Procedure No:	CS-RISK-01
TRIM Ref No:	B/D/12/63934
Reviewed:	12/18
Amended:	12/18
Review Due:	12/20

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 and Compliance
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

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 (GR&C Policy);
- 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.

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 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

'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.

'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.

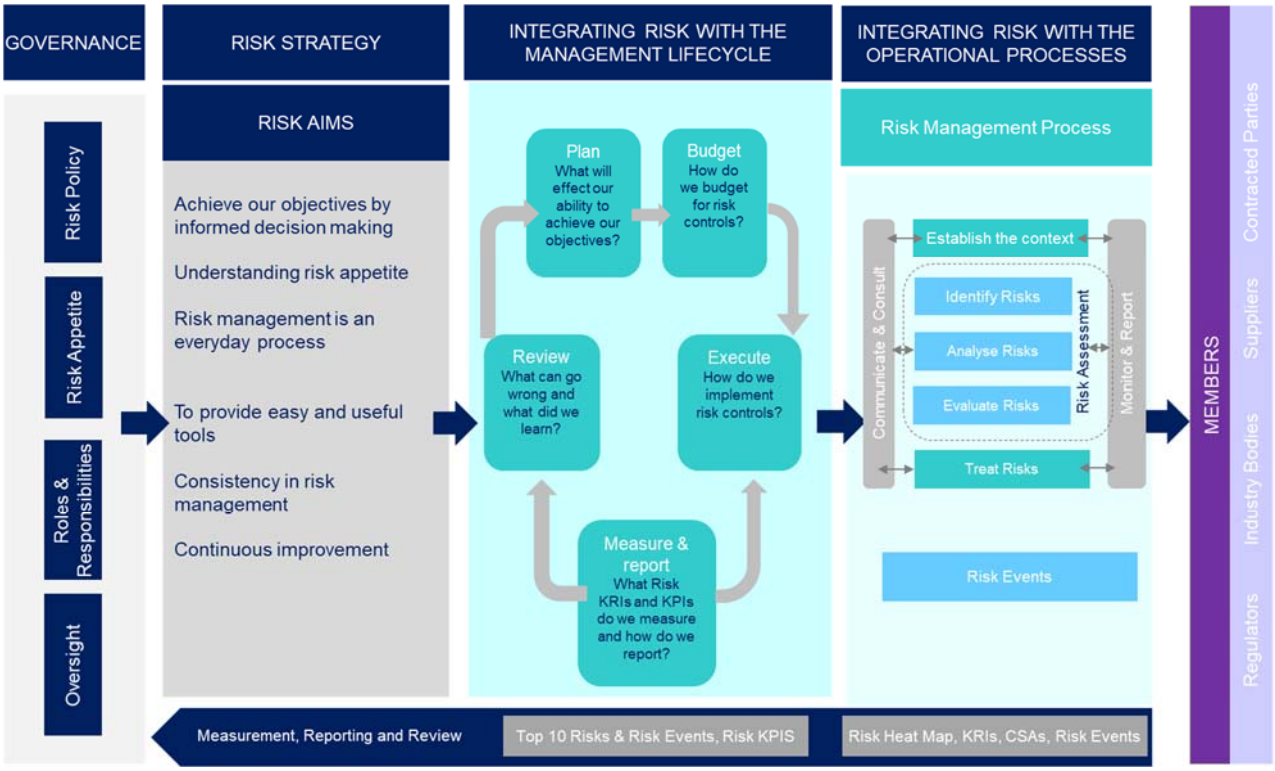
Refer to Section 13 - Definitions for a glossary of the key terms used throughout this Framework.

3.2 Framework Structure

To support effective risk and compliance outcomes, the CS Energy Enterprise Risk and Compliance Management Framework outlines the core elements required to deliver robust risk data and risk management outcomes.

The structure of CS Energy's risk framework is outlined in Figure 1 and is described in more detail throughout this document. Section 7 outlines CS Energy's approach to Compliance Management.

Figure 1 - Risk and Compliance Framework



3.3 Key Risk Categories

The Framework incorporates the full breadth of risks across the organisation, including:

3.3.1 Health, Safety and Security Risks

Health, safety and security risks are identified and managed by the Health and Safety and Process Safety teams, in collaboration with Site Managers and in accordance with the Health and Safety Manual.

3.3.2 Environment Risks

Environment risks are identified and managed by the Environment team, in collaboration with Site Managers and in accordance with the Health and Safety Management System.

3.3.3 Strategic Risks

Strategic risks can be defined as the uncertainties and untapped opportunities embedded in the CS Energy 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.

3.3.4 People and Culture Risks

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. These risks are primarily identified and managed by Operations and Corporate Services Divisions, but culture is an enterprise wide responsibility.

3.3.5 Plant Integrity Risks

Plant integrity risks can be defined as uncertainties and untapped opportunities embedded in the design of process safety and asset management, and the implementation of plant strategies at CS Energy. These risks are identified and managed by Asset Management and Plant Operations Divisions.

3.3.6 Trading Risks

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). These risks are managed through the Energy and Financial Risk team. In addition to market risk, CS Energy is exposed to a range of other trading related risks including fuel price risk, interest rate risk, foreign exchange risk and credit risk.

3.3.7 Financial Risks

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. These risks are identified and managed by the Finance and Energy and Financial Risk Teams.

3.3.8 Stakeholder Relations and Governance Risks

Stakeholder and governance 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, and includes management of change in regulations and law that might affect CS Energy's business. These risks are identified and managed by the Corporate Affairs Team, executed through the owners of the relationship, and are an enterprise wide responsibility.

3.3.9 Legal and Regulatory Risks

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. These risks are identified and managed by subject matter experts within each Division with support from the Legal and Secretariat Team.

3.3.10 ICT Risks

ICT risks are associated with the use, ownership, operation, involvement, influence and adoption of ICT within CS Energy. These risks are identified and managed by the ICT Team.

3.3.11 Enterprise Risks

Enterprise risks can be defined as the uncertainties and untapped opportunities embedded in the management of enterprise-wide operations and include contractor management, enterprise risk framework, fraud, insurance, physical security and business resilience. These risks are managed through the Contracts and Procurement, Risk & Compliance and Finance Teams, and rely on an enterprise wide support.

3.3.12 Major Projects

Projects, including capital projects and overhauls require a risk-based approach ensuring capital expenditure is aligned to key risks across the organisation. In addition, all projects require an execution risk analysis to enable the effective management of project risk. Longer term projects and high-level capital / project risks are elevated to the enterprise risk system.

4 RESPONSIBILITIES AND ACCOUNTABILITIES

4.1 Board

The Board has approved the R&C 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 governance, 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 Audit and Risk Committee

The Audit and Risk Committee 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 governance, risk and compliance management;
- Reviewing reports from Management on the effectiveness of governance, 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 has overall accountability for governance, 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 governance, 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 attestation process (refer to Section 7);
- 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 R&C 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 Audit and Risk Committee on risks including governance, risk and compliance issues and breaches;

- Overseeing processes for the management and resolution of governance, 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 governance, risk and compliance information;
- 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 and Compliance Owners

Risk and Compliance 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 attestation 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:

- Understanding this Framework and the application and use of the related Registers;
- Monitoring the health of the risk and compliance processes in their division/function or the specific risk allocated to them;
- Advising their division/team on the application of this Framework and fulfilling their responsibilities;

- Working with management to identify emerging risks in their division/function, including providing assistance in risk workshops to identify and assess risks;
- Considering risks relevant to their areas of responsibility and facilitating the process of risk analysis;
- Escalating additional risk concerns and movements that require prompt response;
- Reporting potential and actual compliance breaches to the R&C Team by, as soon as practicable.
- Supporting the Risk and Compliance Owners to maintain the Risk Registers, including facilitating a review of registers within that area on a regular basis to ensure information is up-to-date;
- Reporting any issues relating to the risk and compliance policies, procedures, processes and systems to R&C Team in a timely manner; and
- Working collaboratively with the R&C Team and management within their division to promote effective risk and compliance management.

4.8 Control Owners

Each control in the Risk Registers 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 degree described in the Risks and Opportunities Register, and that control enhancements that impact the residual level of risk 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 attestation;
- 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 the Risk Registers 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 level of risk 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 the Risk Registers;
- Examining compliance as part of planned audits where relevant; and
- Reviewing risks and associated controls during scheduled audits 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

5.1 Risk Capacity

An essential element of the CS Energy risk framework is its 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. Risk capacity may change over time and should be reviewed 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 clarified in APPENDIX 1 - Risk Capacity and Risk Appetite . This appendix may be reviewed by the Board without a full review of this Framework and must be reviewed on an annual basis as a minimum, contemporaneously with CS Energy's Risk Appetite and Risk Tolerance.

5.2 Risk Appetite

Risk capacity drives the risk appetite of CS Energy, being the degree of risk that CS Energy is willing to accept in pursuit of its objectives.

Management considers CS Energy's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks. Risk appetite should be reviewed annually or when there is a significant change in the financial position, or operations of the organisation. This enables CS Energy to adjust its view on the acceptable level of risk and the risk it is prepared to take on in the pursuit of its strategy and objectives.

Risk Appetite for CS Energy is articulated by a number of risk appetite principles that broadly outline CS Energy's approach to where and to what extent it is prepared to take on risk in the achievement of an objective. The key principles underpinning CS Energy's risk appetite are stated in Appendix 1. This appendix may be reviewed by the Board without a full review of this Framework and must be reviewed on an annual basis as a minimum, contemporaneously with CS Energy's Risk Capacity and Risk Tolerance.

5.3 Risk Tolerance

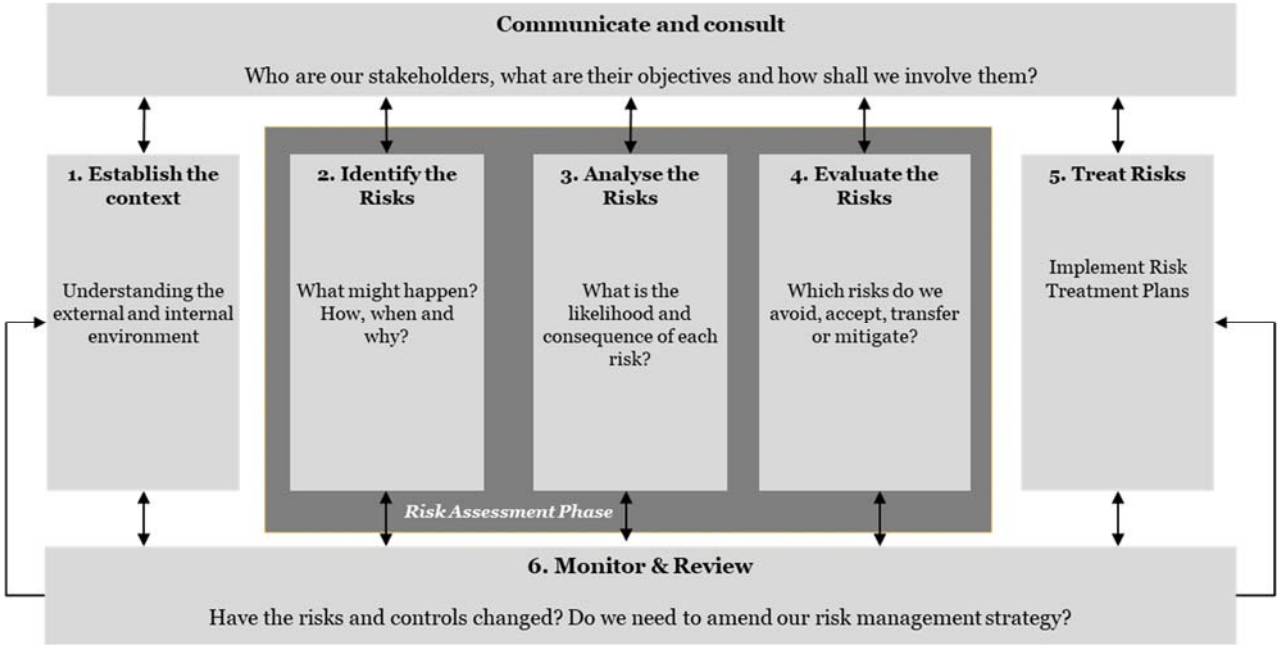
Risk capacity and appetite drive the risk tolerance levels of CS Energy, and these are set regularly with the Executive General Managers to reflect changing capacity and appetite levels and to reflect operational risk requirements.

Risk tolerances are outlined in Appendices 2 & 3. These appendices may be reviewed by the Board without a full review of this Framework and must be reviewed on an annual basis as a minimum, contemporaneously with CS Energy's Risk Capacity and Risk Appetite.

6 RISK MANAGEMENT

A diagram of the ISO 31000:2018 Risk management process is shown in Figure 2 and is intended to be a continuous loop. Each step of the process is described below, whilst guidelines for capturing this data in a risk register are provided in Appendix 4.

Figure 2 - Risk Management Process (ISO 31000:2018)



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), HAZARD 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 the periods between workshops, R&C will work with Risk Owners and Risk and Compliance Facilitators to maintain up-to-date risk information to ensure the effective management and reporting of risks. Significant changes in strategy, operations or the external environment may also prompt a review process.

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 level of risk 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 6. Bowtie risk analysis involves:

1. Identifying the causes of the risk event identified in 6.2, and the consequences if the event were to occur.
2. Determining an Inherent Risk Level by measuring the likelihood of each consequence occurring for that risk event assuming no controls or other mitigating factors are in place. The level is determined using the consequence and likelihood tables in Appendix 5 - CS Energy Risk Matrix.
3. Identifying controls that are already in place. Controls can be preventive (reduce the consequence and likelihood of a risk event occurring) or mitigating (reduce the consequences of an event after it has occurred). In some cases, controls may not yet exist.
4. 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 (where deficiencies exist in the design of the control and it is performed in an ad-hoc manner or not at all), Intermediate (where the control is well-designed and consistently performed) or Strong (where the control is well-designed and always performed).
5. Assigning a Residual Risk Level 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 5 - CS Energy Risk Matrix.
6. Identifying and assigning roles for the risk, including a Risk Owner with the appropriate seniority from the assigned business unit based on Figure 5 in Appendix 5 - CS Energy Risk Matrix. The Risk and Compliance Owner 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 and Compliance Owners are also required to periodically assess the appropriateness of risk ratings and to flag emerging issues to the Executive Leadership Team.

6.4 Risk Evaluation

Risk evaluation is a decision-making activity taking into account the results of the risk analysis and assessing these against the CS Energy Risk Appetite, appropriate risk tolerances, corporate objectives, legislation, regulations and corporate policies that may mandate or guide the response.

A decision is made whether to:

a) Accept and tolerate the risk with its Residual Risk Level — this may occur where the Residual Risk Level falls within the CS Energy Risk Appetite and risk tolerances, or where no action can be taken to further mitigate the risk (e.g. the costs of treatment exceed the benefits gained or the circumstances are beyond CS Energy's influence and control). In this case the Planned Risk Level will be the same as the Residual Risk Level. Approval must be sought to accept a risk outside CS Energy tolerance levels;

b) Treat the risk by applying further risk treatment – this may occur where the Residual Risk Level exceeds the risk tolerances set in the CS Energy Risk Appetite (see 6.5 Risk Treatment). In this case the Residual Risk Rating will exceed the Planned Risk Level; or

c) Avoid the activities and situations which could give rise to the risk – this may occur where the Residual Risk Level is higher than CS Energy risk tolerance levels and cannot be reduced to an acceptable level through risk treatment.

6.5 Risk Treatment

Where existing controls do not reduce a Residual Risk Level 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 level of risk to within required tolerances, which is the Planned Risk Level. 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 plans that outline the actions to be undertaken are developed by the Managers who are accountable and responsible for the particular risk, in conjunction with the R&C team. Due dates and Action Owners, who are responsible for ensuring actions are completed as required by the due date and for providing status updates on progress, are nominated by the Risk Owner. A Planned Risk Level (i.e. target risk rating) is set to ensure that the residual risk remains within risk appetite. Treatment plans 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 10:

Monitoring and Review will assist in providing regular information as to how the risk is impacting the business.

Upon completion of a treatment action, the Risk Compliance 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 Level should be reassessed.

Treatment actions are planned to reduce the level of risk to within required tolerances, which is the Planned Risk Level.

7 COMPLIANCE MANAGEMENT

The basis of CS Energy's compliance management is outlined below.

7.1 Compliance Management Structure

The Compliance Management is integrated with the broader Enterprise Risk Management, but also includes:

- Compliance Requirements Registers;
- Obligations management;
- Compliance attestation process;
- Compliance Certificate; and
- Supporting tools and processes (including policies and procedures).

7.2 Compliance Requirements

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 compliance

requirements must be identified, assessed and managed effectively to ensure CS Energy remains compliant.

For this reason, the R&C team, Risk & Compliance Owners, Risk & Compliance Facilitators and other relevant employees monitor the external and internal business environment for new, changed or obsolete compliance requirements This monitoring may occur through relationships and communication with regulators, advisors and/or industry and professional associations. In addition, regular regulatory newsfeeds are issued by an external provider to the R&C team, Legal, and other relevant staff.

Compliance obligations are subsequently updated (refer section 7.3 below), to take into account any changes in compliance requirements. 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.

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.

7.3 Compliance Risks

To assist in the prioritisation of risks, Compliance Risks (i.e. risks relating to not complying with CS Energy's legislative, regulatory or other requirements) are identified and recorded in the Governance, Risk and Compliance System. Compliance risks are analysed using the risk assessment process outlined in section 6.3 Risk Analysis, considering:

- Consequence – the outcome of an event. A single event can generate a range of consequences which can have an effect on objectives;
- Likelihood – the frequency or chance of the consequence affecting the objectives.

Controls are implemented, where practical, to prevent, detect or mitigate compliance risks and their impacts. Controls may include policies and procedures, systems, reporting, training and/or other compliance management tools and documentation. Monitoring activities are determined dependent on risk level (refer to Section 10 Monitoring and Review).

7.4 Compliance Obligations

Compliance obligations are tasks that must be routinely undertaken to maintain compliance with the requirements listed in the Registers. Management of compliance obligations is a de-centralised responsibility of line management with support, tools and reporting provided by the R&C team.

Compliance obligations are recorded in the Governance, Risk and Compliance System to enable tracking and reporting on the completion of required tasks. For each obligation, information is recorded in relation to the timing, source, due date and person responsible for completing obligations and updating the system accurately and in a timely manner.

7.5 Compliance Attestation Process

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.

8 COMMUNICATION, CONSULTATION AND ESCALATION

Communication and consultation is 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. As important are the appropriate escalation and reporting of risks to ensure that key stakeholders and management are aware of risks and the potential impacts.

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 Executive Leadership Team and Committees, or with external stakeholders such as relevant government bodies, contractors and regulators.

9 RESOURCES AND TRAINING

Risk Owners and Control 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.

There is a Training and Awareness Plan, part of this framework, which facilitates a clear and effective communication to build good awareness of risk management throughout the organisation, whilst ensuring that training is appropriate to positions.

10 MONITORING AND REVIEW

10.1 Structure of Risk Registers

CS Energy has a 3-tier hierarchy of risk registers. Definitions of each risk register and risk assessment tier, and the criteria for the escalation or aggregation of risks are described in Table 1 and illustrated in Figure 3 below.

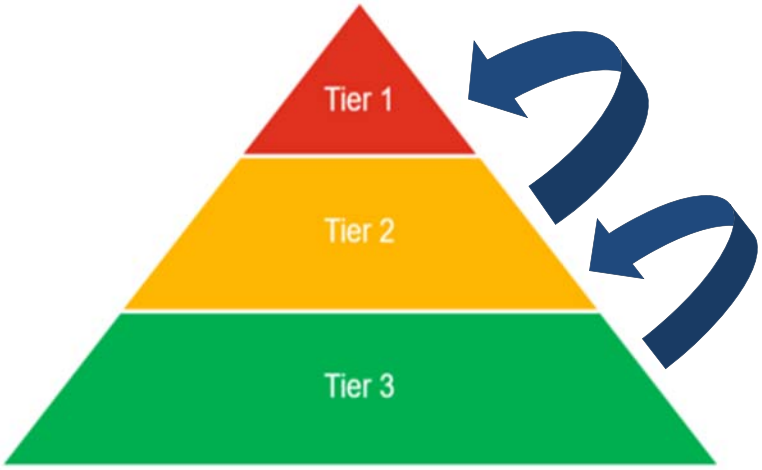
Table 1: Risk Register Hierarchy and Escalation Criteria

Risk Register Hierarchy and Escalation Criteria		
Name	**Description**	**Aggregation / Escalation Criteria**
Tier 1 – **Group Risk Register**	All risks from lower tiers escalated / aggregated to Group Risk Register. **Note**: All Tier 1 risks are recorded and monitored in the R&C System.	Not Applicable
Tier 2 – **Site Risk Register**	Site risk registers include all of the material risks of each site but only “significant” and “high” risks are included in the Divisional EGM’s risk report. **Note**: All Tier 2 risks are recorded and monitored in the R&C System.	Risks to be aggregated to Tier 1 based on the Aggregation Methodology[1]

[1] Aggregation methodology is defined in the CSE Aggregation / Escalation Guidelines document, dated Sep-2018 .

Risk Register Hierarchy and Escalation Criteria		
Name	**Description**	**Aggregation / Escalation Criteria**
Tier 3 – Operational Risk Registers	Operational view of risks for front line management and staff. These will also include the risks from the project risk registers. **Note**: Tier 3 risks may be recorded and monitored in the R&C system or in another system as deemed appropriate by the relevant EGM.	Risks to be aggregated to Tier 1 based on the Aggregation Methodology[1]

Figure 3: Illustration of risk register hierarchy and escalation



- All strategic risks plus escalated / aggregated risks from Tier 2, representing the level of information for ELT / Board
- Tier 3 risks are aggregated to Tier 2 level to provide the level of information the EGM and direct reports require to make decisions at divisional level
- Operational view of risks for front line management and staff

10.2 Risk Reviews

Tier 1 and Tier 2 risk registers are reviewed at least quarterly in accordance with normal business processes (e.g. Plant risk assessments are conducted as part of the ongoing technical reviews).

The risk review process comprises:

i. An annual strategic risk review held with the ELT and Board as part of the annual strategy "Awayday" to ensure the Group Risk Register remains aligned with the strategic plan, and to identify any emergent risks.

ii. Divisional/Site Risk Registers reviewed annually to ensure all risk registers remain aligned to business plans, and to identify any emergent risks.

iii. Quarterly refresh of the Group Risk Register by the ELT and ARC. Each quarterly review includes a "deep dive" into a selection of risks on the Group Risk Register to ensure that all Group Risks are reviewed at least once during the year.

iv. People safety, process safety and environmental risks are identified and managed in accordance with the H&S Plan or Environmental Plan. Key risks are escalated and aggregated, as required, in accordance with the escalation criteria described below.

v. Compliance risks to achieving the objectives and executing the role responsibilities set out in this document, reviewed annually by key stakeholders identified within the framework;

vi. Risk action plans resulting from risk reviews maintained and tracked centrally by GR&C.

10.3 Risk Assurance

Risk Assurance is designed to provide comfort at all levels that risks, including compliance risks, are being adequately managed, that the controls in place are effective and that any issues have been identified, reported and actioned. The assurance framework is a risk-based approach that provides varying degrees of assurance.

Monitoring will occur based on the "Three Lines of Defence" approach outlined below, and may be conducted by the business unit, the R&C team and/or the Assurance team. Monitoring activities may include management oversight, system reporting, reviewing control effectiveness, implementation of treatment plans and/or full internal audits. External audits are also conducted where required by legislation. Monitoring may identify new risks, recommendations in relation to current controls or areas of non-compliance.

	Low Residual Risk	Moderate Residual Risk	Significant Residual Risk	High Residual Risk
Business Unit	On the radar – minimal active monitoring.	Six monthly monitoring at least, unless reasonable and embedded in controls to do more.	Quarterly monitoring and reporting required. Possible implementation of treatment plans.	Treatment Plans to be instigated and implemented with monthly review.
GR&C	Annual review of control effectiveness with business department.	Annual review of control effectiveness with business department.	Quarterly GR&C monitoring quarterly.	Monitor and assist in the implementation of treatment plans. Assist in building ongoing monitoring plans. Review control effectiveness each quarter.
Other Assurance	Nil	As requested.	Where an auditable area, include in cyclical audit program.	Where an auditable area, include in Assurance Plan, with annual review.

10.4 Issue and Breach Reporting

The reporting of compliance issues and risk incidents 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 by the Risk and Compliance Facilitators, as soon as practicable. Breaches may be reported through other channels for specific departments where procedures currently exist, such as Energy Markets, Health & Safety, and Environment, or anonymously if necessary through CS Energy's Whistleblower service.

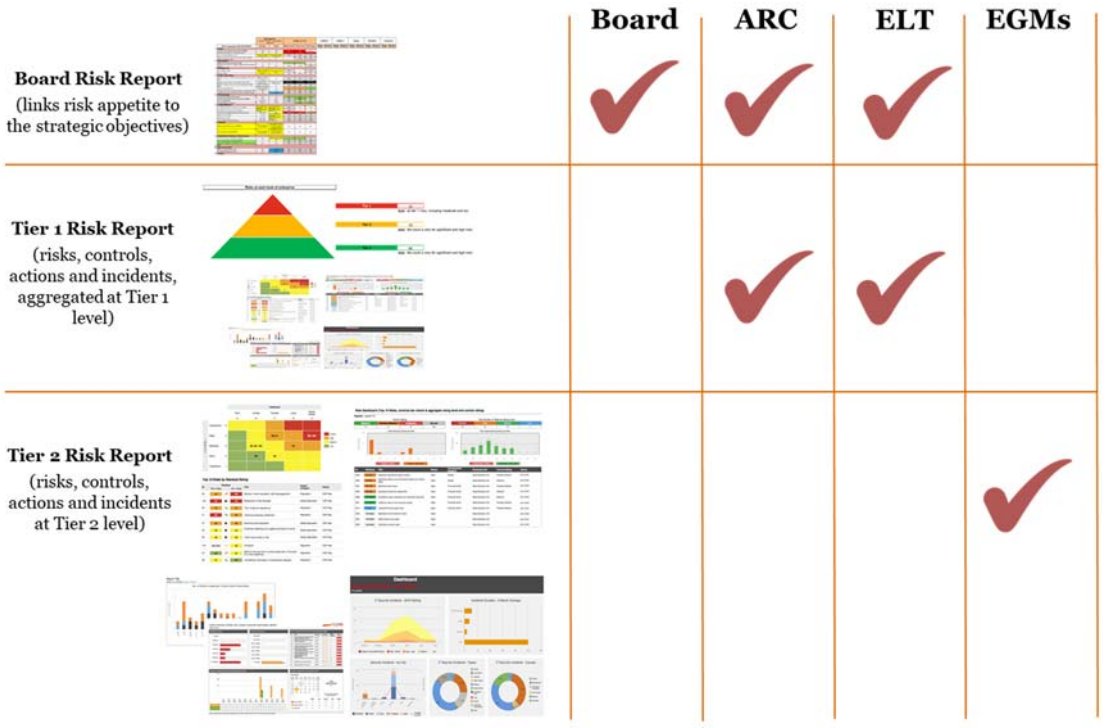
Material compliance breaches will be reported to the Audit and Risk Committee in the R&C Report (unless reported through to another Committee). Serious compliance breaches will be investigated as per the procedures outlined in CS-GOV-13 -Complaints and Investigations Handling.

11 REPORTING

11.1 Risk and Compliance Reports

Reporting at each level of the organisation is summarised in Figure 4. Contents of each report are discussed below:

Figure 4: Risk Reporting at all enterprise levels



Board Risk Report:

"Risk on a page" report summarising the current exposure to risk, by category, and compliance with the Risk Appetite Statement.

Tier 1 Risk Report:

An overview of the Tier 1 risks of CS Energy including: a summary of any 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 level of risk.

Tier 2 Risk Report:

An overview of the Tier 2 risks of each Site / Division including: a summary of any 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 level of risk.

Ad hoc GR&C Reporting:

Other information relevant to the activities of the R&C team.

11.2 Executive Leadership Team

The R&C team will provide additional reporting to the Executive Leadership Team on an ad hoc basis to support Executive Management in the performance of their responsibilities under this Framework.

11.3 Market Risk Committee

The Market Risk Committee, 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.

12 REVIEW AND CONTINUAL IMPROVEMENT

12.1 Framework Review

CS Energy's Enterprise Risk and Compliance Management 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, on an annual basis at a minimum, or more frequently to incorporate material business or regulatory changes.

The Audit and Risk Committee 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.

12.2 Compliance Program Review

Compliance requirements and obligations should be maintained on a continual basis to ensure they align with current legislative, regulatory and other requirements. The Compliance Requirements Registers and obligations will be reviewed on an annual basis by Executive General Managers, in consultation with the relevant Risk and Compliance Facilitator and the R&C team. Gap analyses may be conducted on an ad hoc basis to identify whether any compliance requirements or obligations are not being met or where procedures are not currently documented.

Regular review of policies and procedures, by the document owner, is necessary to ensure they are current and reflect any applicable changes in legislation, regulations or other requirements. Policies and procedures will be updated in the timeframes specified in each document, unless there are material changes which require the documents to be updated prior to the review date. Where new compliance requirements 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.

Other components of the compliance program will be reviewed as follows:

- Compliance risks will be re-assessed dependent on risk level and in line with the frequencies and responsible person/s outlined in the above table;
- Compliance Manuals will be updated periodically by the Legal department; and
- Compliance training will be reviewed and updated on an ad hoc basis by the Risk and Compliance Facilitator for the department receiving the training, in conjunction with the GR&C Team.

13 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 Attestation Process	A signoff completed by Executive General Managers on a quarterly basis to certify that key compliance requirements and obligations have been met.
Compliance requirement	A requirement that must be adhered to, as specified by legislation, regulations, industry standards or codes.
Compliance Requirements Register	The register of all identified CS Energy compliance requirements.
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.
Event	A risk that has 'eventuated' and which leads to consequences. Alternate terms 'Incident' or 'near miss' (without Consequences).
Inherent Risk	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.
Likelihood	The frequency or chance of the consequence affecting the objectives.
Objective	A goal of the business including explicit metrics and timeframes.
Obligation	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.

Term	Definition
Planned Risk	The target level of risk to be achieved when the risk has been mitigated to a tolerable level (as set by the Risk Owner) 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 Level will be the same as the Residual Risk Level.
Residual Risk	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 Aggregation	The consolidation of multiple detailed risks into a fewer number of higher level risks.
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
Risk and Compliance Facilitator	Risk and Compliance Facilitators are appointed by the GR&C Manager to facilitate the execution of the manager's responsibilities in relation to risk management and compliance (typically for a division/function).
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 Register	The register of all identified CS Energy risks, which is maintained in SAP and records the key information for each risk, control and action, and supports enterprise risk reporting.
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 Capacity	The amount and type of risk an organisation is **able** to accept in the pursuit of strategic objectives
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 setting the tolerable or Planned Risk Levels.
Risk Register	A library of risks including the related root causes, consequences, controls and any related actions.
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.

Term	Definition
Risk Tolerance	Acceptable level of variance around the achievement of targets relating to specific risks at an entity or functional level.
Treatment action	Work undertaken to implement, improve or modify a control. See also 'Response'. Treatment Plans are documented for compliance risks with a Residual Risk Level of Medium or High. Treatment actions are designed to improve controls and reduce the Residual Risk Level.

14 REFERENCES

Reference No	Reference Title	Author
"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/13/11406"	Procedure – CS-RISK-03 – Enterprise Risk Management Guideline	CS Energy
"B/D/13/15225"	Form - S2122 - Operations Plant Risk Assessment Template	CS Energy

15 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 - RISK CAPACITY AND RISK APPETITE

Risk capacity is the amount and type of risk an organisation is able to withstand in pursuit of its strategic objectives. This is the starting point for the development of a robust risk management framework.

		FY 19	FY 20	FY21
Total Debt to EBITDA Ratio	QTC Debt Covenant		< 3x	
	Current Total Debt to EBITDA Ratio	1.2	1.2	1.2
	Headroom (EBITDA, $M)	**222**	**230**	**205**
EBITDA Interest Coverage Ratio	QTC Debt Covenant		> 4x	
	Current EBITDA Interest Coverage Ratio	10.5	14.1	13.4
	Headroom (EBITDA, $M)	**228**	**270**	**247**
Total Debt to Capital Ratio	QTC Debt Covenant		< 60%	
	Current Total Debt to Capital Ratio	38%	37%	36%
	Headroom (Debt, $M)	**614**	**662**	**705**
	Total Headroom (EBITDA, $M)	**222**	**230**	**205**

Risk Appetite defines which, why and how much risk the business is willing to take. Used effectively, Risk Appetite provides a structure within which opportunities can be pursued and downsides mitigated by setting out which, why and how much risk the business is willing to take. A Risk Appetite is a statement of intent only, and its value is limits and targets for the delivery of CSE's strategic priorities, incorporated in the intention statements.

2019 Risk Appetite Statements

1. Strategic Risk		
CS Energy's overarching strategy is crafted around our purpose: delivering energy today, powering your tomorrow. By 2030, we will provide 50 percent of Queensland's baseload generation capacity and at least 30 per cent of our earnings will be derived from innovative products and services, independent of our physical assets. Specific strategies to deliver this mission and vision will be assessed on a case-by-case basis but must always be undertaken within CS Energy's risk capacity constraints. Strategic Risk will be determined by monitoring the impact on Gross Margin at Risk and Revenue at Risk.		
Risk Measures	**Tolerance**	**Target**
Gross Margin at Risk	Tolerance managed within market risk appetite	Target will be set by the Board.
Revenue at Risk		
2. Plant Performance Risk – insured and uninsured		
At CS Energy, plant performance is to be managed within a specified range determined by having regard to market outlook and related commercial returns, plant age, condition and technical capability. The asset maintenance strategy will be developed and implemented to allow flexibility within this range. Insurance products are used to mitigate the risk of extreme events.		
Risk Measures	**Tolerances**	**Target**
Thermal Plant Unplanned Outage Rate	<12%	<10%
CSE Owned Thermal Portfolio Commercial Availability	>75%	>80%
Insurance Deductibles	Up to 60 days	60 days
Start Reliability for Wivenhoe	>95.0%%	98.0%
3. Safety Risk		

CS Energy's belief is that safety always comes before production. We have no appetite to expose people to health and safety risks that cannot be effectively managed and aim to minimize the risks to the extent that is reasonably practicable. Our appetite is to operate in low safety risk areas.

Risk Measures	Tolerances	Target
Total Case Recordable Frequency Rate (TCRFR)	<4.0	<3.0
No repeat category 3 or category 4 incidents	Nil	Nil
Process Safety Confidence Level	Positive trend from June 2018 baseline	20% improvement from June 2018 baseline
Moderate and above safety related audit and investigation actions completed on time.	Nil	100%

4. People Risk

CS Energy is committed to attracting and retaining key talent necessary to meet its strategic objectives, and the creation of a safe and constructive culture.

Risk Measures	Tolerances	Target
Number of leaders at full performance (Individual Achievement Plan)	Positive trend from 2018 FY assessment (69%)	80%
Employee Culture Climate Survey (OCI) – March 2019	Positive trend from 2017 FY survey	20% improvement from 2017 FY survey
Number of ready now successors for leadership roles (Nine Box)	Positive trend from 2017 assessment (11%)	20%
Women in leadership roles	Positive trend from June 2018 (26%)	30%
Voluntary staff turnover within 12 months of starting with CSE	<20%	<10%

5. Regulatory Compliance Risk

Regulatory compliance is imperative for CS Energy's 'Licence to Operate'. As such, regulatory risks will be managed so as not to jeopardise this Licence, with a focus on regulatory engagement.

Risk Measures	Tolerances	Target
Act or Code breaches with potential fines	0	0
Regulatory Compliance Investigation actions completed on time	Nil	100%

6. Environmental Risk

CS Energy will take a prudent approach to the management of its environmental social licence to operate, with an emphasis on complying with relevant CS Energy site environmental approvals and environmental legislation and working consultatively with the regulator and communities in which we operate. We proactively manage our operating sites to minimise the risk of a Significant Environmental incident occurring.

Risk Measures	Tolerances	Target
Significant Environmental Incidents	0	0
Year on year trend in community complaints (under reputational risk)	Nil	No increase on previous year
Moderate and above safety related audit and investigation actions completed on time	Nil	100%
Environmental Awareness training completed by CSE employees on time	>95%	100%

7. Reputation Risks

At CS Energy we work to actively build, maintain and reinforce our brand and reputation in the communities in which we operate and with all key internal and external stakeholders. We will balance commercial considerations and community obligations in all our decision-making.

Risk Measures	Tolerances	Target
Year on year trend in community complaints	Nil	No increase on previous year

Business Continuity Plan tested	Nil	Annual
Compulsory internal staff refresher Code of Conduct training	Nil	Annual
Fraud Risk Management Review	Nil	Annual

8. Fuel Price and Foreign Exchange Risks

Given that fuel inputs are essential to the operations of CS Energy, we accept that we are exposed to a certain degree of fuel price risk. However, we expect there is appropriate action taken to hedge exposures given certain market conditions to reduce potential earnings variability.
For current FX exposures arising from capital or operational expenditures, we expect there is appropriate action taken to hedge exposures given certain market conditions to reduce potential earnings variability.

Risk Measures	Tolerances	Target
Percentage of fuel price exposure to be hedged	Refer to Risk Limits standard	
Percentage of FX exposure to be hedged		

9. Other Financial Risks

CS Energy has limited appetite in accepting risk associated with counterparties that have not undergone proper due diligence and credit quality review within the approved counterparty list. Exposures must also adhere to the Portfolio and Counterparty credit limits for each of the external rating groups.

Risk Measures	Tolerances	Target
Portfolio Credit-Adjusted Potential Future Exposure	$5m - $13m	$10m

10. Electricity Price Risk

To mitigate the electricity price risk associated with CS Energy's generation portfolio, cash flows from generation assets are hedged using derivatives and retail contracts within defined limits. CS Energy only has appetite for risks where the financial or other returns are commensurate with the risks, and where it complies with our various risk limits and risk management policies.

Risk Measures	Tolerances	Target
Hedge Tolerance Band	+/- 200MW	Refer to Risk Limits Standard
Daily Spot Loss Limit	$0m - $5m	
Value-at-Risk for Propriety Trades	$0m - $3m	Not applicable

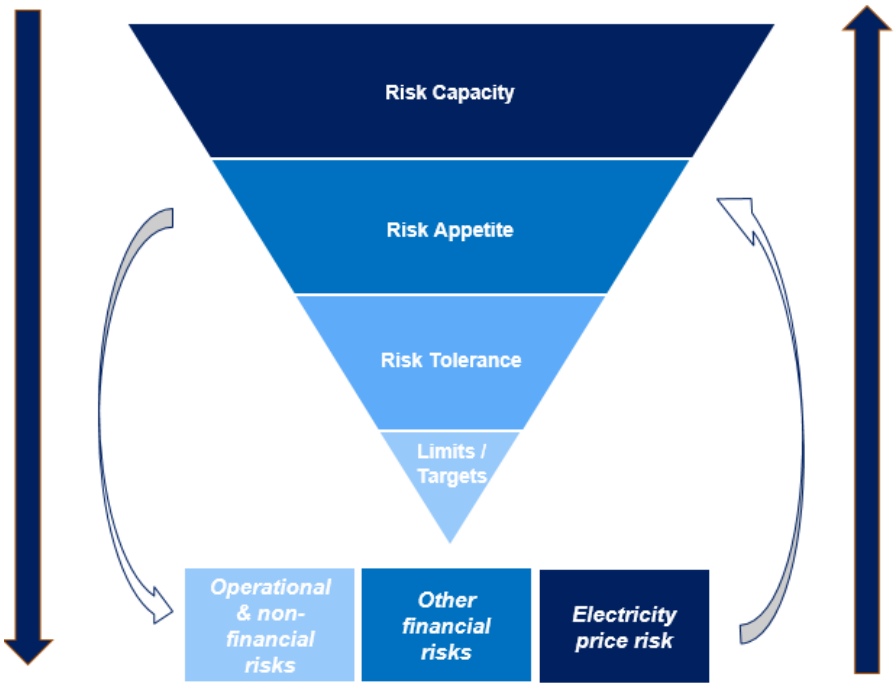
APPENDIX 2 - RISK OPTIMISATION APPROACH

Risk Appetite provides a structure within which opportunities can be pursued and downsides can be mitigated by setting out which, why and how much risk the business is willing to take. Its value is derived by incorporating the intention statements into limits and targets for the delivery of CS Energy's strategic priorities.

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.

From the bottom-up, the business will identify and measure current business risks and assess impact of business risks on the organisation. This approach will provide an aggregated view of the impact of business risks to ensure alignment between the Board's view of risk appetite and the business' current risk landscape.

Risk Tolerance limits are appropriate for a point in time based on risk capacity and appetite. Risk Tolerance levels must be reviewed annually or when a significant change to organisational structure, financial position or external factors occurs.



*** This Risk Tolerance table is in draft only requiring further consultation and discussion and to ensure appropriate alignment with business planning processes. This is provided as an example of the approach only.**

APPENDIX 3 - RISK CATEGORIES

Risk Type	Risk Category
Health, Safety & Security	Design of Health, Safety & Security policies, procedures, practices and governance
	H&S Culture
	Injury prevention
	Occupational health and hygiene
	Physical security
Environment	Design of Environmental governance
	Implementation of Environmental framework
Enterprise Risks	Business Resilience
	Contractor Management
	Enterprise Risk Framework
	Fraud
	Insurance
Financial	Cash Management
	Financial control
	Funding Management
	Tax / Accounting
Plant Integrity	Asset management governance/framework
	Process Safety Governance and Framework
	Kogan/Callide/Wivenhoe Plant Integrity / Process Safety
	Asset management governance/framework
Trading (market)	Credit Risk
	FX
	Market risk (incl. liquidity)
	Implementation of Trading framework
Legal and Regulatory	Legal and corporate governance
	Regulatory compliance
People and Culture	Culture
	L&D
	Talent and succession (including Strategic workforce planning)
	Workplace relations
Strategic Risks	Business planning cycle
	Diversification of Revenues
	Cost of operations
Stakeholder relations and governance	Change in government policy
	Callide JV
ICT	Technology Risk
Project	Investment governance
	Project Execution
	Project management framework

APPENDIX 4 - RISK REGISTER

Outlined below are the required fields and information for a fully detailed risk summary within a risk register.

Process Step	Field	Sub-Field	Content
Establish the Context	Objective	N/A	The goal intended to be accomplished. This may be a strategic, operational or project objective.
Risk identification	Risk name	N/A	Short title describing the risk
	Risk Description	N/A	Detailed description of the risk, including a summary of the key causes, the risk event and the key consequences, enabling stakeholders outside of the team to understand what the risk is (and is not) about. It may be helpful to the describe the risk as follows: => 'Due to [key cause] there is a risk that [risk event] resulting in [key impact]'
	Risk Owner	N/A	Individual accountable for the management of the risk or set of risks
Risk Analysis	Root Causes	N/A	Factors which if left uncontrolled, could result in the risk event occurring
	Consequences	N/A	Description of the key consequences or outcomes if the risk were to be realised. Refer to the consequence categories in the Client Risk Matrix (i.e. Health and Safety, Environment, Financial, Reputation and Brand, Legal and Compliance, Social and Cultural)
	Consequence Rating	N/A	Many risk events have more than one consequence. The Consequence rating records the inherent risk rating for each applicable category of risk
	Inherent Risk	Maximum Foreseeable Exposure (MFE)	An assessment of the credible worst-case scenario for a risk, assuming the risk event occurs in the absence of any and all control. MFE may be expressed in multiple criteria (e.g. a single risk event can have financial, reputational and regulatory MFE). All applicable MFE's must be recorded for each risk.
		Inherent Likelihood	Use the risk likelihood tables to assess the likelihood of the MFE occurring
		Inherent Consequence	Apply the risk consequence tables to the MFE to assign a consequence rating (catastrophic, major, moderate etc) should the risk event occur with no controls in place
		Inherent Risk Rating	Apply the risk matrix (heat map) to the inherent risk likelihood and consequence to assign an inherent risk rating.
		Rating Basis	Description of the scenario and explanation of how and why the MFE level was determined, including the basis of the assessment (e.g. Net Present Value), containing sufficient detail to allow for review and re-performance of the assessment
	Controls	Control	A mechanism which supports the achievement of objectives by reducing the likelihood or consequence of a risk event

Process Step	Field	Sub-Field	Content
		Preventive or Mitigating	A preventive control reduces the likelihood of a risk event occurring. A mitigating control reduces the consequence of the risk should it occur.
		Control Effectiveness	A rating indicating the current level of risk considering controls that are currently in place and effective.
		Control Status	"Operational" means that the control is operating today. "Planned" may be used to describe controls for future projects where the control is not operational today but will be operating when the project is implemented.
		Control Owner	An individual accountable for the design and effectiveness of a specific control in relation to the management of a specific risk.
	Residual Risk	Residual Likelihood	Apply the risk likelihood tables to assess the likelihood of a risk event occurring after consideration of the controls in place.
		Residual Consequence	Apply the risk consequence tables to assess the consequence, after consideration of controls in place, should the risk event occur.
		Residual Risk Rating	An assessment of the current level of risk considering controls that are currently in place and effective. Residual Risk Rating is assessed in accordance with the Risk Matrix (or heat map) by plotting the consequence and likelihood scores
		Rating Basis	Explanation of how and why the consequence and likelihood levels were selected containing sufficient detail to allow for review and re-performance of the assessment. Justify with a scenario.
Risk Evaluation	Target Risk Rating		The level of residual risk that is acceptable to the organisation. This should be based upon the Risk Appetite / Tolerance of the organisation
	Risk Decision		Risk Owner to consciously decide and capture how the risk is to be treated: +> Accept - Current level of risk accepted, without applying any additional action to reduce or further treat the risk. For exposure to risk in the future (e.g. projects), this refers to key controls which will be in place at the time of exposure to the risk => Reduce - Further action to be undertaken to decrease either the likelihood of the risk occurring or the impact of the consequences => Transfer - Some part of the risk is shared or borne by a third party => Avoid - A decision not to engage in the activity giving rise to the risk
Treat Risk	Action Plan		Actions designed to improve the control of risk. Note that where Risk Health is rated as 'Unsatisfactory' or 'Some Weakness', risk control actions must be identified and assigned to Action Owners to improve the controls in order to achieve an acceptable RH & CRR

Process Step	Field	Sub-Field	Content
	Action Owners		Individuals accountable for the performance and close-out of assigned actions
	Due Date		Timeframe by which each action will be completed
Monitor, Review and Report			Current status of each agreed risk control action in terms of progress of implementation against agreed milestones

APPENDIX 5 - CS ENERGY RISK MATRIX

	Consequence Scale					
Category	**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 Multilple fatalities Stolen or impaired asset resulting in plant shutdown
Environmental	Small contaminant release or land disturbance, localised on-site area affected. Routine short-term clean-up/remediation. Category 1 Incident equivalent resulting in an onsite impact.	Moderate contaminant release or land disturbance, localised on-site. Routine short-term clean-up/remediation. Category 2 Incident equivalent resulting in an onsite impact.	Moderate contaminant release or land disturbance, localised on-site. Routine short-term clean-up/remediation. Category 3 Incident equivalent resulting in an onsite impact	Large contaminant release or land disturbance, localised off-site. Short-term clean-up/remediation. Category 3 Incident resulting in an offsite impact	Large contaminant release or land disturbance, localised off-site. Long-term clean-up/remediation, potentially irreversable. Category 4 Incident equivalent resulting in an offsite impact.	Very large contaminant release, extensive off-site area affected. Complex long-term clean-up/remediation, irreversible. Category 4 Incident equivalent resulting in an offiste impact.
Financial impact (excluding insurance) **Note: Refer below to calculate plant performance risk.**	<$2m loss in a year	Up to $5m loss in a year	Up to $60m loss in a year	Up to $120m loss in a year	Up to $200m loss in a year	>$200m loss in a year
Reputation/ Stakeholder Relations (Internal & External)	-No disruption to corporate objectives - Community/stakeholder concerns can be dealt with via normal engagement - Local site issue - Isolated public dissatisfaction with CSE	- Corporate objectives are impacted by an issue - Key stakeholders exercise their authority in response to the issue - Influential community figures exercise their influence within the community - Localised and limited negative media	-Delivery of corporate objective(s) is prevented or delayed (>3 months) - 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	- Pursuit of corporate objectives is severely disrupted (>6 months) - 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	- Pursuit of corporate objectives is severely disrupted (up to 12 months) - Creates a persistent 'headline' issue for the Shareholder - Significant and recurring negative state wide media and/or parliamentary attention - Extensive Shareholder invervention 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	- CSE's achievement of its objectives is permanently disrupted/jeopardised - 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 shuting 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

Level of Risk Probability	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.

Likelihood Scale	Level of Risk Calculator	1. Minor	2. Low	3. Medium	4. Major	5. Severe	6. Catastrophic
A	**Highly Likely**	Low	Moderate	Significant	High	High	High
B	**Likely**	Low	Moderate	Significant	Significant	High	High
C	**Possible**	Low	Low	Moderate	Significant	Significant	High
D	**Unlikely**	Low	Low	Low	Moderate	Moderate	Significant
E	**Rare**	Low	Low	Low	Low	Low	Moderate

Plant Performance Risk:

Plant performance risk will be calculated on the following basis:

1. Assess the maximum foreseeable outage in terms of equivalent days loss of availability, based on incident management data
2. Assess the plausible worst-case scenario in future (if different from (1) above
3. Convert (2) above into loss of availability in MWhrs
4. Convert into financial consequence of loss of availability based on $/MWhr provided by Finance.
5. Assess the cost of remediation in Australian dollars
6. Calculate the total cost of outage (6=4+5)
7. Apply the consequence rating above.

By way of guidance, the financial consequences are broadly aligned to the following outages at each site

Site	1. Minor	2. Low	3. Medium	4. Major	5. Severe	6. Catastrophic
Plant Performance	Kogan: up to 2 days offline equivalent Callide B/Callide C: up to 4 days offline equivalent	Kogan: 3 to 7 days offline equivalent Callide B/Callide C: up to 14 days offline equivalent	Kogan: 8 to 60 days offline equivalent Callide B/Callide C: up to 120 days offline equivalent	Kogan: 61 to 120 days offline equivalent Callide B/Callide C: up to 240 days offline equivalent	Kogan and Callide: 121 to 240 days offline equivalent Callide: up to 365 days offline equivalent	Kogan: > 240 days offline equivalent *Callide: > 365 days offline equivalent

* The definition of catastrophic for Callide B & C reflects the view that an outage of more than 1 year at any plant would be catastrophic regardless of the financial consequence.

APPENDIX 6 - 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.