Procedure No:	CS-RISK-01
TRIM Ref No:	B/D/12/63934
Reviewed:	06/23
Amended:	06/23
Review Due:	06/25

CS ENERGY STANDARD

ENTERPRISE RISK AND COMPLIANCE MANAGEMENT FRAMEWORK
CS-RISK-01

Responsible Officer: Senior Governance Risk and Compliance Advisor
Responsible Manager: Head of Risk Compliance and Assurance
Responsible Executive: Executive General Manager Corporate Services

DOCUMENT HISTORY

Key Changes	Prepared By	Checked By	Approved By	Date
Initial Release	R Roome			April 2011
Amended document as reviewed by Executive Management.	R Roome			April 2012
Document finalised and approved by EMT, Friday 8 June 2012, RCC12-06D1	R Roome			June 2012
Complete re-write for clarity and to align with new business strategy.	B Jardine	A Brown	B Green (interim for implementation)	June 2013
Updates following Risk Committee 22 July 2013 and 29 August 2013 Board. Safety Severe consequence level removed.	B Jardine	Risk Committee Internal Audit	Board	29/08/2013
Re-write to include focus on risk capacity, appetite and tolerance and expand Framework to include compliance.	J Rudd	A Varvari	Audit and Risk Committee	21/10/2014
Updated to include final version of Risk Matrix (B/D/13/17881).	J Rudd	K Hawker	K Hawker	19/03/2015
Updated Risk Categories.	J Rudd	K Hawker	A Varvari	14/08/2015
Updated Risk Categories.	PWC R Chibba	B Hopsick	A Varvari	17/12/2018
Updates to risk categories, tiers, evaluation, review, appetite, tolerance, controls, facilitator's role, reporting and obligations.	RCA Team	S Wells J Rudd	ERC	29/05/2021
Changes to address WHSQ Audit recommendations	B Hopsick	S Wells R Chibba	A Varvari	14/06/2023

CONTENTS

1 PURPOSE AND SCOPE

1.1 Purpose

The purpose of risk and compliance management is to support CS Energy's strategy through understanding and controlling uncertainties, and ensuring compliance with legal, regulatory and other obligations.

The purpose of this Enterprise Risk and Compliance Management Framework document (**Framework**) is to:

- Implement CS Energy's risk and compliance management requirements as established by the Governance, Risk and Compliance Policy (GRC Policy1);
- Describe how CS Energy undertakes risk management and ensures compliance across business activities in an integrated fashion;
- Facilitate the implementation of robust practices for the effective management of risk and compliance;
- Outline the activities designed to foster a culture of active risk management and compliance throughout the organisation;
- Demonstrate the Board and Management's commitment to ensuring risks are adequately managed and compliance requirements are met; and
- Define the accountabilities and responsibilities of the Board and employees.

1.2 Scope

This Framework applies to all CS Energy Directors and employees. The Framework details how risk and compliance management is implemented across all activities at CS Energy.

CS Energy has adopted;

- International standard ISO 31000:2018 Risk Management – Principles and Guidelines ("ISO31000") and
- Australian standard AS19600-2015 Compliance Management – Guidelines ("ISO 19600"), in the design of this Framework.

2 PRINCIPLES

This risk management Framework is based on the following key principles, in accordance with ISO31000:

a. Integrated

Risk management is an integral part of all organisational activities.

b. Structured and comprehensive

A structured and comprehensive approach to risk management contributes to consistent and comparable results.

[1] TRIM - B/D/11/39708

c. Customised

The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.

d. Inclusive

Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e. Dynamic

Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f. Best available information

The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g. Human and cultural factors

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h. Continual Improvement

Risk management is continually improved through learning and experience.

3 OVERVIEW

CS Energy requires a robust risk and compliance framework that enables it to effectively manage organisational risks and compliance requirements by applying a consistent and integrated risk and compliance (**R&C**) approach. This Framework outlines:

- CS Energy's capacity, appetite and tolerance for risk;
- The process for risk identification and analysis;
- How risk methodology is aligned with operational and strategic decision making;
- Methods for developing appropriate levels of engagement in risk and compliance across the business; and
- How compliance risks will be managed effectively.

The risk and compliance framework for CS Energy must be capable of supporting the activities of the business while managing significant financial constraints and the limited capacity to take on risk.

3.1 Risk and compliance definition

3.1.1 Risk

'Risk' is defined in AS/NZS ISO31000 as the '*effect of uncertainty on objectives*'. Uncertainty may be the result of an event, a change in circumstances, an ambiguity or a lack of information. To ensure that CS Energy achieves its objectives by maximising opportunities and minimising threats to shareholder value, risk management must be applied in all decision-making processes in order to manage uncertainty and its impacts on the organisation. Risk can refer to both opportunities and threats,

depending on whether the potential impact is positive or negative, and can include financial loss or gain, injury to people, business interruption and reputational damage.

3.1.2 Compliance

'Compliance' is defined in ISO19600:2015 as 'meeting all the organisation's compliance obligations'.

The key elements to a successful compliance program are commitment, implementation, monitoring and measuring, and continual improvement.

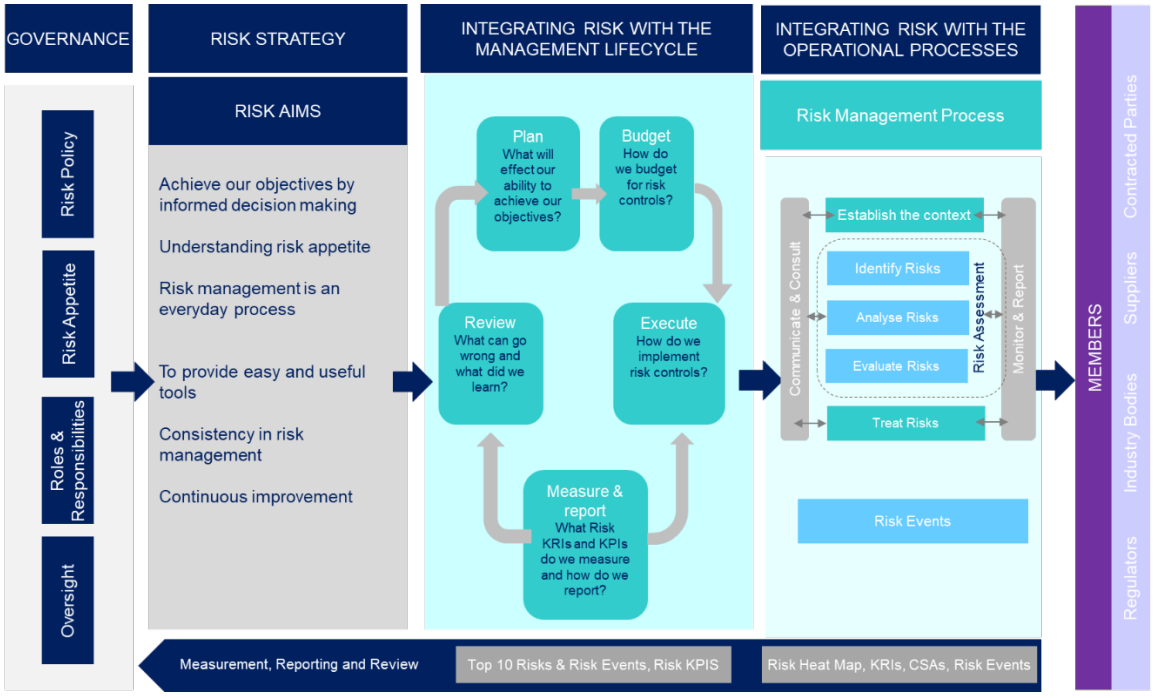
Refer to Section 12 Definitions for a glossary of the key terms used throughout this Framework.

3.2 Framework structure

To support effective risk and compliance outcomes, the Framework outlines the core elements required to deliver robust risk data and risk management outcomes.

3.2.1 Risk

CS Energy's approach to Risk Management is aligned with the below diagram and is described in more detail in Sections 5 and 6 and throughout this document.



3.2.2 Compliance

CS Energy's approach to Compliance Management is set out in Section 7 and throughout this document.

3.3 Risk categories

The Framework incorporates the full breadth of risks across the organisation, which align with the categories in CS Energy's risk system, Insight:

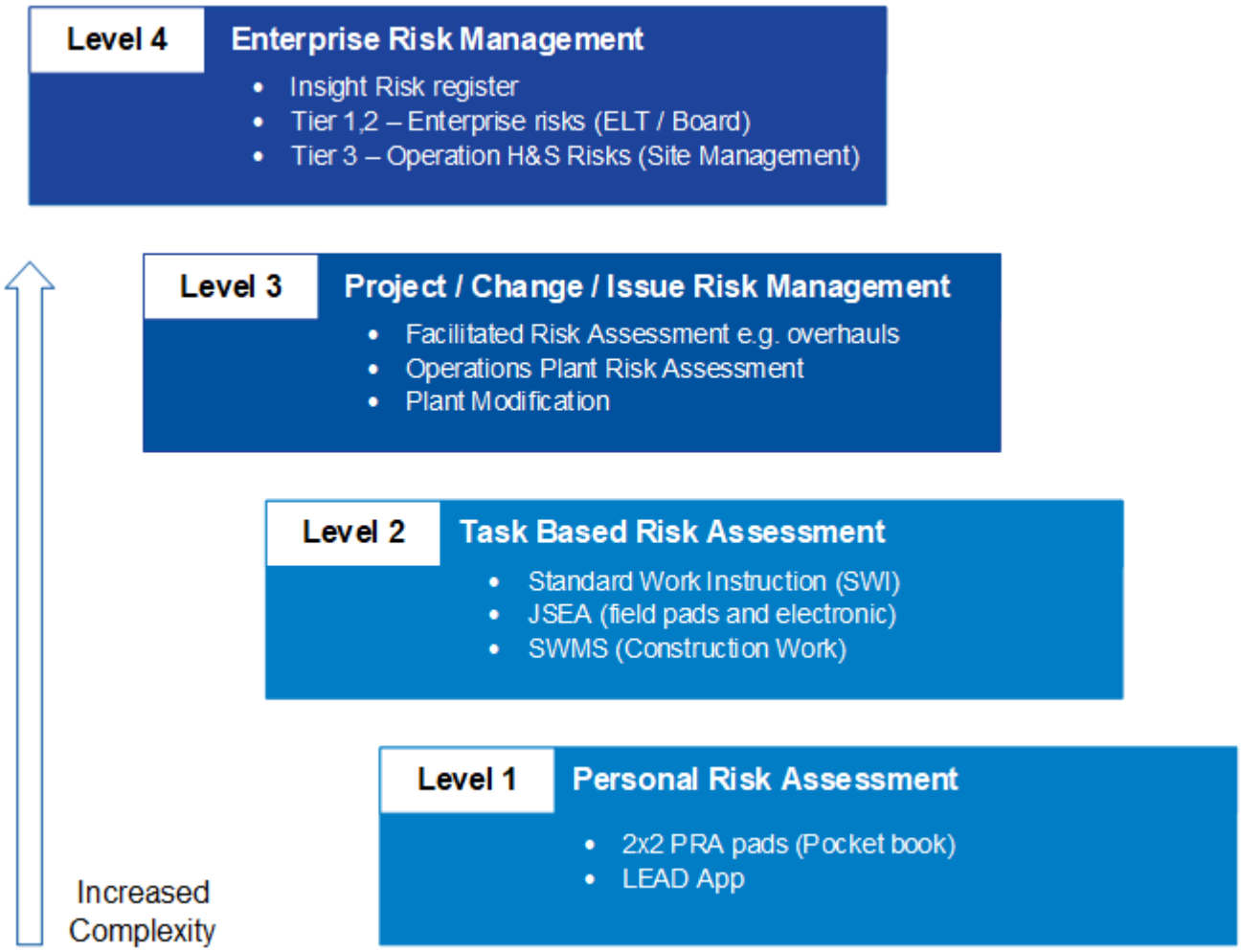
Category	Description	Managed By
Health, safety and security	Includes Serious Injury and Fatality (SIF) risks and Major Accident Hazard (MAH) risks, which are managed in accordance with the Health and Safety Handbook. Also includes other identified risks relating to health and safety of workers and site security.	Health and Safety in conjunction with Asset Management and Site Managers
Environment	Environment risks relate to the potential for environmental harm and are identified and managed in accordance with the Environmental Management System.	Environment in conjunction with Site Managers
Strategic	Strategic risks are related to CS Energy's strategic intent and how well it is executed. These risks are reviewed in conjunction with the annual business planning cycle or during periodic reforecasting / business change initiatives to inform and align with the business planning process and CS Energy strategy.	Executive General Managers
People and culture	People and culture risks relate to CS Energy's commitment to attract, develop and retain the best talent necessary to meet its strategic objectives, in pursuit of the creation of a safe, constructive and high performing culture.	Corporate Services
Loss of availability	Loss of availability (LOA) risks relate to CS Energy's assets and whether budgeted targets for commercial availability will be met.	Asset Management in conjunction with Plant Operations
Trading	Trading risks specifically relate to the sale and purchase of electricity are governed by the application of the Market Risk Policy (CS-RISK-02) and include market risk, credit risk, liquidity risk and operational risk (including legal and compliance risk). In addition to market risk, CS Energy is exposed to a range of other trading related risks including fuel price risk, interest rate risk and foreign exchange risk.	Trading and Analytics
Financial	Financial risks can be defined as the uncertainties and untapped opportunities embedded in the management of CS Energy's financial position whilst complying with regulations.	Finance, Energy and Financial Risk
Stakeholder relations and reputation	Stakeholder and reputation risks are related to the management of CS Energy's relationships and reputation with its stakeholders; these include shareholders, government departments, local communities in which CS Energy operates, contractors and regulators.	Managed by the owner of the relationship with support from Corporate Affairs
Legal and regulatory	Legal and regulatory risks specifically relate to CS Energy's ability to maintain its 'Licence to Operate' through compliance with the laws and regulations relevant to its business.	Managed by the relevant business unit with support from Legal
Technology	Technology risks are associated with the use, ownership, operation, involvement, influence and adoption of operational technology (OT) and information technology (IT) within CS Energy.	ICT (IT risks), Engineering (OT risks)

Category	Description	Managed By
Governance	Governance risks relate to the management of enterprise-wide operations and include the enterprise risk framework, fraud, insurance, and business resilience.	Managed by the relevant business unit with support from the R&C Team
Major projects	Projects, including capital projects and overhauls require a risk-based approach ensuring capital expenditure is aligned to key risks across the organisation. Longer term projects and high-level capital / project risks may be elevated to Insight where appropriate.	Managed by the relevant business unit with support from Projects

Note: risks related to the failure of management systems (i.e. a set of policies/procedures to manage risk for a particular area of enterprise-wide operations, e.g. inventory, contractor management, work management) are not captured as these systems are controls for other risks and are generally tracked in dashboards.

3.4 Risk tiers

CS Energy adopts four levels of health and safety risk evaluation to ensure risks are managed so far as reasonably practicable (refer to Health and safety risk management procedure CS-OHS-76). The diagram below outlines the four levels of risk evaluation.

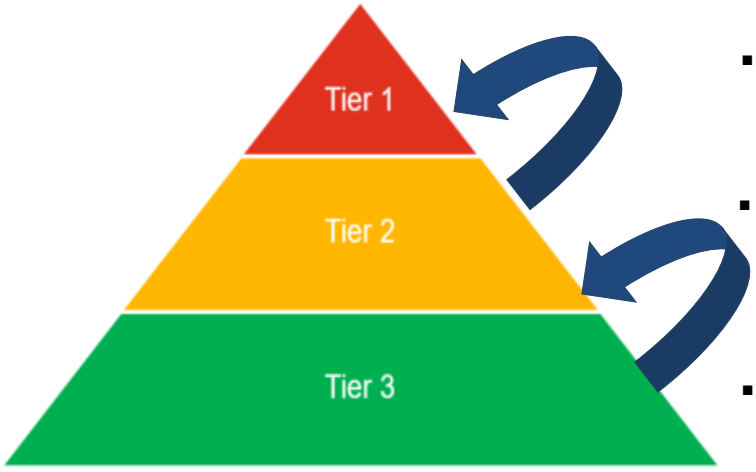


When considering Level 4 (Enterprise Risk Management), CS Energy has a three-tiered risk hierarchy. See below diagram for the description of each risk tier and the escalation process.

Level 4 Safety Risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011. The three procedures that outline the process for evaluating and managing Safety Risks in more detail include:

- CS-OHS-76 Health and Safety Risk Management
- CS-OHS-77 Serious Injury and Fatality Procedure
- CS-PSM-00 Process Safety and Operational Integrity Management

Serious Injury and Fatality Risks and Process Safety Risks are recorded in the CGR Insight system and the risks are managed consistent with the WHS Act and Regulations 2011 and as outlined in the applicable procedures noted above.



- Escalated risks from Tier 2, representing the level of information for ELT / ERC / Board
- 'Significant' and 'High' Tier 3 risks are escalated to Tier 2 level to provide the level of information the EGM and direct reports require to make decisions
- Operational view of risks for front line management and staff

CS Energy Risk Register Hierarchy				
Name	**Description**	**Risk reporting level**	**Risks captured in Insight**	**Risk tier escalation process**
Tier 1 Risks **CS Energy Group risk register**	Highest level enterprise risks for CS Energy Content is informed by Tier 2 risks (see below)	ELT Enterprise Risk Committee Board	All Tier 1 risks	Not applicable. Tier 1 risk information & ratings are based on the highest of the linked Tier 2 risks (below).
Tier 2 Risks **Site/Functional risk registers**	Material risks for each site or functional area	EGMs Heads of Department Site General Managers	All Tier 2 risks	Tier 2 risk information (including causes, consequences, ratings and controls) is escalated to the applicable Tier 1 risk.

CS Energy Risk Register Hierarchy				
Name	**Description**	**Risk reporting level**	**Risks captured in Insight**	**Risk tier escalation process**
Tier 3 Risks **Operational risk registers**	Operational risks typically at a site level	Front Line Management Employees	'Significant' or 'High' Tier 3 risks	Tier 3 risk information (including causes, consequences, ratings and controls) is escalated to the applicable Tier 2 risk. Tier 3 risk information may also inform the Tier 1 risks where no applicable Tier 2 risk is recorded.

3.5 Risk and Compliance Strategy

A separate Risk and Compliance Strategy document supports this Framework and outlines R&C's:

- Function;
- Role and services;
- Linkage of activities to CSE's strategic priorities;
- Success criteria.

It is supported by a detailed Strategic Plan that covers the forward-looking period.

The Strategy document aligns with this Framework and the Finance Risk Assurance Committee (FRAC Charter, and will be reviewed annually and approved by the FRAC.

4 RESPONSIBILITIES AND ACCOUNTABILITIES

4.1 Board

The Board has approved the GRC Policy in which it acknowledges the following responsibilities:

- Setting objectives for CS Energy;
- Delegating authority, setting limits of acceptable behaviour through the Code of Conduct and defining risk capacity, appetite and tolerance by approving CS Energy Policies;
- Establishing and monitoring effective risk and compliance;
- Approving the Risk Appetite Statement and ensuring that CS Energy's risks are managed within this appetite.

The Board may discharge some of these accountabilities through the Board Committees as described in the relevant Committee Charter.

4.2 Finance Risk Assurance Committee

The FRAC has responsibility for:

- Approving and overseeing the operation, management and implementation of the GRC Policy and the Enterprise Risk and Compliance Management Framework;
- Reporting to the Board at least annually as to the adequacy, appropriateness and effectiveness of CS Energy's risk and compliance management;

- Reviewing reports from Management on the effectiveness of risk and compliance management and any material breakdown of internal controls (including incidents of fraud); and
- Ensuring that Management has implemented and is providing appropriate oversight of CS Energy's legal and regulatory compliance processes, including any current legal proceedings.

4.3 Chief Executive Officer

The Chief Executive Officer (**CEO**) has overall accountability for risk and compliance management within CS Energy, including:

- Demonstrating commitment to ensuring CS Energy actively identifies, escalates and manages risks and compliance requirements, promoting a culture of active risk management and compliance throughout the organisation;
- Ensuring that appropriate frameworks are in place to effectively manage and report on risk and compliance;
- Leading the Executive Leadership Team in the delivery of its risk management and compliance responsibilities, including the management of CS Energy's strategic and high risks; and
- The final signoff of all information presented to the Board and Board Committees.

4.4 Executive Leadership Team

Each member of the Executive Leadership Team (**ELT**) is responsible for oversight of the risks and compliance requirements and obligations within their Division, and collectively the ELT is ultimately responsible for managing risks within the organisational risk appetite parameters and ensuring that CS Energy complies with its legal, regulatory and other obligations.

Members of the ELT are responsible for:

- Demonstrating commitment to ensuring CS Energy actively identifies, escalates and manages risks and compliance requirements, promoting a culture of active risk management and compliance throughout the organisation;
- Demonstrating the practice of risk management by applying risk decisions when developing strategy, making operational decisions and assessing changes in the business environment;
- Broadly understanding key risk issues affecting CS Energy and ensuring these are understood by key decision-makers within their area of responsibility;
- Working collaboratively with the R&C Team to ensure risks are appropriately identified, managed, monitored, recorded and reported;
- Ensuring risk and compliance management within their area of responsibility is undertaken in accordance with this Framework. This includes regularly reviewing the objectives of their area of responsibility to identify and assess risk, including the identification of appropriate controls and treatment actions;
- Ensuring that risk management and compliance information presented to the Board is timely, accurate and complete, and provided with relevant context to allow the Board to understand and interpret the information;
- Delegating the ownership of risks, controls and compliance obligations to employees with appropriate experience and expertise;

- Completing and signing off the quarterly Compliance Checklists (refer to Section 7.3 Compliance Checklists);
- Ensuring compliance failures are promptly identified, investigated, reported and addressed (including any appropriate disciplinary action); and
- Ensuring the appropriate number of employees with relevant experience and expertise are appointed as Risk and Compliance Facilitators and are supported in the execution of this role (or delegating this responsibility to a direct report).

4.5 Risk and Compliance Team (R&C Team)

The R&C Team is responsible for:

- Providing expert advice and support in relation to risk and compliance management, including effective ways to manage and control risk and to assist the business in making risk-focussed decisions;
- Engaging the business in the effective management of risk to enable the development and maintenance of data that facilitates a risk-based approach to all key business decisions;
- Facilitate processes that promote a culture of active risk management and compliance;
- Coordinating a consistent approach to the identification, escalation and management of risk and compliance requirements, reporting processes and the integration of risk in project and capital decision-making documentation;
- Reporting to the ERC on risks including risk and compliance issues and breaches;
- Overseeing processes for the management and resolution of risk and compliance issues and breaches;
- Supporting the business to identify changes to legislation, regulations or other applicable standards and update policies and procedures to ensure compliance is maintained;
- Acting as system owner of the system that maintains risk and compliance information (Insight);
- Training and supporting Risk and Compliance Facilitators to ensure they understand the objectives, risks, controls and compliance obligations that relate to their role and activities; and
- The review and continuous improvement of this Framework and risk management and compliance across CS Energy.

4.6 Risk Owners / Obligation Owners

Risk Owners and Obligation Owners have the following responsibilities within their site/function:

- Working collaboratively with R&C Team to ensure this framework is implemented appropriately;
- Ensuring that employees and contractors working in their area understand and conform with this Framework;
- Regularly reviewing the objectives of their area of responsibility to identify and assess risk, including the identification of appropriate controls and treatment actions;
- Monitoring existing controls to verify their effectiveness in managing the risk and liaising with control owners to ensure that any control weaknesses are addressed;
- Appointing Action Owners to implement risk treatment plans;

- Where delegated by their Executive General Manager, ensuring the appropriate number of employees with relevant experience and expertise are appointed as Risk and Compliance Facilitators, and are supported in the execution of this role;
- Recording and maintaining risks and compliance obligations in the appropriate Register;
- Assisting with completion of the quarterly Compliance Checklist process;
- Identifying new compliance obligations and assigning responsibility for completion;
- Ensuring risk management and compliance training is up-to-date and delivered to relevant employees in a timely fashion; and
- Ensuring policies, standards, procedures and forms are reviewed as per the review schedule and aligned with compliance obligations where applicable.

4.7 Risk and Compliance Facilitators

Risk and Compliance Facilitators are appointed by their Manager to facilitate the execution of the Manager's risk management and compliance responsibilities. Risk and Compliance Facilitators are responsible for:

- Assist in coordination of the quarterly Compliance Checklist process;
- Enter rectification plans for Compliance Checklist non-compliances into Insight;
- In conjunction with the Risk and Compliance team, provide Insight training to people on site / in business unit and help them understand their risk and compliance accountabilities/responsibilities;
- Provide onsite support for Insight where requested;
- Follow up overdue actions and risk reviews for relevant site/business unit;
- Update Owners of risks in system as required based on staff movements;
- Assist the Risk / Obligation Owner in entering data in system if required;
- Produce regular reports for Management;
- In conjunction with the R&C Team, assist in the facilitation of risk workshops where requested;
- Working collaboratively with the R&C Team and management within their division to promote effective risk and compliance management; Identify / maintain obligation sources, obligations and obligation actions; and
- Enter internal reviews and external assurance reviews and related actions into Insight.

4.8 Control Owners

Each control in Insight is assigned a Control Owner, and each compliance requirement is assigned a Responsible Person. These roles are responsible for ensuring the following:

- Embedding the control or compliance requirement in policies, standards, procedures, forms and training where required;
- For a control, that it is suitable for mitigating the risks to which it is assigned and is effective to the level described in the risk register, and that control enhancements that impact the Residual Risk Rating are communicated clearly to the Risk Owner;
- Assisting in the establishment of monitoring activities for the control or compliance requirement;

- The control or compliance requirement is reviewed at least annually;
- Ensuring information in the relevant Registers is timely, correct and complete;
- Assisting with completion of the quarterly Compliance Checklist;
- Reporting breaches or issues in line with the relevant breach or incident reporting procedure; and
- If circumstances arise where they can no longer effectively manage the control or compliance requirement, that this is escalated to the Risk Owner or Manager accountable for the compliance requirement.

4.9 Action Owners

Each action in Insight is assigned an Action Owner by the Risk or Control Owner. These roles are responsible for ensuring that:

- For an action, that it is suitable for mitigating the risks to which it is assigned, that it is reviewed on a regular basis, and that completed actions that impact the Residual Risk Rating are communicated clearly to the Risk or Control Owner;
- Performing or coordinating the performance of the action or compliance obligation by its due date;
- Updating the Registers to record the progress and completion of actions and obligation notifications in a timely, accurate and complete manner;
- Recording and escalating any exceptions where the action or compliance obligation has not been completed within the required timeframe; and
- If circumstances arise where they can no longer effectively manage the action or compliance obligations, that this is escalated to the Risk or Control Owner or Manager accountable for the compliance requirement.

4.10 Legal

The Legal team is responsible for:

- Conducting a periodic review of compliance manuals and maintaining those documents as required;
- Maintaining and operating the Complaints & Investigation Handling Standard (Official Misconduct, Public Interest and Protected Disclosure) as varied from time to time, including the Whistleblower Hotline;
- Working collaboratively with R&C Team to promote and administer effective compliance management.

4.11 Assurance

Assurance is responsible for:

- Designing an annual risk-based Assurance Plan using information from Insight;
- Examining compliance as part of planned reviews where relevant; and
- Reviewing risks and associated controls during scheduled reviews and reporting on the effectiveness of controls in mitigating risks to the Board (or its Committees according to the Committee Charters) and Management.

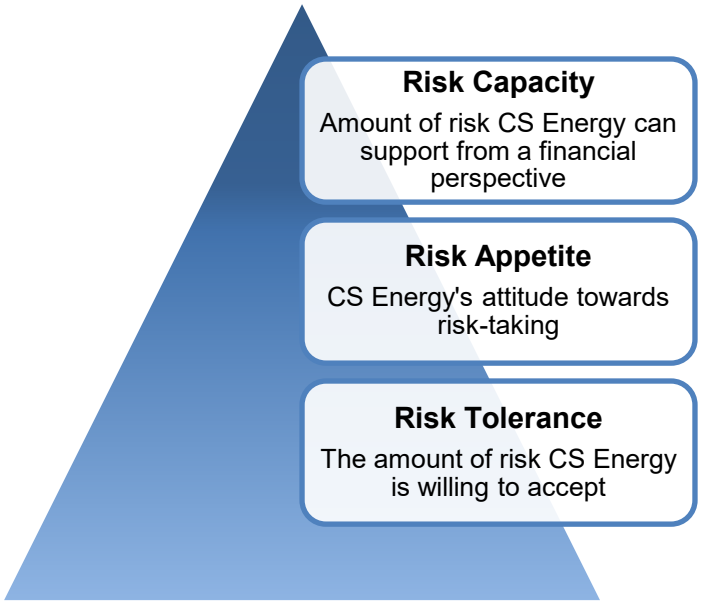
4.12 Employees / Contractors

In addition to any other responsibilities under this Framework, all employees, including contractors, are responsible for:

- Understanding the objectives, risks, controls and compliance obligations that relate to their role and activities;
- Participating in the risk management and compliance processes relevant to their roles;
- Undertaking activities within the risk tolerance of CS Energy (as expressed in policies) and in compliance with legal, regulatory and other obligations, policies, procedures and standards;
- Reporting new risks, risk issues, compliance requirements and obligations, breaches and weaknesses of controls to their Manager and as required under this Framework or other management systems;
- Ensuring that they have the relevant competencies and attend required training in a timely manner; and
- Performing any risk actions or compliance obligations for which they are responsible.

5 RISK PROFILE

CS Energy's risk profile comprises risk capacity, risk appetite and risk tolerance, as illustrated in the diagram below.



5.1 Risk capacity

Risk capacity is the amount and type of risk CS Energy is able to support in pursuit of its business objectives, taking into account its capital structure and access to funding, as well as its "non-financial equity".

Given CS Energy is constrained by its financial position, risk capacity is significantly influenced by its gearing levels and operating cash flows. Risk capacity may change over time and should be reviewed at least annually, however within the operating context of CS Energy it is anticipated that risk capacity constraints will influence the business for a period of time.

CS Energy's risk capacity is calculated by the Finance team and must be reviewed in conjunction with risk appetite and risk tolerance at least annually, or when there is a significant change in financial position.

5.2 Risk appetite

Risk capacity informs risk appetite, which is CS Energy's "attitude" towards risk-taking. Risk appetite provides a structure within which opportunities can be pursued and downsides mitigated by setting out how much risk the business is willing to take. Management should consider CS Energy's risk appetite when evaluating strategic alternatives and managing the related risks.

When managing health and safety risks, while risk capacity will be referred to, the primary objective remains to ensure that safety risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011

A top-down board led philosophical idea of overall risk appetite and available capital helps define the business' risk capacity. Management-led scenario analysis demonstrates range of potential impacts to risk capacity and appetite in times of stress. This is then cascaded down to the business by setting risk limits for key risk types aligned with risk tolerances to ensure day to day operations are within Board-approved appetite.

Risk appetite for CS Energy is articulated in a Risk Appetite Statement[2], which includes guiding principles that broadly outline CS Energy's approach to taking risk in each key risk area. Risk appetite must be reviewed along with risk capacity and risk tolerance at least annually, or when there is a significant change in financial position or operations.

5.3 Risk tolerance

Risk tolerance specifies the amount of risk CS Energy is willing to accept. The risk tolerance will be defined with reference to the Risk Appetite Statement.

The CEO establishes tolerance levels for individual risk categories with reference to the CS Energy risk appetite, which are outlined in the Risk Appetite Statement.

Risk tolerance levels in relation to individual risks within the Board's overall risk appetite are defined in the Risk Appetite Statement. . Risks that are outside tolerance level (i.e. where the Residual Risk Rating is above the maximum acceptable level) and cannot be reduced to within tolerance require escalation and approval at the specified authority level if they are to be accepted.

The risk tolerance for health and safety risks is determined with the primary objective of ensuring that safety risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011.

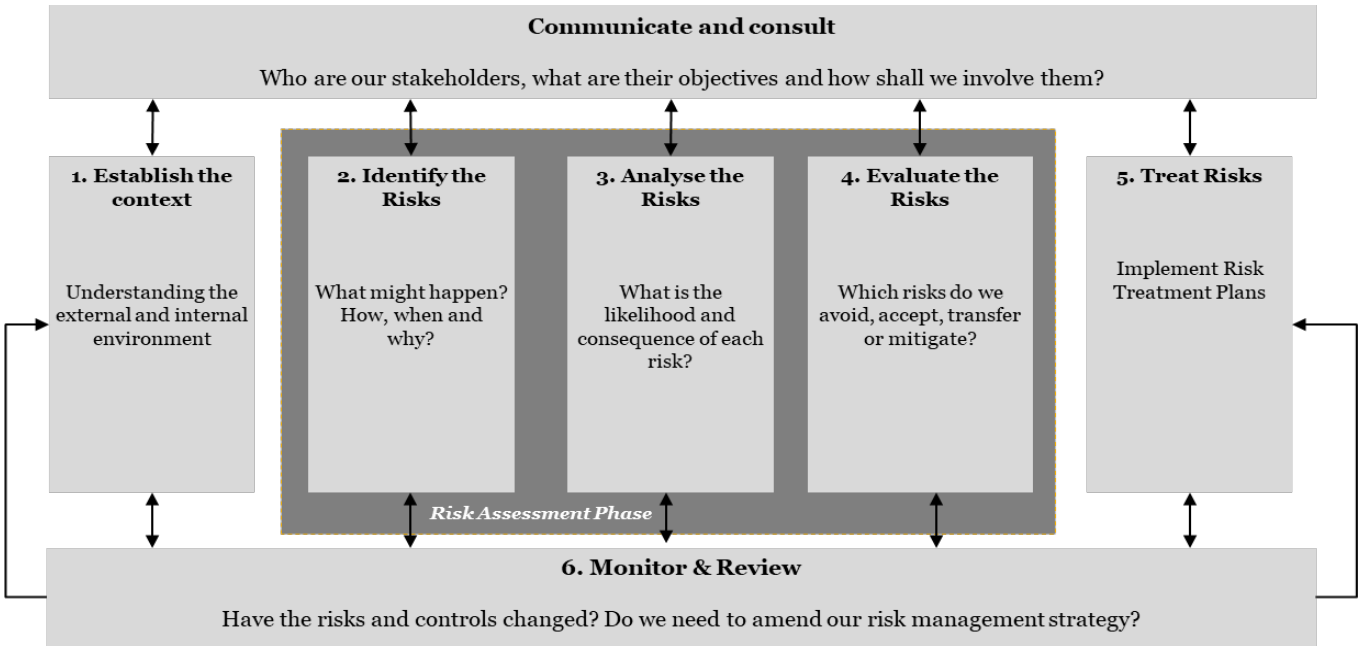
The risk tolerance for health and safety risks is not subject to change based on risk capacity (financial considerations) or consideration of changes in risk appetite.

The Risk Appetite Statement which is approved by the Board annually provides clear direction of the level of uncertainty that CS Energy is willing to accept.

[2] TRIM B/D/20/8887 – Board approved document June 2020

6 RISK MANAGEMENT

A diagram of the ISO 31000:2018 Risk management process is shown below and is intended to be a continuous loop. Each step of the process is described in this section.



6.1 Establishing the context

Defining the risk management context establishes the broader elements and objectives related to the risk area being considered, whether that be an activity, project, division or the whole organisation. The following context considerations should be made as part of the process prior to identifying and assessing risks:

- Scope of risk management process – area of the business involved and the time horizon;
- Objectives and tolerances – what CS Energy is trying to achieve, to what targets and within which tolerances;
- External context – the external influences on CS Energy; and
- Internal context – the internal influences on CS Energy.

6.2 Risk identification

Risk identification is the process of recognising and describing the risks that exist within the agreed scope, objectives, tolerances and context, this includes compliance risks. Methods for identifying risks include consulting with a cross-section of subject-matter experts by conducting risk workshops, desktop reviews, PESTLE and SWOT analyses (to identify strategic risks), HAZID and HAZOP studies, engineering reviews, and legislative reviews. Potential causes and consequences of risks and opportunities are also identified. These are maintained in the CS Energy risk registers in Insight.

6.3 Risk analysis

Risk analysis allows the comparison and prioritisation of risks to understand the overall relativity of identified risks and to drive risk-based decision making. It involves understanding the nature, sources and causes of risks in order to estimate the risk rating and requires consideration of the impacts, consequences and existing controls. This informs the decisions to be made as part of risk evaluation.

Consistent risk measurement requires a consistent approach to the analysis of risk. The primary risk analysis tool used by CS Energy is the "bowtie", which is illustrated in Appendix 3 - Bowtie risk analysis tool. Bowtie risk analysis involves:

6.3.1 Causes and consequences

Identifying the causes of the risk event identified in Section 6.2 Risk identification, and the consequences if the event were to occur.

6.3.2 Inherent Risk Rating

Determining an Inherent Risk Rating by measuring the likelihood of each consequence occurring for that risk event assuming no controls or other mitigating factors are in place. The rating is determined using the consequence and likelihood tables in Appendix 2 - CS Energy Risk Matrix.

6.3.3 Controls

Identifying controls that are already in place. Controls can be;

- Preventive (reduce the consequence and likelihood of a risk event occurring. Apply at the beginning of a risk's life, at or near the root causes(s), they often act as a barrier to the risk),
- Detective (identifies failures in the current control environment). Note: detective controls are added in Insight as "Preventing Controls".
- Mitigative (reduce the consequences of an event). Apply towards the end of a risk's life when the impact is imminent or being felt, it usually modifies the consequence.

In some cases, controls may not yet exist.

6.3.4 Critical controls

Controls can further be classified as a critical control. A critical control is essential to risk mitigation and the absence or failure of a critical control is considered unacceptable.

- Critical controls are defined by the ICMM3 as *"a control that is crucial to preventing the event or mitigating the consequences of the event. The absence or failure of a critical control would significantly increase the risk despite the existence of the other controls. In addition, a control that prevents more than one unwanted event or mitigates more than one consequence is normally classified as critical."*
- What separates critical controls from those that are far less important, is the risk consequence.

6.3.5 Control effectiveness

Assessing control effectiveness, by establishing the degree to which these controls are effective in reducing either the consequence or likelihood of a risk event. Controls may be classified as Weak, Intermediate or Strong[4], the below table provides a summary of attributes associated with each of the effectiveness levels. Further in-depth descriptions are within **Appendix 1 Control Effectiveness.**

Summary of control attributes

	ATTRIBUTES	WEAK *	INTERMEDIATE *	STRONG *
1	Design			

[3]Health and Safety Critical Control Management - Good Practice Guide - International Council on Mining and Metals (ICMM)
[4] Note that these attributes are a guide, the level of application and effectiveness can have subjective elements

2	Documentation	• Not in place or • None / Low	• Partially in place or • Medium	• In place & effective or • High
3	Communication			
4	Implementation			
5	Management Confidence			
6	Reliability			
7	Ongoing assurance			
8	Risk root cause addressed			
9	Management of the risk			
*the attribute may take on various status as applicable				

6.3.6 Residual Risk Rating

Assigning a Residual Risk Rating that measures the consequence and likelihood of an event when considering the identified causes and effectiveness of the existing controls. The rating is determined using the consequence and likelihood tables in Appendix 2 - CS Energy Risk Matrix. All relevant consequences should be considered for each risk.

6.3.7 Risk Owner

Identifying and assigning roles for the risk, including a Risk Owner, who is accountable for the information and decisions relating to the risk, in addition to being responsible for ensuring treatment actions are completed by their due dates with the support of Action Owners. Risk Owners are also required to periodically assess the appropriateness of risk ratings and to flag emerging issues to the ELT.

6.4 Risk evaluation

Risk evaluation is a decision-making activity that assesses the outcome of the risk analysis against CSE's risk tolerance, which is outlined in the below table, to determine what action is required.

Residual Risk Rating	Risk Tolerance	CSE Authority Level (escalate to)	Guidance / Action Required by Risk Owner
High	Outside tolerance	Executive General Manager (EGM)	- Associated activity/project should be suspended where possible - Signoff from EGM required to continue; - CEO to be notified; Site Manager to be notified (for site risks) - Review and verify effectiveness of existing controls - Identify & implement additional risk treatments as a priority
Significant	Outside tolerance	Head of Department; Site General Manager (for site risks)	- Associated activity/project should be closely monitored - Signoff from either Head of Dept. or Site GM required to accept risk - Review and verify effectiveness of existing controls - Identify & implement additional risk treatments as a priority
Moderate	Tolerable	Risk Owner	- Associated activity/project should be monitored - Implement additional risk treatments where practical
Low	Acceptable	Risk Owner	- Proceed & manage using routine procedures

If the Residual Risk Rating is outside the risk tolerance level (i.e. Significant or High), the options are to:

a) Treat the risk – additional controls or treatment plans may be implemented to reduce the Residual Risk Rating to be within tolerance (see Section 6.5 Risk treatment);

b) Accept the risk – approval must be sought to accept a risk outside CSE risk tolerance levels (escalated as per the Authority Level in the above table). This may occur where no action can be taken to further mitigate the risk (e.g. the costs of treatment would exceed the benefits gained or the circumstances are beyond CSE's influence and control); or

c) Avoid the risk – cease the activities and situations which could give rise to the risk. This may occur where the Residual Risk Rating cannot be reduced to an acceptable or tolerable level through risk treatment.

Where the Residual Risk Rating falls within the tolerance level (i.e. Moderate or Low), the risk is accepted in accordance with the specified authority level in the above table.

Note that for Health and Safety Risks, the risk tolerance is to ensure that Health and Safety Risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011.

6.5 Risk treatment

Where existing controls do not reduce a Residual Risk Rating sufficiently to fall within set risk tolerances, a decision may be made to further mitigate the risk by undertaking treatment actions designed to reduce the risk rating to within required tolerances. Treatment actions should be determined with consideration given to the scope, cost and timing of the work, and may include improving existing controls or putting new controls in place to remove causes, to reduce the consequences or likelihood of an event, or to share the risk through contracts and/or insurances.

Treatment actions are assigned an Action Owner, who is responsible for ensuring actions are completed as required by the due date and for updating action status in Insight, and are nominated by the Risk Owner. A Planned Risk Rating is set, which is the target level of risk to be achieved when the risk has been mitigated to a tolerable level due to suitable treatment actions being completed (unless the has already been controlled to a tolerable level or no feasible action plan exists to mitigate it further, in which case the Planned Risk Rating will be the same as the Residual Risk Rating).

Treatment actions will most often not reduce the level of risk immediately, which may mean that CS Energy operates outside its risk tolerance for a period of time. Where this is the case, the monitoring undertaken as outlined in Section 6.6 Risk monitoring will assist in providing regular information as to how the risk is impacting the business.

Upon completion of a treatment action, the Risk Owner should consider whether the action can be listed as a new control for the risk, or if an existing control requires updating in consultation with the Control Owner, and the Residual Risk Rating should be reassessed.

6.6 Risk monitoring

Risk monitoring activities occur across the “Three Lines of Defence” as outlined below, and may identify new risks, recommendations in relation to current controls or areas of non-compliance.

Responsibility	Monitoring activities may include:
Line Management (Risk / Control Owners) Risk Compliance Facilitators	- Management oversight - Review control effectiveness, e.g. CCVs - Key Risk Indicator monitoring
Risk & Compliance team H&S Environment	- Key Risk Indicator reporting - Risk reporting - Review control effectiveness, e.g. CCVs - Internal reviews - Accuracy of risk and compliance data - Benchmarking
Assurance; external auditors	- Continuous assurance program - Assurance reviews - External audits

6.7 Risk review

Risks are required to be reviewed by the Risk Owner on a periodic basis to:

- Provide assurance that risks are being managed as expected;
- Assess whether controls remain relevant and effective;
- Verify whether implemented treatment plans are effective;
- Ensure that the risk profile reflects any changed circumstances; and
- Confirm that any risk issues have been identified, reported and actioned.

Risk reviews occur through the following activities:

- Individual risks are reviewed on a periodic basis based on residual risk rating, regardless of tier, as per the table below. This includes a full review of causes, consequences, risk ratings and controls.

	Low Residual Risk	Moderate Residual Risk	Significant Residual Risk	High Residual Risk
Review Frequency	Annually / archive if no longer relevant	Annually	Six-Monthly	Quarterly

- The CS Energy Group risk register (i.e. **Tier 1 risks**) are reviewed on a quarterly basis by the ELT and ERC.
- The CS Energy Group risk register will form an input into the development of Board Strategy and be reviewed as part of the annual business planning cycle to ensure the content remains aligned with the strategic plan.
- Site/Functional risk registers (i.e. all **Tier 2 risks** for a Site/Functional Area) are to be reviewed at a high level annually during the business planning process to ensure they remain relevant and aligned to business plans and that any emergent risks have been identified.
- Risk deep dives on Tier 1 or Tier 2 risks are completed periodically as per the nominated schedule and presented to the applicable Board Committees. Deep dives are facilitated by the R&C Team in conjunction with relevant Risk Owner. The intent of the risk deep dive is to provide an in-depth assessment of the current state of the risk. It involves a review of the risk rating and control effectiveness taking supporting data into consideration, e.g. incidents, compliance breaches and Critical Control Verifications. The risk rating is also considered in relation to CS Energy's risk tolerance to confirm whether additional treatment plans are required.
- Out-of-cycle risk reviews may be conducted if material changes occur, there is a breakdown of controls or new risks emerge, e.g. due to organisational change, a major process or system change, failure of controls, a major incident, compliance breach, serious complaint or significant near miss.

7 COMPLIANCE MANAGEMENT

CS Energy's compliance program incorporates the following elements which are outlined below:

- Obligations management;
- Compliance risks;
- Compliance Checklists;
- Supporting tools; and
- Monitoring and review.

7.1 Obligations management

CS Energy undertakes diverse activities within a dynamic and complex regulatory environment, and must comply with a significant number of legislative, regulatory and other obligations. These obligations must be identified, assessed and managed effectively to ensure CS Energy remains compliant. Management of compliance obligations is a de-centralised responsibility of line management with support, tools and reporting provided by the R&C Team.

Obligations are captured in Insight at three levels to enable effective management and tracking:

- **Obligation sources** – this includes legislation, regulations and mandatory standards that CS Energy must comply with.
- **Obligations** – these are the specific requirements contained within an obligation source that CS Energy must comply with.
- **Obligation actions** – tasks that must be routinely undertaken to maintain compliance with their related obligation.

7.2 Compliance risks

Compliance risks (i.e. risks relating to not complying with CS Energy's legislative, regulatory or other requirements) are identified and managed in line with Section 7 Compliance management.

7.3 Compliance Checklists

Executive General Managers and relevant Management are to certify on a quarterly basis that key compliance requirements and obligations have been met and report any material non-compliances.

7.4 Supporting tools

Policies and procedures have been documented and implemented to assist CS Energy employees and contractors in meeting all relevant compliance requirements in a consistent manner.

In addition, Compliance Manuals have been developed for areas with significant compliance responsibilities, such as Trading, Health and Safety, and Environment, and provide a thorough overview and analysis of relevant compliance requirements.

Supporting tools[5] such as legislation, regulatory newsfeeds and Australian and International Standards are available to support obligation and risk owners.

7.5 Monitoring and review

The R&C Team, Obligation Owners, Risk & Compliance Facilitators and other relevant employees monitor the external and internal business environment for new, changed or obsolete obligations. This monitoring may occur through relationships and communication with regulators, advisors and/or industry and professional associations and via regular regulatory newsfeeds issued by an external provider to relevant employees.

Where new compliance obligations are identified, a gap analysis will be conducted in consultation with the relevant business unit to identify the processes impacted by the change and implement and communicate any changes required. Obligations will be updated in Insight to take into account any changes in compliance requirements.

Existing compliance obligations should be maintained on a continual basis to ensure they align with current legislative, regulatory and other requirements. Obligation sources and their corresponding obligations will be reviewed on an annual basis by the Obligation Owner, in consultation with the relevant Risk and Compliance Facilitator and the R&C Team as required.

[5] Examples include SAI Global Services and Techstreet Enterprise (standard providers), these may change based on services provided

8 COMMUNICATION AND CONSULTATION

Communication and consultation are integral to the risk management process, providing the basis for decision making across the business. This ensures the appropriate people are involved in the risk assessment process, and during ongoing monitoring management and review.

Communication and consultation is also imperative in compliance management to raise awareness and understanding of compliance requirements and obligations, and to effectively manage those requirements and obligations. When new compliance requirements are introduced, or existing requirements have been updated, relevant departments will be appropriately consulted with to determine the impacts on current processes. Any new or updated policies and procedures will then be communicated to affected employees. Communication and consultation will also occur during monitoring, reporting and review to ensure compliance requirements and obligations are being managed appropriately and any issues are identified and rectified.

Communication and consultation may be with internal stakeholders such as employees, the ELT and Committees, or with external stakeholders such as relevant government bodies, contractors and regulators.

9 RESOURCES AND TRAINING

9.1 Insight

Insight is CS Energy's enterprise risk system, which also includes compliance obligations, assurance review findings and actions.

9.2 Intranet

The Risk, Compliance and Assurance section on CS Energy's Intranet contains an overview of how risk and compliance is managed at CS Energy as well as links to relevant documents and tools.

9.3 Training

Risk Owners, Control Owners and Obligation Owners are ultimately accountable for the identification, analysis, evaluation and control of risk and compliance within CS Energy. They will be briefed on their role and responsibilities regarding risk, controls or compliance, and the tools required to perform the role successfully. They will also receive on-going training and support as required.

Training will also be conducted on an ongoing basis for other employees with risk and compliance responsibilities, including the R&C Team, Legal, Executive General Managers and Energy and Financial Risk, to ensure they are aware of compliance requirements and have the necessary understanding and tools to meet the requirements.

9.4 Quick Guides

A series of Quick Guides have been developed to provide further interpretation and support to embed the Framework, these shall be amended and expanded as required.

10 REPORTING

10.1 Issue and breach reporting

The reporting of compliance breaches and risk issues or events is an important component of a robust risk and compliance program, to enable the identification and recording of control failures and the follow-up actions undertaken to resolve such failures.

Potential and actual compliance breaches are to be reported to the R&C Team as soon as practicable or may be reported through other channels for specific departments where procedures currently exist, such as Energy Markets, Health & Safety, and Environment, or anonymously through CS Energy's Whistleblower service. Serious compliance breaches will be investigated as per the procedures outlined in CS-GOV-13 - Complaints and Investigations Handling.

10.2 Management reporting

Reporting on the status of risk and compliance management is summarised in the table below:

Reporting Type	Description	Board	ERC	MRC	ELT	EGMs
Board Risk Report	Links risk appetite to strategy objectives. A monthly "Risk on a page" report summarises the current exposure to risk by category, and compliance with the Risk Appetite Statement	✓			✓	
Tier 1 Risk Report	A quarterly overview of the Tier 1 risks of CS Energy including a summary of control weaknesses at Tier 1 level, actions designed to address those control weaknesses, any incidents linked to that risk in the last period and an estimate of timing to achieve the Planned Risk Rating.		✓		✓	
Compliance Exceptions Report	**Material non-compliances identified in the Compliance Checklist process are escalated to the ERC on a quarterly basis.**		✓			
Executive Leadership Team	The R&C Team will provide additional reporting to the ELT on an ad hoc basis to support Executive Management in the performance of their responsibilities under this Framework.				✓	
Market Risk Committee	The MRC, comprised of Senior Management representatives, will also consider operational and trading risk reports to ensure the effective management of trading-based risks and compliance activity.			✓		
Ad hoc reporting	**Other information relevant to the activities of the R&C Team.**	✓	✓	✓	✓	✓

11 CONTINUAL IMPROVEMENT

This Framework will be continually reviewed and improved, where practicable, to ensure it meets current requirements and changes in legislation, regulations and standards.

This Framework will be reviewed by the R&C Team, in consultation with Risk and Compliance Facilitators, biennially at a minimum, or more frequently to incorporate material business or regulatory changes.

11.1 Approval authority

The ERC is responsible for approving the Framework where material changes have been made. Where non-material changes have been made, the Framework can be approved by the Executive General Manager Corporate Services.

12 DEFINITIONS

Term	Definition
Action	Work undertaken to: ▪ Implement or improve a control. ▪ Prevent or mitigate a risk. ▪ Address an event.
Action Owner	The person responsible for the delivery of an action.
Board	The Board of Directors of CS Energy Limited.
Cause	Set of circumstances or requirements which, alone or in combination, have the potential to give rise to a risk.
Compliance breach / failure	An act or omission where CS Energy has not met its compliance requirements and/or compliance obligations due to a failure in controls.
Compliance Checklist	A signoff completed by Executive General Managers on a quarterly basis to certify that key compliance requirements and obligations have been met.
Compliance risk	The risk of not complying with CS Energy's legislative, regulatory or other requirements.
Context	A generic term that in effect places a boundary around the subject matter that makes it easier to identify the risks and follow a risk management process. Contexts can be business units, functions, projects, objectives and the like.
Consequence	The outcome of an event. A single event can generate a range of consequences which can have positive or negative effects on objectives.
Contractor	An individual who is employed directly by CS Energy for a defined term.
Control	A way of modifying risk to achieve a more favourable effect on objectives or change the likelihood of the effect. The purpose of a control may be to prevent the event, detect the event or mitigate the consequences of the event and they do this to varying degrees of effectiveness. Controls vary in effectiveness, and may include policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk.
Control Owner	The person responsible for the delivery of a control.
Critical control	A control that is crucial to preventing the event or mitigating the consequences of the event. The absence or failure of a critical control would significantly increase the risk despite the existence of the other controls. In addition, a control that prevents more than one unwanted event or mitigates more than one consequence is normally classified as critical. What separates critical controls from those that are far less important, is the risk consequence
Control effectiveness	The effectiveness of controls may be categorised as Weak, Intermediate or Strong (refer to details included in Section 6.3.5 Control effectiveness).
Event	A risk that has 'eventuated' and which leads to consequences. Alternate terms 'Incident' or 'near miss' (without consequences).
Inherent Risk Rating	The level of risk determined by considering the causes and consequences that an event would pose if there are no controls or other mitigating factors. Performing this analysis is important in determining what could occur in the event of complete control failure.
Insight	CS Energy's enterprise risk system, which also includes compliance obligations and assurance review findings and actions (software provider is CGR https://www.corpgovrisk.com/).
Likelihood	The frequency or chance of the consequence affecting the objectives.
Objective	A goal of the business including explicit metrics and timeframes.

Term	Definition
Obligation	A compliance obligation that must be adhered to, as specified by legislation, regulations, industry standards or codes.
Obligation action	A task that must be undertaken to achieve regulatory and/or procedural compliance. These are stored in the R&C system compliance management system.
Opportunity	A positive event that can cause risk to become a gain.
Planned Risk Rating	The target level of risk to be achieved when the risk has been mitigated to a tolerable level due to suitable treatment actions being completed. The risk may already be controlled to a tolerable level or no feasible action plan exists to mitigate it further, in which case the Planned Risk Rating will be the same as the Residual Risk Rating.
Residual Risk Rating	Level of risk at present, taking into consideration existing controls and their level of effectiveness in reducing the likelihood or consequence of an event (taking into account any weaknesses in their design or application).
Risk	The effect of uncertainty on objectives. It is the possibility that something might go wrong and have a negative impact on the company.
Risk analysis	A process used to understand the nature, sources and causes of the risks identified and to estimate the level of risk. It is also used to examine consequences and to examine the controls that currently exist.
Risk appetite	Amount and type of risk an organisation is willing to accept in the pursuit of strategic objectives. Health and Safety Risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011
Risk and Compliance Facilitator	Risk and Compliance Facilitators are appointed by the respective division/function EGM to facilitate the execution of the manager's responsibilities in relation to risk management and compliance (typically for a division/function).
Risk capacity	The amount and type of risk an organisation is able to accept in the pursuit of strategic objectives. Health and Safety Risks are managed so far as is reasonably practical consistent with the Work Health and Safety Act and Regulations 2011
Risk escalation	The process where an increasingly higher level of authorization is required to sanction the continued acceptance of increasingly higher levels of risk.
Risk evaluation	Process used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
Risk identification	Process of finding, recognising and describing the risks that could affect the achievement of the company's objectives. It includes the identification of possible causes and consequences.
Risk limits	Mechanisms for monitoring and reporting of compliance with risk tolerance.
Risk management process	The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.
Risk Owner	A person appointed to have responsibility for the entire risk, including oversight of controls and actions, development of treatment actions and maintaining currency of data in the risk system.
Risk register	A library of risks including the related root causes, consequences, controls and any related actions, which is maintained in Insight.
Risk retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation.
Risk transfer	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.
Risk treatment	Selection and implementation of appropriate options for dealing with risk. The most commonly used terms for these are avoid, reduce, transfer, accept and retain.
Risk tolerance	Acceptable level of variance around the achievement of targets relating to specific risks at an entity or functional level.

Term	Definition
Risk treatment action	Work undertaken to implement, improve or modify a control. Treatment actions are designed to improve controls and reduce the Residual Risk Rating.

13 REFERENCES

Reference No	Reference Title	Author
B/D/11/39708	Policy - Governance Risk and Compliance	CS Energy
B/D/12/67984	Policy - CS-RISK-02 - Market Risk Policy	CS Energy
B/D/13/28187	Standard - CS-GOV-13 - Complaints and Investigation Handling - Official Misconduct, Public Interest and Protected Disclosure	CS Energy
B/D/13/15225	Form - S2122 - Operations Plant Risk Assessment Template	CS Energy
B/D/18/6609	Procedure - CS-OHS-76 - Health and Safety Risk Management Framework	CS Energy
B/D/20/12713	Risk & Compliance Strategy FY21 - FY25	CS Energy
B/D/20/17649	CSE - Quick Guide - Risk Tiers	CS Energy
B/D/20/17020	CSE - Quick Guide - Risk Tolerance & Evaluation	CS Energy
B/D/20/16995	CSE - Quick Guide - Levels of Risk	CS Energy
B/D/20/16902	CSE - Quick Guide - Risk Review(s)	CS Energy
B/D/20/16167	CSE - Quick Guide - Critical Controls	CS Energy
Techstreet Link	AS19600-2015 *Compliance Management – Guidelines ("ISO 19600")*	Aust Standard

14 RECORDS MANAGEMENT

In order to maintain continual improvement, suitability, safety and effectiveness of the organisation, CS Energy's registered documents will be reviewed on a two-yearly basis or at intervals specified by legislative or regulatory requirements. Review of controlled documents should occur where it has been identified that there are changes in technology, legislation, standards, regulation or where experience identifies the need for alteration to the content. Registered documents should also be reviewed following an incident, change management process, modification or where directed as part of a risk assessment process. A 'review' can simply mean that it has been identified, confirmed and appropriately recorded that no changes are required and that the existing process remains the same.

CS Energy must ensure that records are retained according to accountability, legal, administrative, financial, commercial and operational requirements and expectations. In compliance with records retention and disposal, all documentation created in relation to CS Energy business must be retained in line with minimum retention periods as detailed in legal retention and disposal schedules.

APPENDIX 1 - CONTROL EFFECTIVENESS

- Weak controls may consist of one or more of the below attributes:
- not effectively designed and not in place,
- not or poorly documented,
- not or poorly communicated,
- not or inconsistently implemented in practice,
- management has no / low confidence in the effectiveness of the controls,
- the controls are not reliable / operating as intended,
- none or poor assurance that the control is operatively effectively,
- provides none / limited level of effectiveness in addressing the risk's root cause,
- the risk is not being managed as expected.
- Intermediate controls may consist of one or more of the below attributes:
- partially effectively design and partially in place,
- partially documented and maintained,
- partially communicated,
- partial or inconsistently implemented in practice,
- management has a medium level of confidence in the effectiveness of the controls,
- the controls are partially reliable / operating as intended,
- assurance that the control is partially effective,
- provides medium level of effectiveness in addressing the risk's root cause,
- the risk is being partially managed, but below expectations.
- Strong controls may consist of one or more of the below attributes:
- effectively designed and in place,
- well documented and maintained,
- well communicated and understood,
- consistently implemented and in practice,
- management has a high level of confidence in the effectiveness of the controls,
- the controls are reliable / operating as intended,
- assurance that the control is operating effectively,
- provides a high level of effectiveness in addressing the risk's root cause,
- the risk is being managed as expected.

APPENDIX 2 - CS ENERGY RISK MATRIX

Consequence Table

Category	Consequence Scale					
	1. Minor	2. Low	3. Medium	4. Major	5. Severe	6. Catastrophic
Safety & Security	Incident with no injury sustained Minor non-conformance to security requirements (e.g. gate left open, CCTV camera faulty etc.)	Low level, short term injury (e.g. first aid) Detected security breach with no impact to assets	Impairment including short term medical treatment (e.g. MTI) Security breach with low level impact (e.g. theft of non-essential asset)	Reversible disability or impairment including medium term medical treatment (e.g. short term LTI) Stolen or impaired asset that does not restrict operations	Permanent disability or other injury requirement hospitalisation or long term treatment (e.g. serious LTI) Stolen or impaired asset that restricts operations	Single or Multiple fatalities Stolen or impaired asset resulting in plant shutdown
Environment	Small contaminant release or land disturbance, localised on-site area affected. Routine short-term clean-up/remediation.	Moderate contaminant release or land disturbance, localised on-site. Routine short-term clean-up/remediation.	Moderate contaminant release or land disturbance; localised on-site impact or localised offsite release not resulting in environmental nuisance or harm as per the Environmental Protection Act 1994. Routine short-term clean-up/remediation.	Large contaminant release or land disturbance; localised off-site release resulting in environmental nuisance or harm as per the Environmental Protection Act 1994. Short-term clean-up/remediation.	Large contaminant release or land disturbance; localised off-site release resulting in environmental harm as per the Environmental Protection Act 1994. Long-term clean-up/remediation, potentially irreversible.	Very large contaminant release, extensive off-site area affected. Complex long-term clean-up/remediation resulting in environmental harm as per the Environmental Protection Act 1994. Irreversible offsite environmental harm.
Financial* (excluding Insurance) **see below for Equivalent Period Offline*	<$2m loss in a year	>$2m and <$5m loss in a year	>$5m and <$30m loss in a year	>$30m and <$60m loss in a year	>$60m and <$100m loss in a year	>$100m loss in a year
Reputation/ Stakeholder Relations (Internal & External)	- Community/stakeholder concerns can be dealt with via normal engagement - Local site issue - Isolated public dissatisfaction with CSE	- Key stakeholders exercise their authority in response to the issue - Influential community figures exercise their influence within the community - Localised and limited negative media	- Shareholding Ministers (or other stakeholders) withholding funds/approvals or sanctioning - Isolated negative state wide media coverage - Community dissatisfaction with CSE - Localised level of disengagement - Localised industrial dispute/action impacting a restricted number of employees	- Creates a 'headline' issue for the Shareholder - Significant negative state wide media and/or parliamentary attention - Shareholder intervention in the business - Public and shareholder perception of organisational competence is reduced - Pervasive level of disengagement across a site - Industrial dispute/action impacting a significant portion of a generation site	- Creates a persistent 'headline' issue for the Shareholder - Significant and recurring negative state wide media and/or parliamentary attention - Extensive Shareholder intervention in the business - Public and shareholder perception of organisational competence is undermined - Significant disengagement across a site - Extended industrial dispute/action impacting all operations on a generation site	- Irreparable breach of shareholder and stakeholder confidence - Significant and continuous public criticism - Significant and recurring negative media attention on a national level - Permanent disengagement across one or multiple sites - Extended industrial dispute/action that has the effect of shutting down one or more generation sites
Legal/ Compliance/ Regulatory	- Small number of minor procedural breaches by individual staff members	- Multiple compliance incidents which are not systemic - Minor Act or code breaches - Individual legal actions	- Systemic compliance incident - Minor Act or code breaches with potential moderate range fines	- Criminal or civil regulatory prosecution of CS Energy (or directors/officers) - Multiple and systemic compliance incidents - Act or code breaches with potential fines - Individual legal actions	- Multiple significant compliance incidents - Act or code breaches leading to enforcement action - Multiple legal actions	- Serious compliance incidents creating significant compliance penalties for directors and organisations - Loss of operating licenses and registrations - Multiple legal actions/ class actions
Technology (ICT / OT)	- Support to business processes reduced - Application or device servicing a person or small group disabled	- Public information unavailable - Internal use information unavailable - Application or system disabled - Support/s to non-critical services impacted, support process reduced - Application or non-support system servicing a team disabled	- Public information inaccurate - Internal use information inaccurate - Confidential information unavailable - Support processes impacted with manageable consequences - Service/s impacted with manageable consequences - Application or support system servicing multiple team disabled	- Public information tampered with - Internal use information tampered or leaked - Confidential information inaccurate or leaked - Highly Confidential information unavailable - Support to critical system disabled - Critical system degraded - Support to business objectives degraded - Applications or support systems servicing multiple teams disabled	- Confidential information leaked - Highly Confidential information tampered with or inaccurate - Multiple support to critical systems disabled - One critical system unable to support business objectives	- Technology Infrastructure supporting several critical systems disabled - Critical systems disabled and unable to support business objectives

*By way of guidance, Financial consequence is broadly aligned to the following outages (Equivalent Period Offline):

Station / Season	1. Minor	2. Low	3. Medium	4. Major	5. Severe	6. Catastrophic
Kogan (Jan-Mar)	Up to 2 days	3 to 5 days	6 to 35 days	36 days to 2.5 months	>2.5 months to 4 months	>4 months
Kogan (Apr-Dec)	Up to 3 days	4 to 9 days	10 days to 2 months	>2 to 4.5 months	>4.5 months to 7.5 months	>7.5 months
Callide B (Jan-Mar)	Up to 4 days	5 to 12 days	13 days to 3 months	>3 to 6.5 months	>6.5 months to 10 months	>10 months
Callide B (Apr-Dec)	Up to 12 days	13 to 35 days	36 days to 10 months	>10 months to 1.5 years	>1.5 years to 2.5 years	>2.5 years
Callide C (Jan-Mar)	Up to 4 days	5 to 10 days	11 days to 2.5 months	>2.5 to 5 months	>5 months to 7.5 months	>7.5 months
Callide C (Apr-Dec)	Up to 8 days	9 to 23 days	24 days to 6 months	>6 to 1 year	>1 year to 1.5 years	>1.5 years

Risk Likelihood Table *(excluding Technology risks - see table below)*

Likelihood Level	Descriptive Guidance	Probability	Frequency
Highly Likely	The event is expected to occur in most circumstances	Higher than 80%	The event and consequence is expected to occur at least once per year
Likely	The event will probably occur in most circumstances	From 33% up to 80%	The event and consequence is expected to occur at least once in 1 to 3 years
Possible	The event could occur at some time	From 5% up to 33%	The event and consequence is expected to occur at least once in 3 to 20 years
Unlikely	Not expected but the event may occur at some time in the future	From 1% up to 5%	The event and consequence is expected to occur at least once in 20 to 100 years
Rare	The event may occur only in exceptional circumstances	Less than 1%	The event and consequence is expected to occur less than once in every 100 years.

Risk Likelihood Table *(for risks with ICT/OT consequence only)*

Likelihood Level	Descriptive Guidance	Probability	Frequency
Highly Likely	Almost certain to occur during the project/ contract/business plan/technology life span	Higher than 80%	The event and consequence is expected to occur more than once a week
Likely	Likely to occur during the project/contract/ business plan/technology life span	From 33% up to 80%	The event and consequence is expected to occur at least once a week to once a month
Possible	Possible to occur during the project/contract/ business plan/technology life span	From 5% up to 33%	The event and consequence is expected to occur at least once a month to once a year
Unlikely	Unlikely to occur during the project/contract/ business plan/technology life span	From 1% up to 5%	The event and consequence is expected to occur at least once in 1 to 3 years
Rare	Rare to occur during the project/contract/ business plan/technology life span	Less than 1%	The event and consequence is expected to occur less than once in every 3 years

RISK MATRIX

Likelihood Level / Consequence Scale	1. Minor	2. Low	3. Medium	4. Major	5. Severe	6. Catastrophic
Highly Likely	Low	Moderate	Significant	High	High	High
Likely	Low	Moderate	Significant	Significant	High	High
Possible	Low	Low	Moderate	Significant	Significant	High
Unlikely	Low	Low	Low	Moderate	Moderate	Significant
Rare	Low	Low	Low	Low	Low	Moderate

outside tolerance

within tolerance

RISK EVALUATION

Residual Risk Rating	Risk Tolerance	CSE Authority (escalate to)	Guidance / Action Required by Risk Owner
High	Outside tolerance	Executive General Manager (EGM)	- Associated activity/project should be suspended where possible - Signoff from EGM required to continue; - CEO to be notified; Site Manager to be notified (for site risks) - Review and verify effectiveness of existing controls - Identify & implement additional risk treatments as a priority
Significant	Outside tolerance	Head of Department; Site General Manager (for site risks)	- Associated activity/project should be closely monitored - Signoff from either Head of Dept. or Site GM required to accept risk - Review and verify effectiveness of existing controls - Identify & implement additional risk treatments as a priority
Moderate	Tolerable	Risk Owner	- Associated activity/project should be monitored - Implement additional risk treatments where practical
Low	Acceptable	Risk Owner	- Proceed & manage using routine procedures

RISK REVIEWS

	Low Residual Risk	Moderate Residual Risk	Significant Residual Risk	High Residual Risk
Review Frequency	Annually / archive if no longer relevant	Annually	Six-Monthly	Quarterly

APPENDIX 3 - BOWTIE RISK ANALYSIS TOOL

Consistent risk measurement requires a consistent approach to the analysis of risk. The Bowtie method is the primary risk analysis tool used by CS Energy. It has two key features:

- It provides a visual summary of all plausible scenarios that could exist around a chosen risk event.
- It displays the corresponding control measures that either prevent the risk event from occurring or mitigate the outcome if it does occur.