses, and High Potential Incidents.

Hierarchy of control

Control effectiveness is measured against the '*Hierarchy of Control'* and the type of control implemented affects the residual risk outcome.

To determine what controls are needed, start above the red line at the top of the matrix.

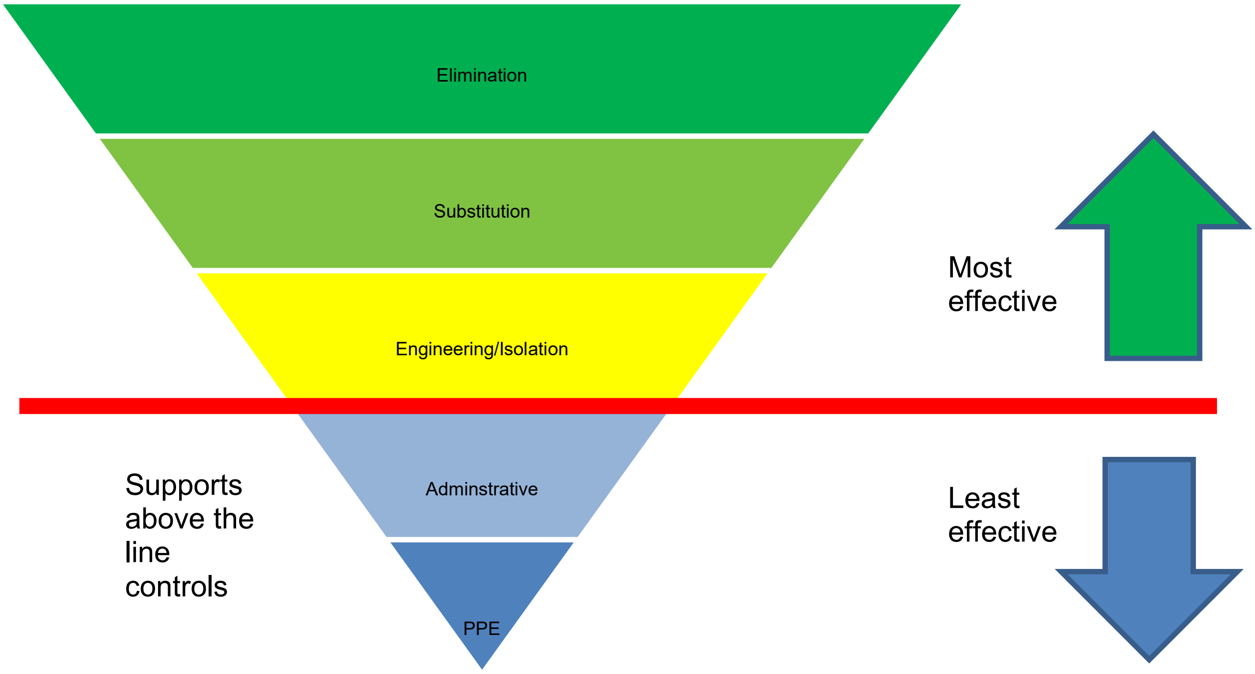


Figure 7 Hierarchy of control

You can **eliminate** risks by removing an existing hazard, for example,

- by removing trip hazards on the floor.
- disposing of unwanted chemicals, or
- not working in an isolated or remote area.

If it is not reasonably practicable to eliminate the hazards and associated risks, you must minimise the risks using one or more of the following approaches, so far as is reasonably practicable.

- **Substitute** - the hazard with something safer. For example – replace solvent-based paints with water-based ones.
- **Isolation** - means physically separating the source of harm from people by distance or using barriers or by isolating an energy source.
- **Engineering** - may include adding a guard to a piece of machinery or physical barrier to prevent access. Essential Energy has extended this concept to include systems as an Engineering solution that recognises it as a superior solution than an administration control
- **Administration** - controls include training a person to be competent in a task or operation. A procedure is also an administration control.
- **PPE** - is the least effective control and if often the last control to prevent you from harm. For example, when working on the network the usual controls are isolation, engineering, and procedures, with PPE (HV gloves) as the last barrier.

Control types

A control is something we do or implement to reduce risk.

Control types	***Explanation***
Control	Control measures include actions that can be taken to: • Remove the threat/hazard (elimination) from the Hierarchy of control. • Reduce the likelihood of exposure to that threat/hazard (preventative). • Reduce the consequences of exposure to the threat/hazard (mitigative). • Detect exception in the control environment.
Critical control	The following are *indicators* that a control may be a critical control. **This is not an absolute (yes/no) standard.** All items are indicators of criticality, the more present, the higher the indication. • The control is crucial to preventing or mitigating one or more severe consequence events. • The control's absence or failure would significantly increase the likelihood of one or more severe consequence events occurring, despite the existence of other controls. • The control's absence or failure would result in the residual risk rating being outside the Board's risk appetite
Interim control	• Control(s) that are put in place as a temporary measure whilst more robust controls are developed or sourced. • Must be reviewed as working at intervals determined by the residual risk level (refer to the Corporate Risk Matrix).

Table 8 – Control types

Critical controls must be identified for all risks with a residual risk of severe consequences. Critical controls must have control verifications added in the risk assessment and assigned to an appropriate person to verify control effectiveness and currency at the required intervals

Annexure C: Bow Tie / Threat-Barrier Tool (CEOF0002.21c)

On of the tools utilised as part of the CRMF is the Bow-Tie or Threat Barrier risk assessment methodology that centres on the identification of preventative and mitigation controls in the management of identified potential hazardous events.

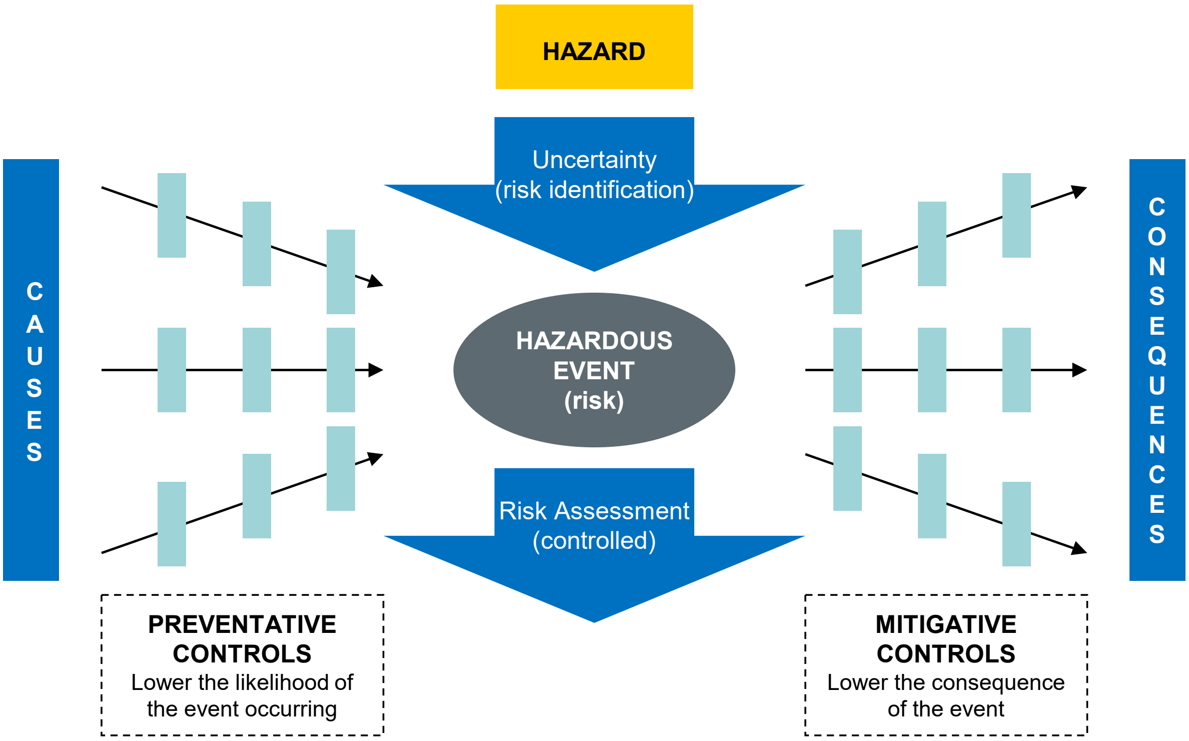
An example Bow-Tie is shown in **Figure 8**, clearly defining the links between the hazardous event, causes, consequences and controls. Controls will be defined as either preventative controls or mitigation controls. Bow-Tie diagrams will be developed/reviewed and updated in consultation with the Risk Owner to maintain integrity of the data and to manage version control.

The development of a Bow-Tie starts with the identification of uncertainty, hazards or a potential source of harm that will impact an objective. The uncertainty or hazard will then be characterised in the form of a hazardous event and placed at the centre of the Bow-Tie. The causes of the hazardous event will be identified and placed to the left, followed by the consequences on the right.

Pathways connecting the individual causes and consequences to the hazardous event will then be drawn, with the preventative and mitigation controls placed along each of the pathways, respectively. Control weakening or escalation factors may also be added to these controls to describe mechanisms that may reduce or defeat a control's effectiveness. Supporting controls may then be added to show how a control weakening may be detected or prevented.

For consistency, the Risk Owner will maintain the Bow-Tie/ Threat-Barrier diagrams.

Figure 8 – Bow-Tie diagram



Annexure D: Key Risk Indicators for Risk Management

The following Essential Energy Key Risk Indicators have been developed in line with the CRMF.

Key Risk Indicators (KRIs) within risk management plans, monitor:

- Progress with the implementation of controls and treatments.
- The effectiveness of treatments and controls post implementation.
- Signals that the validity of the risk assessment may be/has been impacted; and
- Timely review of existing risks.

Table 9 provides some examples of common KRIs. A set of common KRIs will be defined and monitored by Risk and/or Control Owner(s).

.

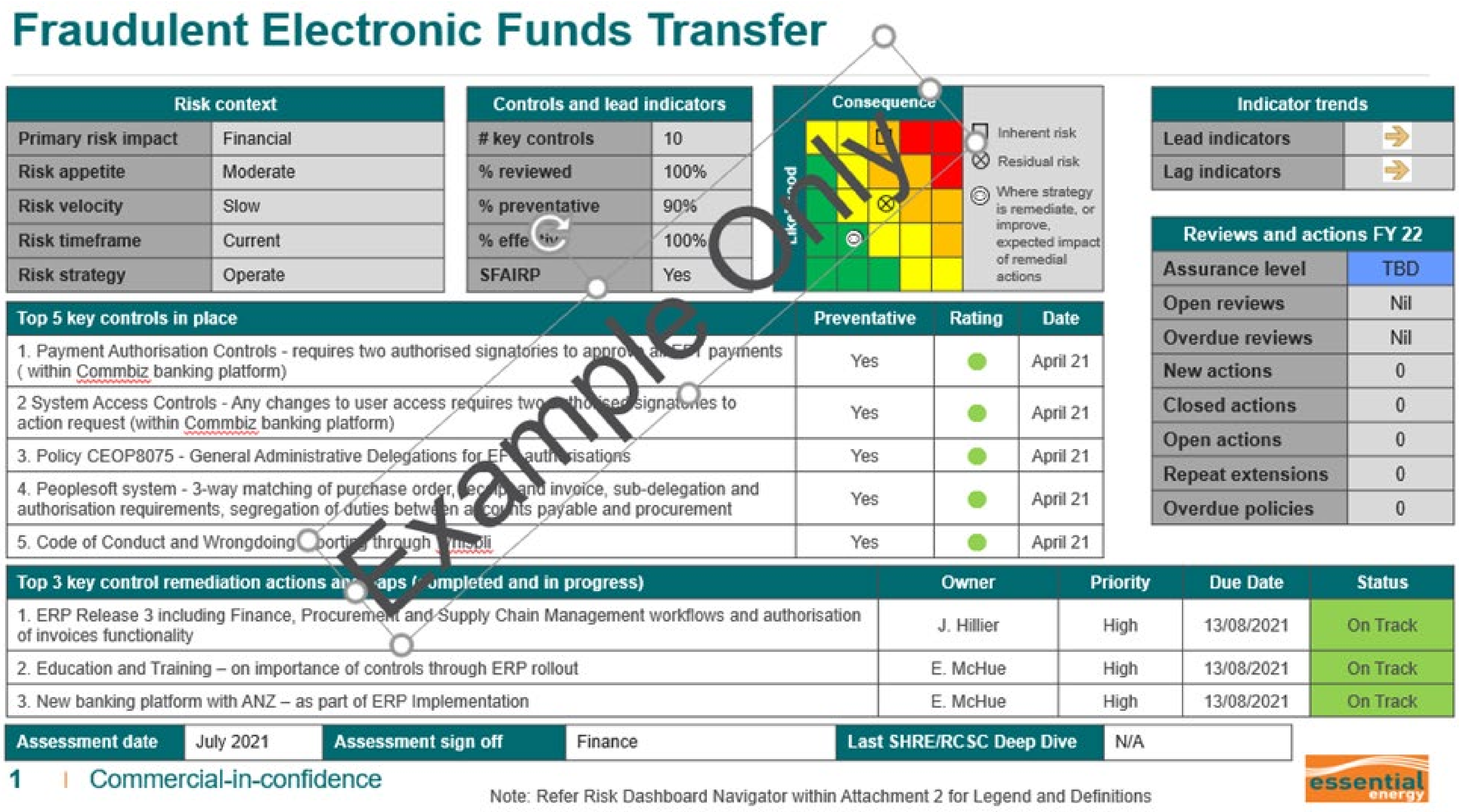
Table 9 also provides some examples of potential risk-specific KRIs. The Risk Owner is responsible for defining and monitoring risk-specific KRIs and reporting material changes to line management

Risks	Example Common KRIs	Example Risk-Specific KRIs
Controls and treatments are not implemented as agreed in Risk Management Plans	• 100% of critical controls and treatments implemented for network risks • 100% of controls and treatments implemented for network risks with 'High' residual risk rating or above • > 80% of controls and treatments implemented for network risks with 'Medium' residual risk rating or below	• 100% of critical controls and treatments implemented per risk management plan (schedule, cost, quality) • > 80% of controls and treatments implemented per risk management plan (schedule, cost, quality)
Controls and treatments are not effective	• 100% of critical controls and treatments are rated as 'Effective' • >80% of controls and treatments assessed as partially or fully ineffective have agreed action plans in place • Actual numbers of residual risk events resulting from implementation of the designed system of control are within defined tolerance of numbers expected/forecast from risk assessment • Actual type and severity of consequences resulting from implementation of the designed system of control are within defined tolerance of numbers expected/forecast from risk assessment • 100% of critical controls and treatments are effective for network risks	• 100% of critical controls are assessed as 'Effective' • >80% of controls and treatments assessed as partially or fully ineffective have agreed action plans in place • <= X unassisted asset failures per annum, as a result of the defined risk event • <= Y 'Moderate' network outages per annum, as a result of the defined risk event

Risks	Example Common KRIs	Example Risk-Specific KRIs
Key aspects of the risk environment, or underpinning assumptions are significantly changed and / or proven incorrect	• In-year environmental conditions are in line with long-term averages (bushfire danger, storm conditions) • Change in regulatory requirements, including compliance criteria / definition of a 'breach' • Material and widespread change in outage response capability	• Change in relative frequency of risk-specific causal factors • Changes to the design of existing critical controls or implementation of new critical controls
Risk assessments are not reviewed to ensure continued relevance	• 100% of time-based reviews for network risks with 'High' residual risk rating or above are competed on time • 80% of time-based reviews for network risks with 'Medium' residual risk rating or below are completed on time	• Time-based triggers for risk reviews defined and acted upon • Event-based triggers for risk reviews defined and acted upon

Table 9 – Key Risk Indicators

Annexure E: Single Page Risk Dashboard (CEOF0002.21f)



Fraudulent Electronic Funds Transfer

Risk context	
Primary risk impact	Financial
Risk appetite	Moderate
Risk velocity	Slow
Risk timeframe	Current
Risk strategy	Operate

Controls and lead indicators	
# key controls	10
% reviewed	100%
% preventative	90%
% effective	100%
SFAIRP	Yes

Inherent risk

Residual risk

Where strategy is remediate, or improve, expected impact of remedial actions

Indicator trends	
Lead indicators	→
Lag indicators	→

Top 5 key controls in place	Preventative	Rating	Date
1. Payment Authorisation Controls - requires two authorised signatories to approve all EFT payments (within Commbiz banking platform)	Yes	●	April 21
2 System Access Controls - Any changes to user access requires two authorised signatures to action request (within Commbiz banking platform)	Yes	●	April 21
3. Policy CEOP8075 - General Administrative Delegations for EFT authorisations	Yes	●	April 21
4. Peoplesoft system - 3-way matching of purchase order, receipt and invoice, sub-delegation and authorisation requirements, segregation of duties between accounts payable and procurement	Yes	●	April 21
5. Code of Conduct and Wrongdoing reporting through Whispli	Yes	●	April 21

Reviews and actions FY 22	
Assurance level	TBD
Open reviews	Nil
Overdue reviews	Nil
New actions	0
Closed actions	0
Open actions	0
Repeat extensions	0
Overdue policies	0

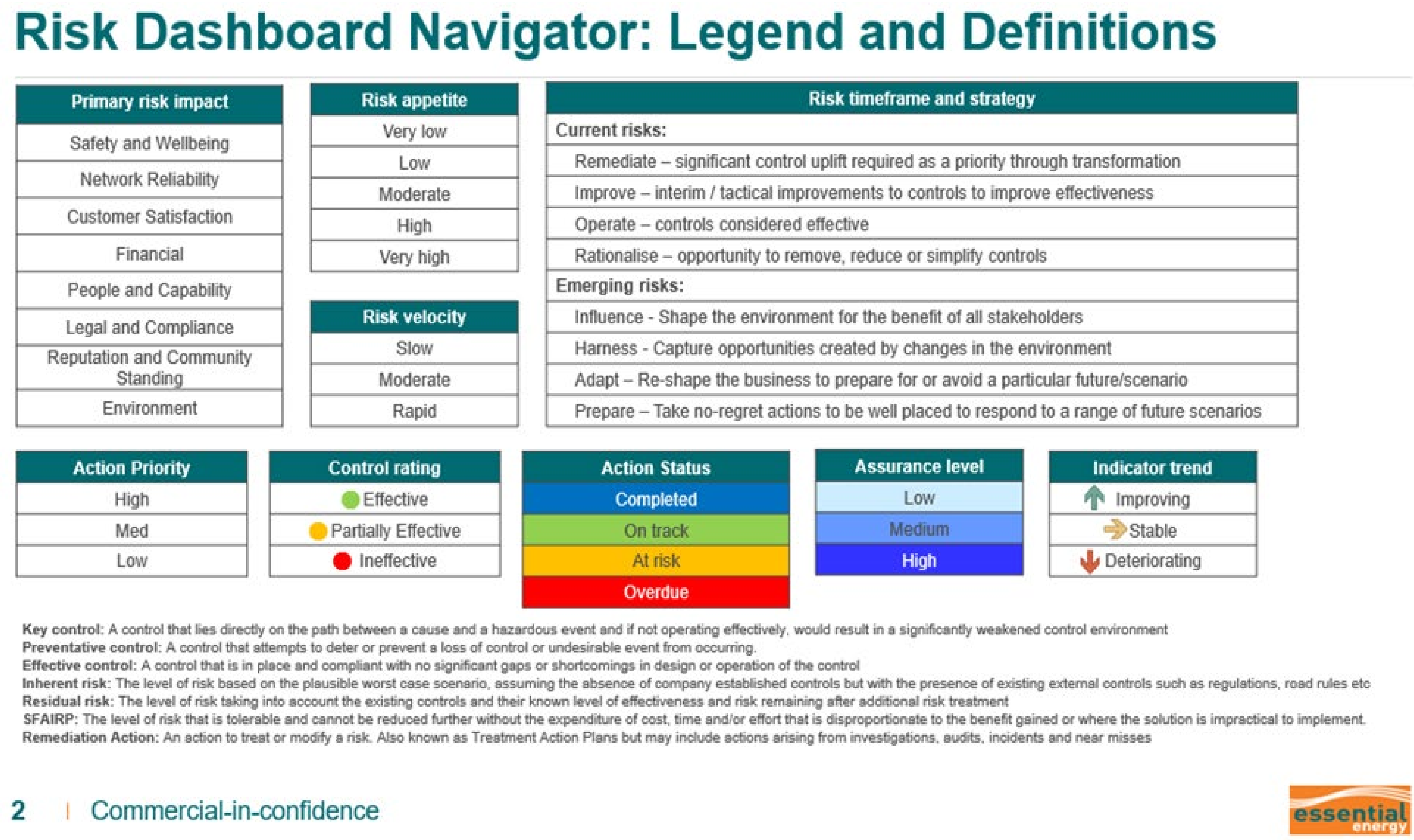
Top 3 key control remediation actions and gaps (completed and in progress)	Owner	Priority	Due Date	Status
1. ERP Release 3 including Finance, Procurement and Supply Chain Management workflows and authorisation of invoices functionality	J. Hillier	High	13/08/2021	On Track
2. Education and Training – on importance of controls through ERP rollout	E. McHue	High	13/08/2021	On Track
3. New banking platform with ANZ – as part of ERP Implementation	E. McHue	High	13/08/2021	On Track

Assessment date	July 2021	Assessment sign off	Finance	Last SHRE/RCSC Deep Dive	N/A

1 | Commercial-in-confidence

Note: Refer Risk Dashboard Navigator within Attachment 2 for Legend and Definitions

essential energy



Risk Dashboard Navigator: Legend and Definitions

Primary risk impact
Safety and Wellbeing
Network Reliability
Customer Satisfaction
Financial
People and Capability
Legal and Compliance
Reputation and Community Standing
Environment

Risk appetite
Very low
Low
Moderate
High
Very high

Risk velocity
Slow
Moderate
Rapid

Risk timeframe and strategy
Current risks:
Remediate – significant control uplift required as a priority through transformation
Improve – interim / tactical improvements to controls to improve effectiveness
Operate – controls considered effective
Rationalise – opportunity to remove, reduce or simplify controls
Emerging risks:
Influence - Shape the environment for the benefit of all stakeholders
Harness - Capture opportunities created by changes in the environment
Adapt – Re-shape the business to prepare for or avoid a particular future/scenario
Prepare – Take no-regret actions to be well placed to respond to a range of future scenarios

Action Priority
High
Med
Low

Control rating
🟢 Effective
🟡 Partially Effective
🔴 Ineffective

Action Status
Completed
On track
At risk
Overdue

Assurance level
Low
Medium
High

Indicator trend
↑ Improving
→ Stable
↓ Deteriorating

Key control: A control that lies directly on the path between a cause and a hazardous event and if not operating effectively, would result in a significantly weakened control environment
Preventative control: A control that attempts to deter or prevent a loss of control or undesirable event from occurring.
Effective control: A control that is in place and compliant with no significant gaps or shortcomings in design or operation of the control
Inherent risk: The level of risk based on the plausible worst case scenario, assuming the absence of company established controls but with the presence of existing external controls such as regulations, road rules etc
Residual risk: The level of risk taking into account the existing controls and their known level of effectiveness and risk remaining after additional risk treatment
SFAIRP: The level of risk that is tolerable and cannot be reduced further without the expenditure of cost, time and/or effort that is disproportionate to the benefit gained or where the solution is impractical to implement.
Remediation Action: An action to treat or modify a risk. Also known as Treatment Action Plans but may include actions arising from investigations, audits, incidents and near misses

2 | Commercial-in-confidence

essential energy

Annexure F - Risk Assessment Schedule

Enterprise Risk area	Owner	Inherent Risk	Residual Risk	Qtr 1	Qtr 2	Qtr 3	Qtr 4
Worker Safety	CHRO						
Public Safety	CHRO						
Environmental contamination or damage	CHRO						
Lack of key employees / skills	CHRO						
Electrical distribution network outage or instability	COO						
Major fire caused by network or network activity	COO						
Water services unable to meet demand or quality standards	COO						
Unauthorised control of the power network	CIO						
Unavailability of critical IT/OT and communication systems and data	CIO						
Unavailability of critical suppliers/supplies	CCO						
Failure to deliver agreed service levels	CCO						
Failure to deliver forecast financial performance	CCO						
Failure to accurately report financial performance	CCO						
Damage or loss caused to third parties (excluding personal injury and bushfire)	GCCS						
Non-compliance with obligations and standards	GCCS						
Corrupt conduct by an employee, consultant or contractor	GCCS						
Loss of, damage to or theft of Essential Energy assets	GCCS						
Ineffective incident response (including reputational incidents)	GCCS						
Failure to engage stakeholders and operate in line with community expectations	SRCA						
Publication of incorrect non-financial information	SRCA						
Failure to develop and/or deliver strategic plans and initiatives (including benefits)	SRCA						