CS ENERGY PROCEDURE FOR

BUSINESS CONTINUITY MANAGEMENT FRAMEWORK AND PROGRAM
CS-RISK-09

Responsible Officer: Senior Governance, Risk and Compliance Advisor
Responsible Manager: Group Manager Governance Risk and Compliance
Responsible Executive: Executive General Counsel and Company Secretary

DOCUMENT HISTORY

Key Changes	Prepared By	Checked By	Approved By	Date
Initial Release	AON/RiskLogic L Kayess	D Clarke	K Hawker	30/09/2016

CONTENTS

1 PURPOSE

The purpose of this Framework is to outline CS Energy Limited's (CSE) approach to developing and maintaining an effective Business Continuity Management Program. This includes the objectives and scope of the program, leadership requirements, roles and responsibilities, team structures, workflows for each part of the Business Continuity lifecycle and processes for monitoring performance.

As a Queensland Government Critical Infrastructure Asset, the objective of a Business Continuity Program is to maintain electricity generation and market participation for Queenslanders and other key stakeholders by minimising the impact that an unplanned event could have on the viability of the organisation and the provision of its customer services.

The goal of this Business Continuity Management Program is therefore to ensure the operational integrity of critical business functions and to ensure that such business functions can be maintained or restored within acceptable timeframes should a business continuity event disrupt CSE's operations.

2 SCOPE

The scope of Business Continuity Management (BCM) covered by this Framework includes all business areas. It includes all staff within these business areas, that:

- Are designated with responsibilities for the management of business continuity activities, prior to or proceeding a business continuity event.
- Affected by any business continuity event and/or any staff responsible for undertaking any actions in relation to the management of, or response to, a business continuity event.

3 RESPONSIBILITIES AND ACCOUNTABILIITIES

This section addresses the governance responsibilities and accountabilities for Business Continuity, refer to Section 8 for Crisis / Recovery team responsibilities.

3.1 Board

The Board has approved the Governance, Risk and Compliance Policy and has delegated the endorsement and approval of all Business Continuity documents to CSE Management (Executive Leadership Team).

3.2 Audit and Risk Committee

The Audit and Risk Committee has responsibility for approving and overseeing the operation, management and implementation if the Governance, Risk and Compliance Policy and the Business Continuity Management Framework.

3.3 Executive Leadership Team

The Executive Leadership Team has responsibility for:

- The management of the organisation's Business Continuity Program as part of its corporate governance role.
- Providing visible support and endorsement for BCM by communicating the importance of effective business continuity management and promoting continual improvement.
- Ensuring that appropriate financial and people resources are available to establish and manage an effective program.

- Ensuring the integration of this Business Continuity Program into the organisation's business processes.

3.4 Group / Site / Functional Managers

The Group, Site and Functional Managers have the following responsibilities within their site/function:

- With support from Governance, Risk and Compliance, coordinate updates to Business Continuity Plans to reflect changes within their respective business area.
- Approve all material amendments to individual Business Continuity Plans.

3.5 Governance, Risk and Compliance

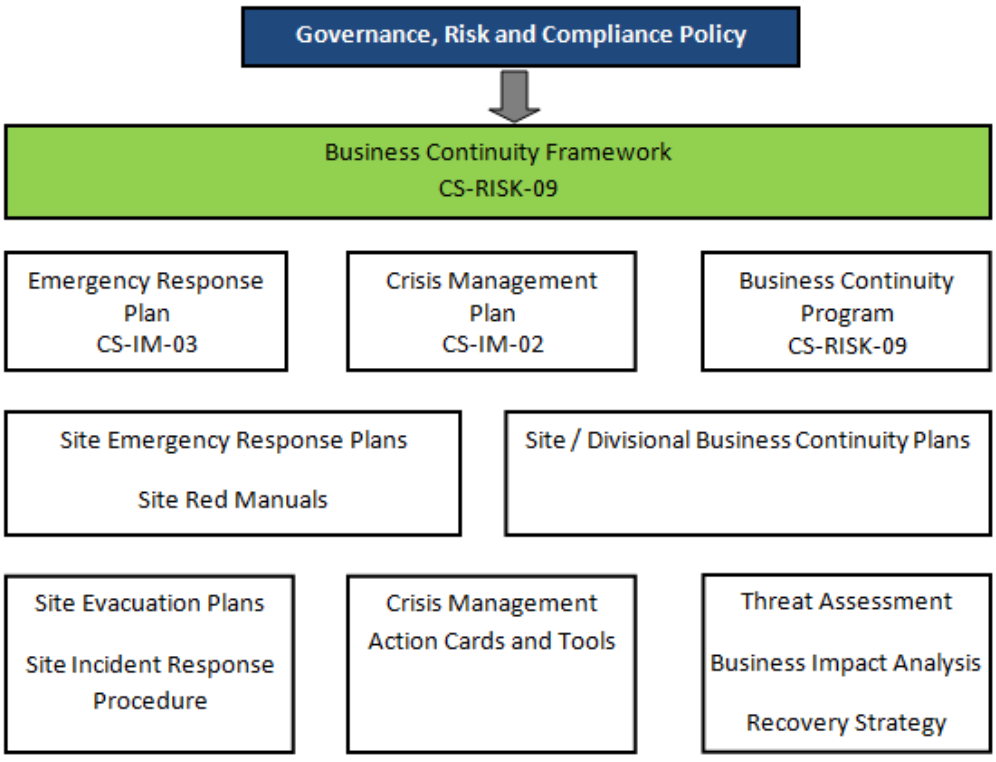
The Governance, Risk and Compliance (GRC) team has responsibility to:

- Approve the content of, and any subsequent amendments to, this Framework and distribute to the CSE Board Audit and Risk Committee.
- Coordinate regular reviews and testing of the validity, integrity and practicality of implementing Business Continuity Plans (BCPs).
- Coordinate the regular review and assessment of the recovery strategies outlined in BCPs as well as the adequacy of associated insurance, financial and resource provisioning. Where there is a material change in this assessment, BCPs are to be updated to take into account and to make adequate provisioning for these changes.
- Maintain the currency of this Framework document and provide updates on significant changes of BCPs to the CSE Board Audit and Risk Committee.
- Report on the performance of this Business Continuity Program to the CSE Executive Leadership Team and Board Audit and Risk Committee.
- Ensure the performance of this Business Continuity Program is reported to senior management and facilitate communications relating to the Business Continuity Program throughout CSE.

4 BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

Business Continuity Management (BCM) is a systemised approach for ensuring that critical business activities can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the financial, legal, regulatory, reputational and other material consequences arising from a disruption. The CSE Business Continuity Framework includes policies, standards and procedures that outline the CSE approach to preparing for and managing a disruption event.

CSE's BCM framework addresses requirements for each phase of the busines continuity lifecycle as detailed in the above diagram.



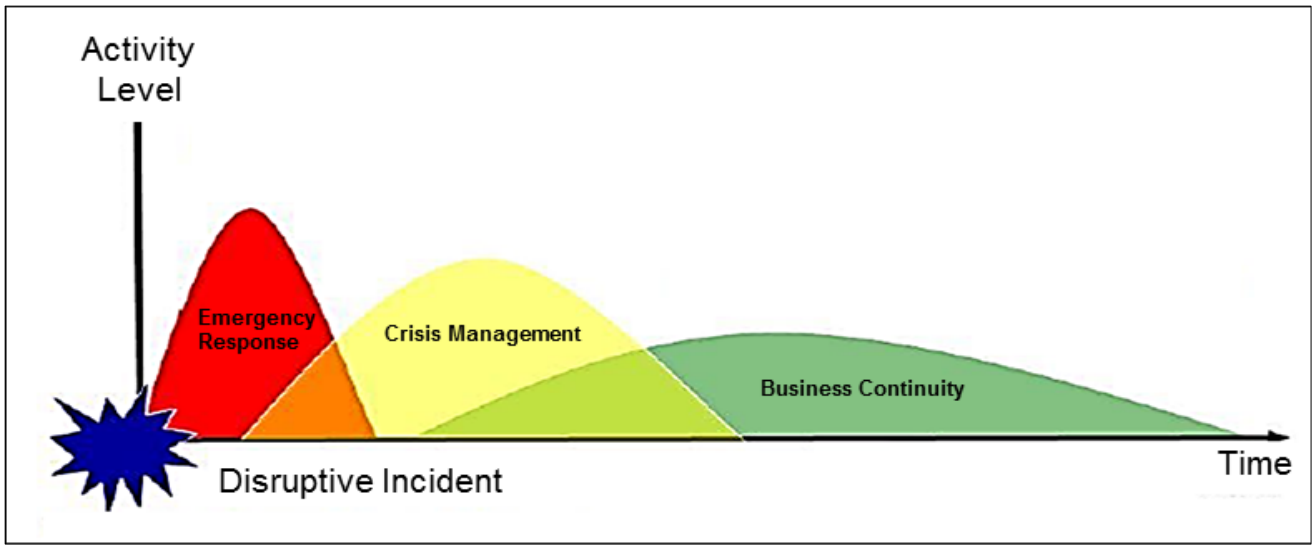
4.1 Crisis Management and Business Continuity

The following diagram illustrates the relationship between emergency response, crisis management and business continuity.

Emergency Response is the immediate response to a business disruption event (outage) and the primary concern is the protection of life and safety. This may require use of CSE Emergency Management Plans.

Crisis Management involves taking actions to stabilise the event to prevent further escalation and implementing strategies to minimise loss or damage to CSE. For disruptive events, this may involve the initial activation of CSE's Business Continuity Plans.

Business Continuity involves the use of alternative processes, capabilities and resources to ensure critical activities continue at acceptable levels of service (Continuity); and implementation of actions to return processes, capabilities and resources to business-as-usual levels (Resumption).



5 BUSINESS CONTINUITY PROGRAM

5.1 Purpose

The purpose of the Business Continuity Program, as part of the overall Business Continuity Framework, is to establish an effective, documented methodology to minimise the impact that an unplanned event could have on the viability of CS Energy and "protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise." (ISO 22301) This includes:

- Ensuring the welfare of personnel.
- Protecting the organisation's image and reputation.
- Maintaining an appropriate level of electricity generation.
- Maintaining an appropriate level of electricity market participation.
- Enhancing organisational stability.
- Reducing risk exposures and potential economic losses.
- Minimising legal liabilities.

5.2 Assumptions

In the event of a business disruption, CSE will not be operating at its normal capability and performance. The organisation will be operating a reduced capacity, or at a level which is not sufficient to perform and maintain critical business functions. This will require CSE to ensure that:

- Recovery timeframes and the corresponding Minimum Operating Requirements for critical functions, staff, plant and equipment, systems / applications and vital records are identified. This applies to both electricity generation assets and corporate support areas.
- The CSE Board approves the Strategy and allocated these resources to fulfil the requirements of approved Critical Business Functions.
- Resources have been allocated and made available based on the Minimum Operating Requirements of all sites and business areas in a disruption environment.
- The procedures and processes documented in Business Continuity Plans and other supporting plans be tested, maintained and updated on a regular basis.

5.3 Components

In accordance with the BCM lifecycle and best-practice standards, CSE's approach to BCM incorporates the following components:

- Development and ongoing review of an organisation-wide Threat Assessment which identifies all potential sources of disruption risk. These sources of risk will be analysed and prioritised for treatment. The Threat Assessment will also identify Plausible Disruption Scenarios.
- Development and ongoing review of a Business Impact Analysis (BIA) for all business areas which identifies all critical business functions, resources and infrastructure that would have a material impact on operations if disrupted.
- Identification of appropriate business continuity strategies for protecting infrastructure; stabilising the situation; continuing, resuming and recovering critical business functions; and mitigating the impacts of an event.
- Development, implementation and ongoing maintenance of Business Continuity Plans for relevant business areas.
- Management of a program for testing Business Continuity Plans and supporting procedures.
- Management of a program for training staff with designated responsibilities during a disruption and for the development of general BCM awareness for all staff.
- Management of a process for reviewing, evaluating and monitoring all components of CSE's Business Continuity Program on a periodic basis as defined by this Framework.

6 BUSINESS CONTINUITY MANAGEMENT TEAMS

6.1 CSE Executive Leadership Team (pre-crisis and post crisis)

The CSE Executive Leadership Team is responsible for:

- Overseeing the development, implementation and maintenance of the Business Continuity Program.
- Approving and allocating sufficient resources to facilitate resumption of Critical Business Functions within approved RTO's.
- Ensuring that this Business Continuity Program and BCM activities are reviewed on a periodic basis

6.2 Crisis Management Team

The Crisis Management Team (CMT) comprises executive and senior management and the appropriate support personnel representing the core functional areas of CS Energy necessary to respond to and resolve the crisis. The CMT is tasked to respond to a decisive and/or negative event, or series of events, that has the potential to significantly impact on, or destabilise CS Energy. Responsbilities include:

- Determining the strategy for ensuring an effective conclusion to the crisis.
- Responding to issues as they arise.
- Making decisions and giving instructions on the management of the crisis.
- Obtaining any relevant background information from internal and external sources.
- Ensuring key stakeholders are identified and kept informed of events.
- Managing internal and external communications.
- Ensuring clear differentiation between crisis management, local emergency management, and business recovery management.

6.3 Business Recovery Coordinator (Business Continuity Team)

Depending on the nature of the incident, relevant Business Recovery Coordinators will form a Business Continuity Team to coordinate activation and implementation of BCPs.

Pre-crisis:

Business Recovery Coordinators are responsible for ensuring that:

- Critical business functions and recovery timeframes are appropriate for the nature and scope of work performed by the Business Unit.
- BCPs remain current.
- Key staff within business unit have access to BCPs.
- Training is provided to staff to facilitate effective activation of BCPs.

During a Crisis:

Business Recovery Coordinators are responsible for providing leadership, guidance and support to their Business Units during a Business Continuity event. They will be responsible for activation of their Business Continuity Plans and managing, in conjunction with the CMT, local level recovery efforts. Other functions include:

- Providing initial notification of an incident to their teams and providing regular updates of the incident and recovery efforts to staff (under guidance from the CMT).
- Ensuring critical work processes continue in accordance with BCP recovery objectives.
- Managing business continuity arrangements for their business units.
- Providing regular updates to the CMT on status of recovery efforts, resource requirements and staff welfare.

Post crisis and return to normal operation:

Business Recovery Coordinators are responsible for:

- Conducting a debrief of the incident.

- Evaluating communication and information flows.
- Identifying and implementing actions to improve recovery capabilities.

7 IMPLEMENTING THE BUSINESS CONTINUITY PROGRAM

7.1 Managing the Risk

The identification and management of high impact events is of critical importance in maintaining business operations. This will be achieved by conducting a Threat Assessment within the context of 'Disruption Risk' to identify potential threats and Plausible Disruption Scenarios that may trigger activation of a Business Continuity Plan.

7.2 Threat Assessment

7.2.1 Overview

The identification and management of high impact risk events is of critical importance in maintaining operations at CSE. A Threat Assessment will be conducted to identify any threats that have the potential to significantly harm CSE and necessitate the use of a Business Continuity Plan.

Conducting a Threat Assessment as part of this Business Continuity Program involves a process of risk identification, risk analysis and risk evaluation. The objective of conducting a Threat Assessment is to identify and treat sources of risk that have greatest potential to result in activation of a Business Continuity Plan. This also involves the identification of Plausible Disruption Scenarios. These scenarios will form the basis for developing recovery strategies that feed into the Business Continuity Plans.

Threat Assessments will be conducted in accordance with principles defined by ISO 31000 and CSE's Risk Management Framework. This includes the following:

- Analysis will be conducted in the context of Disruption Risk which relates to those events that have potential to result in activation of the BCP.
- Risk ratings will be established for the quantitative assessment process in accordance with CSE's risk appetite.
- Risk ratings are established around relevant people, financial, legislative compliance, plant performance, reputational, strategic growth and other impacts.
- Threats will be assessed based on their likelihood of occurrence as well as the consequence of a threat resulting in relevant disruption scenarios.

7.2.2 Methodology

The process for conducting a Threat Assessment is detailed in the following table:

Threat Assessment		
Step	**Requirement**	**Responsibility**
Information Collection	Conduct interviews and facilitate workshops to collect information relating to: - Potential sources of risk. - Likely causes. - Existing control measures.	Governance Risk and Compliance
Risk Analysis	Establish and approve risk ratings.	Governance Risk and Compliance Group Managers / Asset Management and Technical
	Assess and categorise all identified disruption related risks.	

Threat Assessment		
Step	**Requirement**	**Responsibility**
	Group risks into key disruption scenarios.	Services
	Confirm threat assessment	
Risk Treatment	Identify gaps in control measures and document.	Governance Risk and Compliance Group Managers / Asset Management and Technical Services
	Implement treatment plans.	
	Monitor and review.	

7.3 Business Impact Analysis

7.3.1 Overview

This involves identification of recovery priorities for all business areas. It includes critical business functions, recovery timeframes and required resources. This stage also includes an objective assessment of a business continuity event in relation to the following:

- Market / Generation impacts.
- Financial impacts.
- Impacts on the CSE's business reputation and its ability to maintain the confidence of key stakeholders.
- Ability for CSE to continue to meet (or otherwise) its operational, financial, legal, regulatory and other material obligations to stakeholders.
- Estimated time CSE could reasonably continue to operate successfully and continue to meet its obligations to stakeholders while seeking to address and recover from the disruption to critical business functions, resources and infrastructure.

7.3.2 Methodology

Each business area will identify their recovery priorities by completing the following activities:

Business Impact Analysis		
Step	**Requirement**	**Responsibility**
Capture recovery information	Conduct interviews and facilitate workshops to collect the following information: - Business processes and their recovery timeframes. - Critical services, systems, applications, resource requirements and internal/external dependencies.	GM Governance Risk and Compliance
Prioritise critical functions	Complete Process Impact Analysis including: - Categorisation of business processes. - Determination and prioritisation of critical business processes. - Identification of Maximum Allowable Outage (MAO) and Recovery Time Objectives (RTO) for each business process.	GM Governance Risk and Compliance
Validation	Approve business area recovery priorities	CSE Executive Leadership Team

7.4 Recovery Strategy Identification

7.4.1 Overview

CSE will identify strategies to facilitate the recovery of Critical Business Functions within agreed timeframes. This includes strategies to reduce the impact of an event, including:

- Protecting property and infrastructure.
- Stabilising the situation.
- Continuing, resuming and recovering Critical Business Functions.

Strategies will examine:

- Recovery team structures and critical roles. This includes activation, escalation and communication procedures.
- Incident management procedures. This includes strategies relating to how an incident is detected, assessed, monitored, recorded and communicated.
- Recovery action steps. I.e. loss of IT and communications systems, temporary denial of access to site/ buildings, total loss of buildings, loss of key people, loss of material service provider.
- Redundancy options for physical sites, operational infrastructure and technology.

7.4.2 Methodology

Strategies will leverage off the recovery priorities identified in 10.2 and will consider key disruption scenarios derived from the Threat Assessment process in 10.1.

A process to manage the risk will be applied when selecting strategy options. This includes:

- Reducing the likelihood of a disruption.
- Reducing the period of disruption.
- Limiting the impact of disruption

7.5 Business Continuity Plans

7.5.1 Overview

CSE will develop, implement and maintain Business Continuity Plans that provide sufficient information to enable the organisation to respond to disruptions caused by a business continuity event, to recover critical business functions that may be impacted and to resume normal business operations.

Business Continuity Plans (BCPs) cater to the following activities in the event of an incident or major disruption:

- Pre-incident preparation.
- Responding to an incident, emergency or disaster.
- Recovering and resuming critical business functions.
- Restoring and returning all business operations

BCPs address the unique organisational structure and requirements of CSE and follow a consistent structure and layout, containing unique business area considerations based on outputs from work completed in 10.1, 10.2 and 10.3.

BCPs will contain all critical information and be structured in a logical flow that provides a standardised protocol for managing disruption events. They will be supported by quick reference tools to provide further practical guidance in the event of plan activation.

7.5.2 Methodology

The process for developing Plans is detailed in the following table.

Business Continuity Plans		
Step	**Requirement**	**Responsibility**
Plan Development	Populate BCP templates	GM Governance Risk and Compliance Group Managers
Plan Approval	Approve draft BCPs	Group Managers
	Roll out BCPs to nominated personnel	GM Governance Risk and Compliance Group Managers

7.5.3 Criterion for Activation of Business Continuity Plans

Activation of Business Continuity Plans will be in response to an actual or potential disruption to the organisation's critical business functions. Potential scenarios include:

- Temporary denial of access to site/buildings
- Total loss of building/s and/or generation assets
- Loss of key people/human loss
- Sustained loss of IT and communications systems
- Sustained loss of generation

8 TRAINING AND TESTING

8.1 Training

Training will be provided to relevant staff to build a proactive business continuity culture and to continually improve CSE's level of resilience.

Business Continuity training will be designed to provide an overall awareness and understanding of business continuity principles and preparations. Other training may also be provided including Business Continuity Leadership training and Crisis Management training.

All plan recipients will be provided with the required training in the use of their plans and tools.

8.2 Testing and Exercising

The Business Continuity Program will be tested via a combination of scenario exercises and by periodic recovery infrastructure testing to confirm resumption of critical business functions. Training and exercising would likely be conducted in conjuction with Crisis Management and Emergency Response testing and exercising.

Testing and exercising will assist to:

- Build familiarisation with staff roles, responsibilities, processes and available tools.

- Identify practical program improvements.
- Provide a high level of stakeholder assurance in CSE's recovery capability.

Types of testing and exercising that may be conducted include:

Type of Test	Description
Desk-top scenario exercise	Application of a BCP based on response to a scenario. This can be conducted at an organisation wide or at a business unit level. Does not include live recovery of people, IT and/or infrastructure.
Live scenario exercise	Application of a BCP based on response to a scenario. Includes live elements of the recovery process for people, IT and/or infrastructure.
Live tests for activation of recovery infrastructure	These end-to-end tests are designed to confirm full recovery of services and/or interconnected work processes.

Testing of BCM arrangements are to be conducted periodically or when material changes to business operations or to regulatory requirements warrant additional testing. The testing process is to include persons nominated in relevant Plans as having authority to implement the document, as well as staff who may be called upon to assist in the implementation of the BCPs.

The testing process may include the following:

- Assessment of critical business functions, resources and infrastructure, which, if adversely impacted by either internal or external events, could reasonably lead to a material business disruption.
- Assessment of the recovery strategies outlined in the BCPs as to their validity, practicality and likely effectiveness in addressing material business disruption risks and in enabling CSE to return to normal business operations.
- Assessment of the communication strategies outlined in the BCP as to their validity, practicality and likely effectiveness in addressing communication challenges, issues or requirements arising from a material business disruption.
- Validation and re-confirmation of all recovery and support arrangements with third parties that are referred to in the BCPs.

9 REVIEW AND EVALUATION

CSE will review and evaluate the performance of the Business Continuity Program on a periodic basis. The objectives of the performance monitoring process are to:

- Facilitate prompt action when adverse trends are detected or a non-conformity occurs.
- Ensure that the Business Continuity Program continues to be an effective system for managing disruption-related risk.

CSE's Business Continuity Program must continue to evolve and improve as the organisation changes over time. To achieve this, an on-going maintenance program will be established. This will involve a process of program reviews, supported by regular training and exercising of personnel.

All elements of the Business Continuity Program, including the identification of recovery priorities and the development of tools, are to be reviewed periodically or more frequently if there are material changes to business operations or to regulatory requirements, to ensure that the BCPs are fit for purpose and can meet the objectives of this Framework document.

9.1 Performance Monitoring

Performance monitoring will be conducted to evaluate:

- Achievement of objectives and targets.
- Effectiveness of processes, procedures and functions that have been established to support resumption of critical business functions.
- Compliance with best practice standards.
- Rectification of past non-conformities.

All monitoring activities will be recorded and reported to management to facilitate a process of continual improvement.

The following activities will be conducted as part of the performance monitoring process:

Performance Monitoring			
Activity	**Description**	**Responsibility**	**Frequency**
BC Program Review	Full program review	GM Governance Risk and Compliance	Periodically
Management Review	- Outstanding actions from previous review - Changes in internal/external environment affected BCM - Recent incident and exercise/testing reports - Results of BC Program audits - Other opportunities for program improvement	CSE Executive Leadership Team	Every two years
Incident Review	- Post incident review of events that resulted in activation of the BCP(s)	Crisis Management Team Business Continuity Team GM Governance Risk and Compliance	As required

10 DEFINITIONS

Term	Definition
Business Continuity Manager (BCM)	The individual responsible for coordinating continuity efforts within CS Energy.
Business Continuity Plan (BCP)	The plan of controls implemented by CS Energy and its business units to manage its business continuity risks and ensure the uninterrupted availability of its key business resources that support critical business processes.
Business Recovery Coordinator (BRC)	The individual(s) responsible for coordinating the implementation of a business unit's Business Continuity Plan.
Business Continuity Team (BCT)	The recovery and support team that includes the Business Continuity Manager, Business Recovery Coordinators and Business Unit Team Members who are responsible for coordinating continuity efforts and providing support for business critical processes.

Term	Definition
Business Unit Team Members (BUTM)	The individual(s) responsible for implementation of a Business Continuity Plan.
Crisis	A Crisis is a decisive and/or negative event, or series of events, that has the potential to significantly impact on, or destabilise CSE. The event could affect CSE's personnel, operations and commercial viability. It could also attract intense negative scrutiny from a vast array of stakeholders and jeopardise CSE's public or stakeholder image. Crisis events fall outside the normal business contingency and emergency response arrangements.
Critical functions	Critical functions are any processes or systems that control the health and safety of persons, environment, property or production on a site, or in the off-site community. Loss of critical functions means that there is an uncontrolled risk to people, environment, property or production.
Emergency	An emergency is a sudden, unexpected, abnormal or extreme event requiring precise and timely operational action to control, contain and restore to a safe condition. It may be a localised event or one that has the potential to impact on the wider community and possibly overwhelm the Company. Depending on their size and impact, emergencies can become crises, though the vast majority do not. Once the situation is controlled and rendered safe, the emergency is over.
Disaster	A condition or situation of significant destruction and/or distress to the business of CS Energy, interrupting normal business to the extent that corrective action is required (e.g. internal staff shortages, denial of access, failure in technology, loss of utility services and failure of key suppliers).
Disaster declaration	An event, announced by the Crisis Management Team (or Executive General Manager where appropriate) that requires any number of Business Continuity Plans to be invoked.
Disaster Recovery (DR) site	The site at which business operations are recovered.
Maximum Acceptable Outage (MAO)	The tolerable time available to recover disrupted critical functions and processes.
Recovery	Process to manage the re-establishment of critical functions and processes as soon as possible following a business interruption. The duration of the recovery phase will depend on the extent of disruption and actions required to return to a business-as-usual state. For an extended period of disruption, the recovery phase may become a temporary business-as-usual state for CSE.
Resumption	Process to manage the longer-term recovery issues to enable restoration of "business-as-usual" where possible.

11 REFERENCES

Reference No	Reference Title	Author
B/D/11/39708	Policy – Governance, Risk and Compliance	CS Energy
B/D/12/63934	Standard – CS-RISK-01 – Risk and Compliance Management Framework	CS Energy
B/D/11/45318	Procedure – CS-IM-01 – Incident Management Plan	CS Energy
B/D/11/43851	Procedure – CS-IM-02 – Crisis Management Plan	CS Energy
-	Business Continuity Institute 'Good Practice Guidelines 2013'	Business Continuity Institute
BS ISO 22301:2012	Societal security - Business continuity management systems - Requirements	International Standards Organisation
AS/NZS 5050:2010	Business Continuity - Managing disruption-related risk	International Standards Organisation
ISO 31000	Risk Management Standard	International Standards Organisation
-	Business Continuity Management: Building resilience in public sector entities – Better Practice Guide 2009	Australian National Audit Office

12 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.

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.