Australia Pacific LNG Project

Narrows Crossing Pipeline Environmental Management Plan

Attachment 3 Crisis and Emergency Management Directive

Directive
ORG-HSE-DVE-003

Crisis and Emergency Management

This document outlines the requirements for the plans, procedures and resources we need in order to prepare for and respond to crisis and emergency situations.

Version	1.1
Released	August 2010
Document owner	Group Manager HSE
Review date	July 2012

*Please see Document control section for more information.

Security: [Review whether the document is available for viewing by all interested Origin users, or whether restrictions should apply.]

Contents

1. Purpose and application

This Directive defines the Origin requirements to effectively respond to crisis and emergency situations in a way that minimises adverse impacts on:

- the health and safety of people;
- the environment;
- plant;
- property; and
- other harm to any aspect of our business.

This Directive applies to all operating sites and activities where we are considered the operating company having prevailing influence.

2. Responsibilities

To efficiently and effectively implement this Directive we require commitment from all our people, at every level.

Everyone must:

- meet the requirements explained in this Directive and participate in any necessary training; and
- familiarise themselves with relevant site emergency response and evacuation requirements.

Supervisors and Managers must:

- ensure that everyone they supervise is made aware of, and understands, the requirements of this Directive and that they are adequately trained and competent to carry out their assigned tasks; and
- observe the activities they control and regularly check that they conform to this Directive.

General Managers must:

- demonstrate commitment to emergency and crisis preparedness by understanding and implementing this Directive;
- establish and implement a group emergency management plan for the business unit;
- reinforce their people's expectations about being prepared for emergencies and crises to ensure they conform with this Directive; and
- communicate our expectations of business continuity and disaster recovery plan requirements, development and implementation.

The Chief Risk Officer must:

- establish and implement our emergency response framework;
- implement an audit process to review, update and test emergency response, crisis management, business continuity and disaster recovery; and
- provide training to ensure our people are able to follow the crisis and emergency management Directive.

The Emergency Team Leader must:

- follow the responsibilities as defined in the site emergency response and group emergency management plan templates

3. Requirements

3.1 General

In any crisis or emergency our priorities are to:

- ensure the safety of all our people, relevant contractors and any public associated with, or affected by our operations and our activities;
- secure the site and minimise any effect on the environment by timely and effective management;
- minimise any effect on property and assets;
- contain and manage any effect on our company's reputation and business continuity; and
- minimise any disruption to our operations and activities.

3.2 Emergency Escalation Process

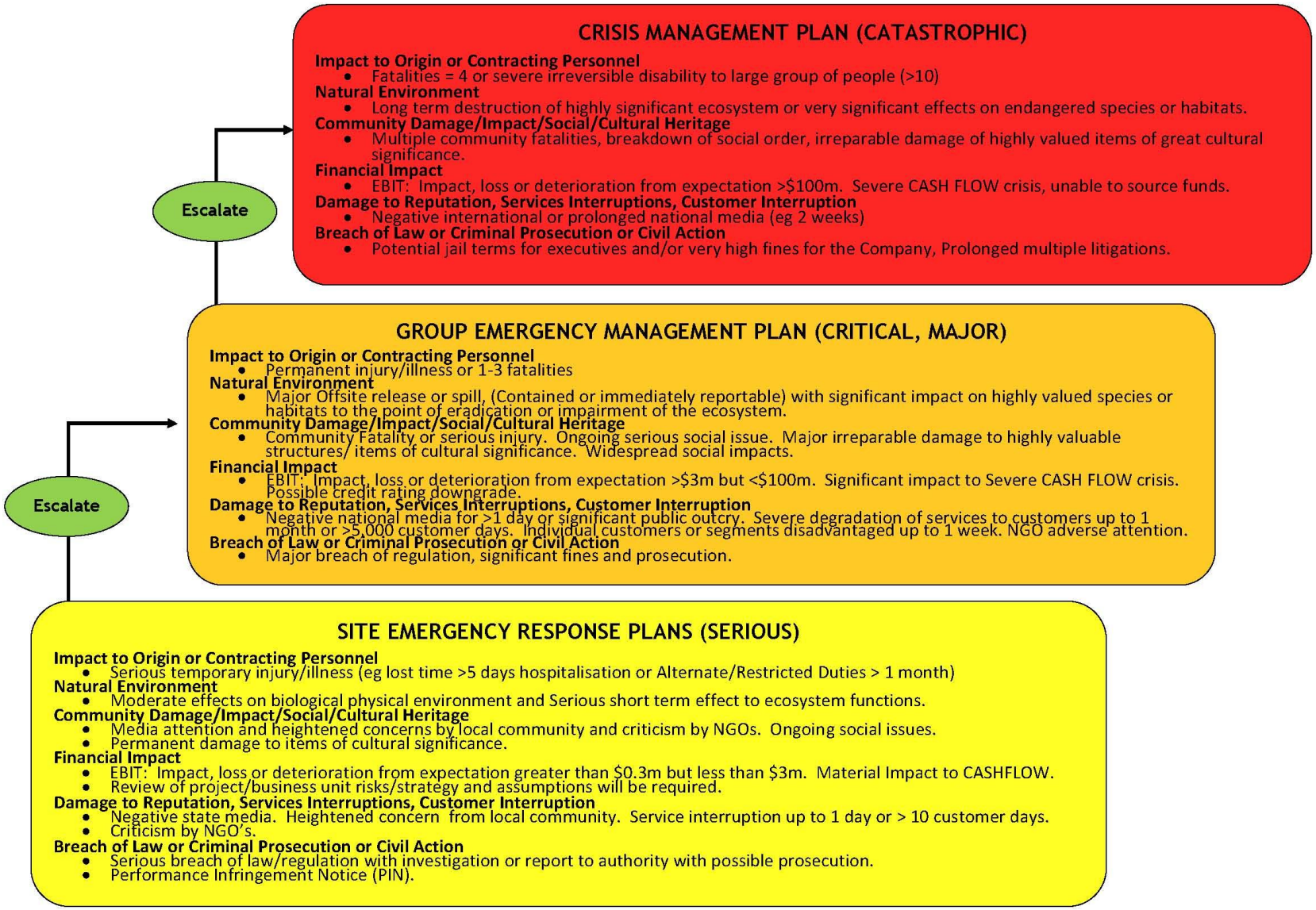
We have a three tier structure (Site Emergency, Group Emergency and Crisis) in our emergency response system, as shown in Figure 1 below.

Escalation to the next tier must occur if the emergency team leader decides it is appropriate to do so. In any case, if an adverse event invokes either the site emergency response or group emergency management plan, the next tier leader must be informed, using the requirements of the First Response Protocol.

After an event is escalated, the lower tier emergency team must continue operating, in conjunction with the upper tier.

The plans outlined above must be developed and effectively implemented for all our operating sites and premises, in accordance with this Directive.

3.2.1 Figure 1: Emergency Response Framework



3.3 Crisis and Emergency Management Plans

Plans must be maintained in electronic format and controlled hard copies of relevant plans must be readily available in the designated emergency or crisis control room.

Emergency or crisis plans must be reviewed annually to ensure they cover all possible emergency scenarios and contain all the information our people need to deal with them. In addition relevant plans must be reviewed when improvement opportunities have been identified by post emergency or crisis exercise debriefings.

3.3.1 Site Emergency Response

All operating sites/activities must have a site emergency response plan, for which the emergency team leader is responsible. The site emergency response plan provides guidelines for initiating and maintaining effective emergency responses to likely emergency scenarios.

The plan must include:

- means by which emergency responses are initiated;
- definitions of key roles and their responsibilities in an emergency response;
- descriptions of facilities and equipment required to coordinate an emergency response;
- a key contacts directory, which is reviewed and updated every quarter;
- the criteria for escalating an emergency and the means by which the group emergency management plan is initiated;
- typical emergency scenarios and guidelines for responding to them;
- communication and documentation requirements; and
- evacuation protocols and muster points.

In developing and reviewing a site emergency response plan the relevant site or activity risk register (details are in the Risk Management Directive) must be used to validate the scope (emergency scenarios covered) of the Plan. At sites where Process Hazard Analysis (PHA) (details are in the Asset Integrity Directive) has been conducted, the validation of scope must also consider the consequence analysis.

The annual review of the site emergency response plan must also consider the adequacy of the site's emergency response capability, including the availability of emergency equipment and typical emergency scenarios.

Sites classified as a Major Hazard Facility or a Dangerous Goods Location must incorporate the requirements of the National Standard for the Control of Major Hazard Facilities, or equivalent local or state legislation, into their site emergency response plan.

Additional information for developing a site emergency response plan can be found in the Site Emergency Response Plan template.

3.3.2 Group Emergency Management

Group emergency management addresses wider business unit activities that may encompass multiple sites or locations, and supports the site emergency response.

It is the responsibility of the General Manager of each business unit to have an established group emergency management plan, developed using the Group Emergency Management Plan template

The group emergency management plan template outlines the minimum mandatory requirements.

The plan must include:

- a description of how an emergency response is initiated;
- the first response protocol;
- criteria for escalating an emergency and how the crisis management plan is initiated;
- definitions of key roles and their responsibilities in an emergency response;
- communication and documentation requirements;
- a list of the facilities and equipment required to coordinate the emergency response; and
- a key contacts directory, which is reviewed and updated every quarter.

If the business unit needs additional resources to effectively respond to and manage an emergency situation, they may be added to the provided template. However, business units are not authorised to remove any information in the current template.

There is more information about developing the group emergency response plan in the Group Emergency Management Plan template.

3.3.3 Crisis Management

Crisis management is managed by the Chief Risk Officer (or delegate) and focuses on high level support, advice and coordination of additional resources. Their aim is to assist emergency response efforts and determine appropriate strategic responses to protect our reputation and viability.

The crisis management plan must contain:

- a description of an established crisis management team, consisting of key personnel, representative of the organisation as a whole;
- criteria for escalating an emergency;
- the roles and responsibilities of each crisis management team member;
- reporting processes and requirements for internal and external stakeholders;
- a key contacts directory, reviewed and updated quarterly;
- communication and documentation requirements;
- a list of facilities and equipment required to coordinate the emergency response;
- a process to regularly review and test the plan;
- training requirements; and
- details of established rooms and conference calls.

There is more information about developing the Crisis Management Plan in the Crisis Management Plan document.

3.3.4 Business Continuity

The aim of business continuity planning is to ensure the availability of the resources needed to support essential business processes.

Business continuity plans are invoked as a consequence of adverse events which affect critical activities, as a result of:

- loss of people;
- loss of workplace;

- loss of technology; or
- loss of assets.

All business units must follow the Business Continuity Development Process and complete a business impact analysis every 12 months (or when there are significant changes to the business) to identify business critical activities.

Critical activities that are identified must be included within a Business Continuity Plan and have an associated Recovery Plan developed. The Recovery Plan must identify key recovery processes, alternative resources and interdependencies.

The business continuity plan must contain:

- a critical activity list;
- key contacts;
- technology requirements; and
- recovery plans and associated business procedures.

Business units must complete annual business continuity training for all personnel holding a business continuity role, and test plans annually, at a minimum.

There is more information about developing a business continuity plan in the Business Continuity Plan – Development Guide.

3.3.5 Disaster Recovery

Disaster recovery is the ability to re-instate systems to their production state after an adverse event. Disaster recovery needs access to completely separate infrastructure, including an alternative communications network, server capacity, disk storage capacity, and tape drives, at an alternative site.

Information Technology (IT) must develop a disaster recovery plan, which includes:

- processes for the declaration of a disaster;
- plans for activating the recovery and its ongoing co-ordination;
- timeframes for recovering systems, software, data and infrastructure outlined as dependencies in business continuity plans; and
- plans for initial and ongoing communications to management and other relevant part of our business.

At a minimum, the plan must be tested annually.

3.4 Crisis/Emergency Control Rooms, Equipment Selection, Maintenance and Reporting

Each site or area and relevant business function must establish and maintain a crisis or emergency control room and an alternative location, should the primary room be affected. Where possible, control rooms should be away from areas which may be affected by an emergency situation e.g. a fire in the plant.

The emergency control room must have all the equipment and documentation needed to run an effective emergency or crisis response.

People who work in the crisis or emergency control room during an emergency or crisis must be competent in the set-up, running and roles and responsibilities of relevant specified positions of the response plan.

Risk management must be used (see the Risk Management Directive for details) to determine the type, quantity and location of emergency equipment needed for an operational site. The site or area risk register should be used to help determine and validate emergency equipment.

Emergency equipment must:

- be installed in accordance with manufacturer's instructions and/or relevant Australian Standards or equivalent;
- be readily accessible and within a reasonable distance from the source of the hazard; and
- have appropriate signage and lighting.

Each site must have emergency response equipment identified in a site asset register and have a scheduled equipment maintenance program to ensure checks are documented and recorded.

Emergency equipment must be regularly inspected and tested in accordance with the relevant legislative requirements, standards and manufacturer's instructions, including the requirements of AS1851(Maintenance of Fire Protection Systems and Equipment).

Inspections must be done by competent people, following controlled inspections check sheets.

3.5 Emergency Exercises

Emergency exercises must be conducted to:

- test the effectiveness of crisis or emergency plans;
- validate the competency of key emergency response people;
- assess our capability to respond to an emergency;
- reinforce prior training; and
- identify opportunities for improvement.

Emergency exercises must be designed to systematically include everyone likely to be involved in an incident, and may be in the form of:

- simulated emergencies;
- practical drills
- desktop exercises;
- resources and equipment checks; or
- other exercises.

An annual exercise must be conducted at sites with the potential for incidents requiring the initiation of the group emergency response plan or crisis management plan. The annual exercise should involve people from all relevant functional groups and test specific aspects of the site's emergency response plan.

Group emergency plans and crisis management plans must be tested annually. A plan will be considered to have been tested if an actual emergency occurs and components of the plan are activated.

3.6 Personnel Location

Sites must maintain a system that enables timely identification of all people who:

- are in the facility; or
- are not accounted for following an emergency evacuation of the facility.

3.7 Layout Drawings

All operational sites must maintain up to date location plans showing the positions of emergency response and fire fighting equipment. A copy of the plan must be available at all times.

3.8 Emergency Power Supply

An emergency power supply must be provided for critical equipment required in the event of an emergency (e.g. warning sirens, communications, fire pumps, extraction fans, etc) and to instruments and control systems needed to safely shut down the plant.

Inspection and testing programs for emergency power systems must be incorporated into site critical function testing programs.

4. Records

Maintaining appropriate records is an essential part of implementation. The following records must be retained for five years:

- training records;
- records of emergency exercises; and
- full records of emergency equipment inspections and testing.

5. Training and Competence

Our people must be trained and competent to fulfil their roles as defined in the relevant emergency and crisis management plans.

Training must be refreshed annually. People participating in an emergency exercise, in their defined roles, are considered to have met their refresher training requirement.

To develop and maintain our emergency process competency, minimum training requirements have been established in a Diagnostic Matrix for each tier of the emergency response framework.

Training and materials provided fall under three main categories.

Crisis Management, which includes:

- the Origin crisis management plan;
- consistent training provider; and
- one consistent training package.

Group Emergency Management, which includes:

- Group Emergency Management Plan template;
- consistent training provider; and
- one consistent training package.

Site Emergency Response, which includes:

- Site Emergency Response Plan template;
- consistent competency assessment tool; and
- training delivery coordinated and administered within the business unit.

6. Deviations

Deviations from the requirements of this directive may only be considered when:

- regulatory obligations dictate otherwise;
- implementation of the requirement is not technically feasible due to local conditions; or
- the cost of implementing the requirements substantially exceeds the benefits.

To deviate from a Directive, you must:

- Specify the implications of implementing the requirement as specified within the directive.
- Determine the risk of not implementing the requirement of the directive (in accordance with the Origin Risk Management Directive) and document the impact and duration of the deviation and identified control measures
- Have the deviation authorised by obtaining documented approval from the Origin business unit General Manager (or equivalent person with DOA of 3 or higher) and the Chief Risk Officer.

Authorisation of all deviations, whatever their duration, will be recorded on Origin's Deviation Register. The risk associated with the deviation is to be recorded on the relevant business unit or site risk register.

Refer to ORG-HSE-GDE-001 Deviation Guide and ORG-HSE-FRM-001 Deviation Request Form.

7. Compliance and Assurance

We require all of our employees to comply with this directive. Compliance with this directive will be periodically monitored by the Chief Risk Officer or delegate and will be included in the scope of relevant audits/reviews.

Compliance against the requirements established within this directive must be reviewed as part of the business unit internal audit schedule, and the HSE management system audit cycle.

Monitoring and verification of key requirements is to be included in business unit key performance indicator reporting requirements, and must include, but is not limited to:

- plan development;
- exercise schedule;
- training and testing completion;
- equipment maintenance and testing;
- critical function and control testing of emergency equipment and backup power supplies; and
- corrective action completion following exercise debriefs.

The crisis and emergency management directive audit tool has been established to assist the business in reviewing compliance to the requirements established within this directive.

Any breaches of this directive by employees will be addressed in accordance with Origin's Employee Counselling and Disciplinary Policy and its associated procedures.

8. Toolkits

The following materials support the implementation of this directive:

1. Crisis Management Plan
2. Group Emergency Management Template
3. Site Emergency Response Template
4. Business Continuity Plan – Development Guide
5. Business Continuity Plan – Development Process
6. Critical Process/Activity Recovery Plan - Template
7. Business Continuity Plan – Template
8. Audit Protocol – Crisis and Emergency Management Directive
9. Diagnostic Matrix

9. Definitions

Refer to glossary database on source

10. Document control

AUTHOR

Adrian Debrincat

STAKEHOLDERS AND OTHER CONTRIBUTORS

Position	Incumbent
Principal Process Safety and ER Advisor	Scott Cornish
Manager Systems Development – Operational Risk	Anthony Masciangioli
HSE Manager - Energy Markets	Christine Martin
Manager – Health, Safety and Environment Generation	Simon Asimus
Manager – HSE Risk and Assurance Group	Nigel Staker
Senior Risk Adviser (Contact)	Ray Willows
Manager – Electricity Ops and Projects	Allison Neesham
HSE Manager - Finance & Strategy	Adrian Debrincat
Chief Risk Officer	John Rodda

REVIEWED BY

Position	Incumbent	Review date
Principal Process Safety and ER Advisor	Scott Cornish	July 2010
Manager Systems Development – Operational Risk	Anthony Masciangioli	July 2010
HSE Manager - Energy Markets	Christine Martin	July 2010
Manager – Health, Safety and Environment Generation	Simon Asimus	July 2010
Manager – HSE Risk and Assurance Group	Nigel Staker	July 2010
Senior Risk Adviser (Contact)	Ray Willows	July 2010
Manager – Electricity Ops and Projects	Allison Neesham	July 2010
HSE Manager - Finance & Strategy	Adrian Debrincat	July 2010

APPROVED BY

Position	Incumbent	Approval date
Chief Risk Officer	John Rodda	July 2010

HISTORY

Author	Nature of change	Version	Date
Adrian Debrincat	Development	0.0	February 2010
Adrian Debrincat	Review and Update	0.1	March 2010
Adrian Debrincat	Review and Update	0.2	April 2010
Adrian Debrincat	Review and Update	0.3	May 2010
Adrian Debrincat	Review and Update	0.4	June 2010
Adrian Debrincat	Release	1.0	July 2010
Adrian Debrincat	Updated Figure 1: Emergency Response Framework	1.1	August 2010

RELATED DOCUMENTS

Title	Review date
Crisis Management Plan	12/2011
Group Emergency Management Template	01/2012
Site Emergency Response Template	04/2012
First Response Protocol	12/2011
Business Continuity Plan – Development Guide	12/2010
Business Continuity Plan – Development Process	12/2010
Business Continuity Plan – Template	12/2010
Critical Process/Activity Recovery Plan - Template	12/2010
Origin Risk Management Directive	TBA

CONTROLLED DOCUMENT LOCATION

KEY DOCUMENT

This document is an Origin Key Document