APRIL 2004

REGIONAL ASSOCIATION OF OIL AND NATURAL GAS COMPANIES IN LATIN AMERICA AND THE CARIBBEAN

Developing Emergency Response Programs: Natural, Man-made and Operational Risks

Canadian International Development Agency

Environmental Services Association of Alberta

ARPEL Guideline

Developing Emergency Response Programs: Natural, Man-made and Operational Risks

Authors:
Mr. Jim Swiss
Mr. Peter Devenis
Ms. Cari Chernichen

ARPEL, April 2004

ARPEL Guideline # 36-2004
Developing Emergency Response Programs: Natural, Man-made and Operational Risks
April 2004

Funding

This document has been exclusively prepared for the ARPEL Environmental Project Phase 3. The Project was funded by the Canadian International Development Agency (CIDA) and co-managed by the Environmental Services Association of Alberta (ESAA) and the Regional Association of Oil and Natural Gas Companies in Latin America and the Caribbean (ARPEL).

Environmental Services Association of Alberta
#1710, 10303 Jasper Avenue
Edmonton, Alberta T5J 3N6
Tel: (1-780) 429-6363
Fax: (1-780) 429-4249
E-mail: info@esaa.org
http://www.esaa.org

Regional Association of Oil & Natural Gas Companies in Latin America and the Caribbean
Javier de Viana 2345
CP 11200 Montevideo, URUGUAY
Tel.: (598-2) 410 6993
Fax: (598-2) 410 9207
E-mail: arpel@arpel.org.uy
http://www.arpel.org

Copyright

The copyright in this document or product, whether in print or electronically stored on a CD or diskette or otherwise (the "Protected Work") is held by the Environmental Services Association of Alberta (ESAA). The Regional Association of Oil and Natural Gas Companies in Latin America and the Caribbean (ARPEL) has been granted a license to copy, distribute and reproduce this "Protected Work" on a cost-recovery and non-commercial basis. This "Protected Work" shall not, in whole or in part, be copied, photocopied, reproduced, translated or reproduced to any electronic means or machine-readable form without prior consent in writing from ESAA. Any copy of this "Protected Work" made under such consent must include this copyright notice.

Authors

These Guidelines have been prepared upon request of ARPEL and its Environment, Health and Safety Committee through the collaborative efforts of the following authors:

Jim Swiss, President
Swiss Environment & Safety Inc.
145 Evergreen Way SW Calgary AB T2Y 3K8
jjswiss@aol.com

Peter Devenis, President
Envision - Planning Solutions Inc.
131 Scenic Hill Close NW Calgary AB T3L 1R1
envision@shaw.ca

Cari Chernichen, President
Oricom Original Communications Inc.
302, 603 – 11 Avenue SW Calgary AB T2R 0E1
chernichen@oricominc.com

The Consultants were assisted in detailed drafting and revision by the ARPEL Emergency Response Planning Working Group.

Reviewers

Ernesto Pesce	ANCAP	Marcius Vinicius Lisbôa Brandão	PETROBRAS
Alberto Casco	BP	Ricardo Bell Pantoja	RECOPE
David Henry	BP	José Luis Vásquez Mora	RECOPE
David Davidson	ChevronTexaco	Gustavo José Correa Bertazzuni	RepsolYPF
César Aldana	ECOPETROL	Ezequiel Arturo Sánchez	ECOPETROL
Horacio Villagra	Pan American Energy	Héctor Ochoa	PEMEX
Claudio Correles	PETROPAR	Miguel Moyano	ARPEL

Disclaimer Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither ARPEL, nor any of its member companies, nor ESAA, nor any of its member companies, nor CIDA, nor the authors, will assume liability for any use made thereof.

Table of Contents

1.0 Introduction 1

1.1 What is an Emergency? 1
1.2 Purpose of this Guideline 1
1.3 Business Sustainability 2
1.4 Format 3
1.5 Key Definitions 4

2.0 How to Use this Guideline 5

2.1 Scope of this Guideline 5
2.2 Improving Your Company's Emergency Response Capabilities 5
2.3 Develop Planning and Preparedness Components 6
2.4 Prepare Emergency Response Plans 6
2.5 Prepare Implementation and Continuous Improvement 7

3.0 Planning and Preparedness 8

3.1 Defining Commitment and Policy 8
3.2 Appointing a Planning Coordinator and Establishing a Planning Committee 11
3.3 Understanding Regulatory Requirements and Industry Codes of Practice 13
3.4 Assessing Risk 14
3.5 Establishing a Response Organization 29
3.6 Identifying Emergency Resources 38
3.7 Developing Mutual Aid Agreements 41
3.8 Establishing Emergency Communication Systems 45
3.9 Defining How to Communicate with the Public 46

4.0 Emergency Response Plans 49

4.1 Assigning Roles and Responsibilities 49
4.2 Developing an Activation Plan 50
4.3 Defining Notification and Mobilization 56
4.4 Developing Risk- and Site-Specific Response Strategies 56
4.5 Defining Reporting Processes 59
4.6 Establishing Incident Command Posts 59
4.7 Providing Security 61
4.8 Establishing a Process for Damage and Claims Assessment 61
4.9 Providing Critical Incident Stress Management 62

5.0 Implementation and Continuous Improvement 64

5.1 Obtaining Approval of the Emergency Response Program 64
5.2 Distributing Emergency Response Plans 66
5.3 Training Response Teams 66
5.4 Inspecting and Maintaining Emergency Resources 67
5.5 Conducting Emergency Exercises 68
5.6 Consulting with Stakeholders 70
5.7 Updating Program Components 71
5.8 Auditing the Emergency Response Program 71

6.0 Bibliography 74

List of Figures

Figure 1: Workflow for Developing, Maintaining and Continuously Improving Emergency Response Capabilities 5
Figure 2: Sample Policy Statement 10
Figure 3: Risk Assessment Process Flow Diagram 15
Figure 4: Sample Risk Assessment Process 17
Figure 5: Sample Frequency and Consequence Definitions 20
Figure 6: Sample Risk Ranking Matrix 21
Figure 7: Basic ICS Functional Organization 31
Figure 8: Expanded ICS Organization 32
Figure 9: Example Mutual Aid Agreement 43
Figure 10: Sample Initial Incident Report Form 52
Figure 11: Sample Risk-specific Response Strategy 58

List of Tables

Table 1: Natural Risks 23
Table 2: Man-made Risks 25
Table 3: Emergency Levels 55

1.0 Introduction

1.1 What is an Emergency?

An emergency is a situation that demands immediate attention. For the purpose of this ARPEL *Guideline for Developing Emergency Response Programs: Natural, Man-made and Operational Risks*, an emergency situation can be the result of one or more unexpected incidents that could lead to or have already caused a loss of control. The loss of control may then result in the potential for or actual damage to human life, the environment or company and third-party property.

Responding to emergencies is a process that begins long before the incidents that cause emergencies. Effective response begins with the development of emergency response programs that:

- prepare companies to respond
- provide tools with which to respond efficiently and effectively
- establish methods for ensuring emergency response programs are implemented and maintained for the long term
- streamline emergency response capabilities in the regions in which companies operate
- demonstrate leadership
- add value to the community by contributing resources and capabilities
- can result in the creation of contingency networks, the sharing of resources and mentoring of facilities that need to improve their response

In the oil and gas industry in Latin America and the Caribbean, there are both legal requirements and industry best practices that drive the development of emergency response programs for exploration, production, processing and transportation of oil and gas. However, the value of developing and implementing emergency response programs goes far beyond regulatory compliance by helping operators:

- identify and quantify the risks of their operations
- identify strategies to minimize or eliminate risks before they contribute to incidents
- manage the remaining risks so that any incidents that might occur have minimal impact
- ensure immediate and effective actions by operating personnel
- encourage cooperation between responders and government agencies
- reduce danger to workers and responders
- control the risks they introduce into the communities in which they work
- minimize damage to property and the environment
- maintain effective communication with all parties involved in or impacted by any emergency

These outcomes of effective emergency preparedness and response can strengthen company and industry infrastructures and lessen the potential for negative human, environmental and financial impacts when emergencies occur.

1.2 Purpose of this Guideline

This *Guideline for Developing Emergency Response Programs* has been created to help oil and gas companies operating in Latin America and the Caribbean improve their emergency response capabilities. Through improved response capabilities, companies can better protect employees, the public, the environment and corporate facilities and equipment from the negative impacts of emergencies.

Emergency response programs usually address four key elements including:

- preparedness and planning
- response
- business continuity

- business recovery

This Guideline, however, focuses specifically on preparedness, planning and response. The remaining topics of business continuity and business recovery may be covered as part of future ARPEL guidelines.

It is ARPEL's intention that this Guideline be used in a number of ways. At a corporate level, companies will use the Guideline to direct and support efforts focused on increasing the capability of individual facilities belonging to each company or operated by them as part of joint-venture activities. At the facility level, the Guideline will be used to improve local capabilities and will need strong support from the corporate level to be successful. Effective implementation will also depend on the priorities of the individuals who directly impact each facility's priorities (e.g., productivity vs. response).

While this Guideline was not developed to meet any specific regulatory requirements, it does provide essential advice in developing emergency response programs that, if properly implemented, will help companies in meeting their regulatory requirements. However, companies must also be aware of the regulatory requirements in the jurisdictions in which they operate.

For advice on how to get the most out of this document, see also 2.0 How to Use this Guideline on page 5.

1.3 Business Sustainability

This Guideline on "Developing Emergency Response Programs: Natural, Man-made and Operational Risks" is intended to provide practical advice for improving emergency preparedness within your company. Following the steps provided within this Guideline to identify risks and develop appropriate emergency response plans to deal with these risks will result in an improved emergency response capability throughout the organization. The plans you develop from this Guideline will help your company to better protect workers and the public. The process you use to develop emergency response plans will help reduce incident impacts as you identify risks that can be mitigated before they result in incidents.

In the end, your company's comprehensive and well-organized Emergency Response Plan will[1]:

- clearly establish roles and responsibilities of all responders
- identify response organizations and command control structures
- ensure quick access to critical information
- identify resources, required personnel, equipment and services
- coordinate response activities among industry responders, emergency services, governments and local authorities involved in emergency response
- ensure communication with all parties involved in or potentially affected by emergencies
- assist company personnel in determining and performing remedial actions
- increase public confidence in the ability of industry to handle emergencies

However, improved emergency response capability is not the only benefit of adopting this Guideline. In addition to the benefits described above, improvements in emergency preparedness and enhanced response capabilities will also result in improved business performance and sustainability of operations. Improved sustainability will position ARPEL members to ensure they meet the standards that allow them to compete as oil and gas markets open up in Latin America.

In today's business environment, being able to respond to and recover from emergency incidents while protecting human and environmental health is as important as having the best technology and dedicated effective managers.

Improving emergency response capability will result in 1) **improved worker confidence and productivity,** 2) **enhanced public confidence** and 3) **improved cost control and profitability**. These in combination will lead to business that is sustainable in the long term.

[1] Adapted from Alberta Energy and Utilities Board Guide 71: Emergency Preparedness and Response Requirements for the Upstream Petroleum Industry (June 2003)

1) Improved Worker Confidence and Productivity

Improving emergency response standards and developing a safer working environment through risk management provides employees and contractors with confidence that a company is responsible and cares about them. A safer workplace demonstrates the company's commitment to the safety of employees, contractors and the public. By involving everyone from the most senior managers to junior workers in developing and maintaining emergency response plans, employees will share the same commitment to being prepared for and responding to emergencies. This in turn creates ownership and pride among workers and improved confidence and productivity.

2) Improved Public Confidence

When your company develops comprehensive well-organized emergency response plans, and shares these plans with your stakeholders (e.g., employees, workers, communities, shareholders, regulators and customers), the level of confidence in your company's ability to respond to and manage emergency incidents effectively and reduce loss by protecting neighbors and communities will increase. This in turn translates into earning the consent of stakeholders in the community to conduct operations and grow your business[2]. In addition, shareholders and customers will have more confidence that their investments in your company will result in positive returns. Overall this enhanced confidence can lead to stronger corporate reputation, credibility, improved community relations and a better understanding of your company's response capability.

3) Improved Cost Control and Profitability

Maintaining a comprehensive emergency response capability also reduces costs associated with emergency incidents and will result in improved cost control and higher profits. These costs can result from production downtime, plant and equipment damage, injured employees, lower morale affecting productivity, and the cost of paying for damages and compensating individuals impacted by incidents (e.g., the Exxon Valdez incident cost approximately 6 billion US dollars). In addition, there can be considerable costs related to litigation and violations of regulatory requirements, increased insurance premiums, reduced quality of operations and loss of community and shareholder confidence. All of these emergency-related costs can be avoided by promoting the development of an effective, well-planned and tested emergency response capability. In the long term, demonstrating a responsible and professional approach to emergency preparedness will result in an improved business atmosphere and increased profitability.

In summary, an effective emergency response capability can produce a variety of positive effects related to business sustainability including:

- reduced incidents and liabilities
- decreased human, environmental and property costs and production losses
- improved compliance with regulatory requirements
- demonstrated due diligence to both internal and external audiences
- improved corporate image
- improved access to funding
- improved ability to obtain permits and approvals
- improved access to insurance at reasonable costs
- improved public and community relations
- improved investor and customer satisfaction
- improved government and industry relations

1.4 Format

To offer the most effective information related to developing emergency response programs, each of the elements within the three sections of this Guideline has been addressed as follows.

[2] Adapted from Suncor "What's at Stake" Document. (2003)

- **Objective and Scope** are briefly stated as the desired outcome of the element and an overview of its contents.
- **Key Components** focus on specific management activities that can lead to improved emergency response. Each key component describes **Essential Actions,** which deliver clear, concise, key steps toward achieving the stated objective. Essential actions are highlighted inside a yellow box.
- **Background** is provided to describe the purpose of the element and offer additional supporting information where appropriate.

1.5 Key Definitions

The scope and context of some important terms as they are used in this Guideline are defined below.

- **Emergency:** A present or imminent event that requires prompt coordination of actions or special regulation of persons or property to protect health, safety, or welfare of people, or to limit damage to property and the environment (CAN/CSA-Z731-03, Emergency Preparedness and Response, Canadian Standards Association.
- **Incident:** An uncontrolled or unplanned event, or sequence of events, that results in a fatality, injury, environmental impact or reduced business sustainability.
- **Accident:** Same as an incident and not used in this document.
- **Hazard:** A condition with the potential for causing an undesirable adverse effect to human health and safety, property or the environment.
- **Risk:** A measure of the probability and severity of an adverse effect to human health and safety, property or the environment.

2.0 How to Use this Guideline

2.1 Scope of this Guideline

This Guideline contains a substantial collection of information and useful tools to help oil and gas companies improve emergency response capabilities. In most cases, companies have already developed and implemented at least a few components of emergency response programs, although the components may not always be organized or managed under the banner of emergency response. In addition, the types of emergency response programs and their components developed by companies will vary depending on where and what each company operates, individual corporate needs and jurisdictional regulatory requirements.

However, at some point, every company needs to update or develop new emergency response capabilities. This Guideline provides all the basic components of an effective emergency response program and can be used by companies to determine what they need, what they already have and how to develop missing components or improve on existing components.

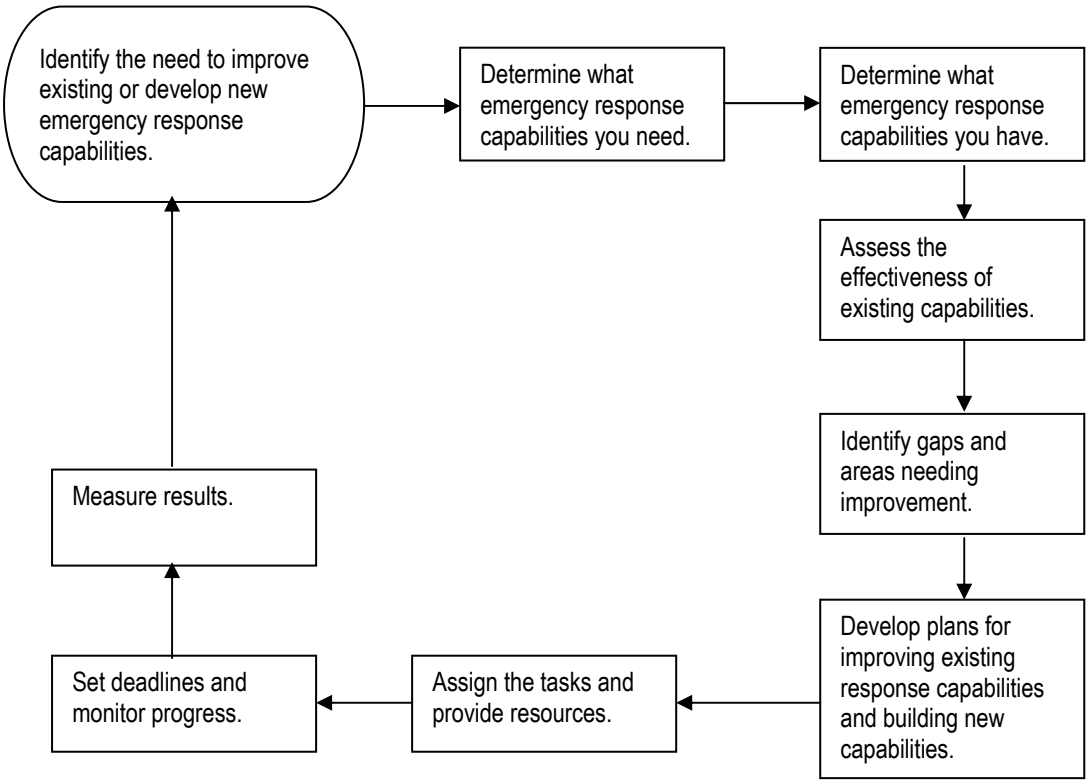
The components in this Guideline are divided among three key elements of emergency response:

- Planning and Preparedness
- Emergency Response Plans
- Implementation and Continuous Improvement

2.2 Improving Your Company's Emergency Response Capabilities

To make the best use of this Guideline, familiarize yourself with the three key elements and then choose the components your company needs to either develop or improve. The workflow demonstrated in Figure 1 below shows a simple process for developing, maintaining and continuously improving your company's emergency response capabilities.

Figure 1: Workflow for Developing, Maintaining and Continuously Improving Emergency Response Capabilities



Once you decide which emergency response components need to be developed or improved, use the checklists on the following three pages to plan your work. Checklists are provided for each of the three key elements of emergency response and provide a tool to help you:

- Identify the key components of each element.
- Locate components within this Guideline.
- Make a decision whether you want the component to be part of your response plan.
- Judge whether the component is complete or needs to be developed.
- Make the decision to develop the component.
- Assign a responsibility for developing the component.
- Establish a deadline for completing development of the component.

As you work through each component, refer to the Background sections as well as the Bibliography for additional information and resources.

2.3 Develop Planning and Preparedness Components

Planning and preparedness are essential to effective emergency response and represent the first key phase in the development of emergency response programs. Planning and preparedness lay the foundation for emergency response by defining a company's commitment to emergency management, identifying risks that might result in incidents and emergencies, and ensuring all appropriate resources and people are in place and ready to effectively respond.

The following checklist presents the essential components of planning and preparedness.

Planning and Preparedness Components	**Page**	**Is the component required?**	**Is the component already in place?**	**Should the component be developed or improved?**	**Who is responsible?**	**Deadline**
Define Commitment and Policy	8					
Appoint Coordinator and Committee	11					
Understand Regulatory Requirements and Industry Codes of Practice	13					
Assess Risks	14					
Establish Response Organization	29					
Identify Resources	38					
Develop Mutual Aid Agreements	41					
Establish Communications Systems	45					
Define Communication with Public	46					

2.4 Prepare Emergency Response Plans

An effective emergency response plan is concise and well organized with sufficient detail to ensure quick access to critical information collected through the Planning and Preparedness phase. It also provides specific information to assist responders in focusing their efforts on various aspects of response (e.g., notification versus establishing Incident Command Posts).

The following checklist describes the key sections required to develop an emergency response plan that can be effectively used to initiate a response to any incident.

Emergency Response Plan Components	**Page**	**Is the component required?**	**Is the component already in place?**	**Should the component be developed or improved?**	**Who is responsible?**	**Deadline**
Assign Roles and Responsibilities	49					
Develop an Activation Plan	49					
Define Notification and Mobilization	56					
Develop Risk and Site-specific Response Strategies	56					
Define Reporting Processes	59					
Establish Incident Command Posts	59					
Provide Security	61					
Establish a Process for Damage and Claims Assessment	61					
Provide Critical Incident Stress Management	62					

2.5 Prepare Implementation and Continuous Improvement

The success of emergency management programs depends heavily on how well the programs are implemented and maintained. As new programs and components are developed, it is essential to ensure they are integrated into the overall management of company operations. It is also important to constantly re-evaluate response programs to ensure they are current, relevant and effective.

The following checklist describes the key actions necessary to implement and properly maintain an emergency response plan.

Implementation and Continuous Improvement Components	**Page**	**Is the component required?**	**Is the component already in place?**	**Should the component be developed or improved?**	**Who is responsible?**	**Deadline**
Obtain Management Approval	64					
Distribute Emergency Response Plans	66					
Train Response Teams	66					
Inspect and Maintain Resources	67					
Conduct Emergency Exercises	68					
Consult with Stakeholders	70					
Update Program Components	70					
Audit the Emergency Response Program	71					

3.0 Planning and Preparedness

Overview

Planning and preparedness are essential to effective emergency response and represent the first key phase in the development of emergency response programs. Planning and preparedness lay the foundation for emergency response by defining a company's commitment to emergency management, identifying risks that might result in incidents and emergencies, and ensuring all appropriate resources and people are in place and ready to effectively respond.

Scope

This ARPEL *Guideline for Developing Emergency Response Programs: Natural, Man-made and Operational Risks* provides guidance and resources for the following elements of emergency planning and preparedness:

- Defining Commitment and Policy
- Appointing a Planning Coordinator and Establishing a Planning Committee
- Understanding Regulatory Requirements and Industry Codes of Practice
- Assessing Risk
- Establish Response Organization
- Identifying Emergency Resources
- Developing Mutual Aid Agreements
- Establishing Emergency Communication Systems
- Defining How to Communicate with the Public

3.1 Defining Commitment and Policy

3.1.1 Objective and Scope

The primary objective of defining and documenting a policy on emergency response is to verify and demonstrate your company's level of commitment and acceptance of accountability and liability for the impact of its operations.

Your emergency response plan should contain a policy statement that describes the intent and scope of your company's commitment to emergency preparedness and response and provides information on the responsibilities of those who are involved in the emergency response plan.

Key components of defining commitment and policy include:

- Creating and Maintaining a Policy
- Communicating the Policy to Stakeholders

3.1.2 Creating and Maintaining a Policy

Essential Actions

- Establish clear and concise statements for your company's emergency response policy that describe:
  - company commitment to effective emergency response
  - key company objectives and goals
  - company commitment to compliance with regulated requirements
  - methods to measure compliance
  - general responsibilities of management, employees and contractors to prevent incidents
- Compare company objectives to emergency response planning activities and expenditures to ensure they are compatible.
- Consult legal counsel to ensure goals and objectives are in accordance laws and regulations in the jurisdictions in which you operate.
- Determine if any existing safety or environment policies adequately cover emergency response commitments or can be modified to include emergency response.
- Review examples of emergency response policy statements from peer companies.

  Tip: *If you find one that meets your needs, use it as a model to create your own policy.*

  See also: *Figure 2: Sample Policy Statement on page 10.*
- Prepare a draft policy that includes several approaches for company directors to consider.
- Ask directors and other personnel to review the draft policy and provide feedback.
- Prepare a final statement incorporating reviewer comments.
- Have the company's most senior officer sign and date the policy.
- Review and update the policy on a regular basis.
  - Check the policy against measured goals and objectives.
  - Assess employee and contractor knowledge of the policy.
  - Update as necessary to reflect new goals and company activities.
  - Distribute updated policies and ensure outdated policies are discarded.

  Tip: *Annual reviews can be incorporated into overall company and individual performance reviews as well as in annual goal setting.*

Figure 2: Sample Policy Statement

Our company strives to provide and maintain a workplace free of incidents. Despite our best efforts to prevent incidents, there may be occasions where our actions, the actions of others or natural occurrences result in the need for emergency response actions.

To ensure our company is prepared to respond effectively, we commit to:

- Providing the resources necessary to prepare for, respond to and recover from incidents in a timely manner.
- Developing an appropriate emergency response process for the control of emergencies within company sites.
- Responding as quickly as possible to protect the health and safety of our employees, contractors, stakeholders and the communities near our operations.
- Ensuring we have an adequate pool of trained response personnel available to us at all times.
- Providing appropriate training for all members of the company Emergency Response Organization and the provision of appropriate information for employees, with emphasis on induction of new employees and persons with disabilities.
- Being responsive, understanding and compassionate to the needs of stakeholders impacted by any incident related to our operations.
- Respecting the rights of our employees and other stakeholders to be kept informed about the risks and outcomes of incidents that do occur.
- Complying with regulatory requirements and industry best practices for all aspects of emergency response.
- Adopting a positive and pro-active approach to emergency response with the aim of minimizing the adverse affects relating to the potential results of an emergency
- Encouraging participation in, and ownership of emergency response procedures to ensure individuals can take part in their own safety management.
- Establishing meaningful methods for tracking and measuring our response capabilities, particularly during incidents.
- Using the lessons we learn through training exercises, audits, inspections and actual incidents to continuously improve our emergency response capabilities.
- Listening to our employees and other stakeholders who offer comments on our response capabilities.

All employees across our organization share responsibility for ensuring our company is capable of effective emergency response. By accepting this responsibility we take control of our own health and safety and contribute to the health and integrity of the company and the communities in which we work.

3.1.3 Communicating the Policy to Employees and Stakeholders

Essential Actions

- Publish the policy as one of the lead items in corporate and field emergency response plans and other significant documents from your emergency response program.
- Post the policy on the company website and in other areas where employees, contractors and visitors can easily see and read it.
- Include the policy in new employee and contractor orientations.
- Review the policy periodically with staff and contractors at safety meetings and during emergency training and exercises.
- Provide the policy as part of community information packages at open houses and other events that showcase company operations and activities related to emergency response or environment, health and safety management.

3.2 Appointing a Planning Coordinator and Establishing a Planning Committee

3.2.1 Objective and Scope

The primary objective in appointing a Planning Coordinator to your emergency response programs is to ensure centralized coordination and consistency in development, implementation and continuous improvement of your emergency response programs. The Planning Coordinator also gives the program an identity and provides a vehicle of communication between those developing the program and those using it.

The primary objective of establishing a Planning Committee is to provide support and direction to the Planning Coordinator from a group that represents a variety of concerns from across the company. The Planning Committee is responsible for ensuring emergency response programming activities are consistent with company standards and implemented across the organization.

Key components of this element are:

- Appointing a Planning Coordinator
- Establishing a Planning Committee

3.2.2 Appointing a Planning Coordinator

Essential Actions

- Define the Planning Coordinator's role to include:
  - coordination of development, implementation and continuous improvement of emergency response programs across your organization.
  - corporate-level guidance to individuals and groups tasked with development, implementation and continuous improvement activities
  - development of formats, templates and requirements that allow field or operational personnel to build their risk-specific and site-specific emergency response program components (e.g., response plans)
  - auditing the program and mentoring program participants

  Tip: *The Planning Coordinator does not typically hold responsibility for actual creation and updating of program components, unless it is a small company. The coordinator usually acts as an auditor and mentor rather than the person tasked with building components of the emergency response program.*
- Identify individuals within the company who have adequate experience and skills to coordinate the development, implementation and continuous improvement of the emergency response program.

  Tip: *Adequate experience will be defined by the extent of program development, implementation and continuous improvement necessary in your company. Individuals with direct experience in emergency response as well as in health, safety an environmental management at a corporate or field level may offer the best combination of experience and skills.*
- Ensure the coordinator has the authority and resources to:
  - delegate development of program components
  - provide the format and framework to allow components to be developed
  - ensure components are developed and implemented
  - ensure program components are kept up to date (e.g., regular maintenance of contact lists and operational information in response plans)
  - provide guidance on training requirements for response personnel
  - monitor training results
  - provide guidance on emergency drills and exercises and ensure results are documented and implemented within the plans
  - periodically audit the emergency response program and its components to ensure commitments are being met

3.2.3 Establishing a Planning Committee

Essential Actions

- Select members for the Planning Committee to represent geographic areas of your operations or individual business units such as:
  - community affairs
  - engineering
  - land
  - legal
  - security
  - seismic
  - health, safety and environment
  - human resources
  - operations
  - community affairs / communications
  - purchasing
  - risk management
  - transportation

  Tip: *The size of the planning committee should reflect the size of your organization, the extent of your operations and the risks they present.*
- Establish roles for the Planning Committee to include:
  - understanding the risks that need to be managed across the organization to prevent emergencies
  - development and verification of company standards for emergency response programs and their components
  - guidance, direction and support for the Planning Coordinator
  - assignment of resources to the development, implementation and continuous improvement of the emergency response program
  - periodic review of the Planning Coordinator's activities and the results of emergency response program audits
- Establish a collaborative approach between the Planning Committee and representatives from outside your organization who can add external expertise or resources, such as:
  - government and regulators
  - police
  - fire
  - utilities
  - consultants
  - municipal emergency planners
  - members of the community
  - media relations experts
  - emergency medical services
  - industrial hygiene

3.2.4 Background

Senior management usually holds responsibility for appointing the Planning Coordinator and assigning the necessary authority and resources to fulfill the company's emergency response planning objectives. The Planning Coordinator's job may be full time or an addition to other related responsibilities such as environment, health and safety management. The Planning Coordinator reports to or works with the Planning Committee to ensure overall emergency response programming initiatives, standards, guidelines and audits are implemented and understood across the company. The Planning Coordinator usually establishes the Planning Committee.

Typically the Planning Committee is made up of business unit managers from across the company with responsibility for emergency preparedness. The primary responsibility of the Planning Committee is to provide overall corporate governance, verify and ensure consistency with company standards, and provide sufficient resources to ensure programs are developed and implemented across the organization.

3.3 Understanding Regulatory Requirements and Industry Codes of Practice

3.3.1 Objective and Scope

The primary objective of understanding regulatory requirements is to ensure compliance. The primary objective of understanding industry codes of practice is to ensure due diligence by providing your company the benefits of existing guidance commonly available to it through industry associations and standard setting bodies (e.g., International Standards Organization, International Labour Organization).

Key components of this element are:

- Identification and Interpretation of Regulatory Requirements
- Identification and Integration of Industry Codes of Practice

3.3.2 Identification and Interpretation of Regulatory Requirements

Essential Actions

- Assign competent personnel to address all matters related to legislated requirements.

  Tip: *Personnel responsible for identifying and interpreting regulatory requirements need a clear understanding of the company's operations as well as the risks those operations present. They should also be skilled in reading legislation, determining how it might impact operations, and developing processes and procedures for ensuring compliance.*
- Develop resources and processes for identifying, maintaining and communicating current information on legislated requirements.

  Tip: *Resources for identifying legislative information include government websites, printed legislation and bulletins produced by government departments, third-party legal databases accessible by subscription, individual contacts within relevant government departments, and individuals within your organization that have knowledge of the regulatory environment.*
- Assess operations to determine which pieces of emergency management legislation govern your operations and how that legislation affects emergency response programming.
- Identify and develop contacts within government departments or agencies that are responsible for administering legislation that addresses emergency response programs.

  Tip: *If properly maintained, these contacts can be very helpful in alerting your company to pending and actual changes to requirements.*
- Document all regulatory requirements applicable to your emergency response programming activities.
- Assess your emergency response program and its components against the requirements to ensure compliance.
- Monitor for regulatory changes and determine how they impact your emergency response programs.
- Update processes and documentation to reflect changes.
- Make documentation readily available to all employees.
- Discuss regulatory requirements as part of training, orientations, work permits, safety meetings and pre-job meetings.
- Incorporate regulatory requirements into new project planning and design (e.g., facilities design) to eliminate risks that otherwise have to be managed as part of emergency response programs.

3.3.3 Identification and Integration of Industry Codes of Practice

Essential Actions

- Assign competent personnel to identify and integrate industry codes of practice into company processes and procedures.

  Tip: *Personnel responsible for identifying relevant industry codes of practice need a clear understanding of the company's operations as well as the risks those operations present.*
- Develop resources and processes for identifying, maintaining and communicating current information on industry codes of practice.

  Tip: *Resources for industry codes of practice include industry association websites, association newsletters, individual contacts within relevant associations, and individuals within your organization that have knowledge of the industry codes of practice, perhaps as members of industry committees.*

  See also: *6.0 Bibliography on page 74 for references to a variety of codes of practice and the organizations that develop them.*
- Develop a process for assessing codes of practice to determine their relevance and value to your operations.
- Identify and develop contacts within associations that develop codes of practice for emergency response programs.

  Tip: *If properly maintained, these contacts can be very helpful in alerting your company to pending and actual changes to practices. It will also provide you opportunity to have input into proposed changes.*
- Identify and integrate applicable codes of practice into your emergency response programs.
- Ensure emergency response processes and procedures that integrate codes of practice are well documented.
- Monitor for association activities for changes to codes of practice and to determine how they impact your emergency response programs.
- Update processes and documentation to reflect changes.
- Make documentation readily available to all employees.
- Discuss codes of practice as part of training, orientations, work permits, safety meetings and pre-job meetings.
- Incorporate codes of practice into new project planning and design (e.g., facilities design) to eliminate risks that otherwise have to be managed as part of emergency response programs.

3.4 Assessing Risk

3.4.1 Objective and Scope

The primary objective of risk assessment is to identify potential risks, evaluate their significance and prioritize risks that require response organizations and strategies to be developed. Risk assessment should be conducted at a variety of levels including site, region and corporate to ensure your company fully understands its vulnerabilities and develops a response organization, plans and strategies that effectively minimizes those vulnerabilities.

Risk assessment contributes directly to the development of emergency response plans, particularly activation plans which are described on page 49, and response strategies which are described on page 56.

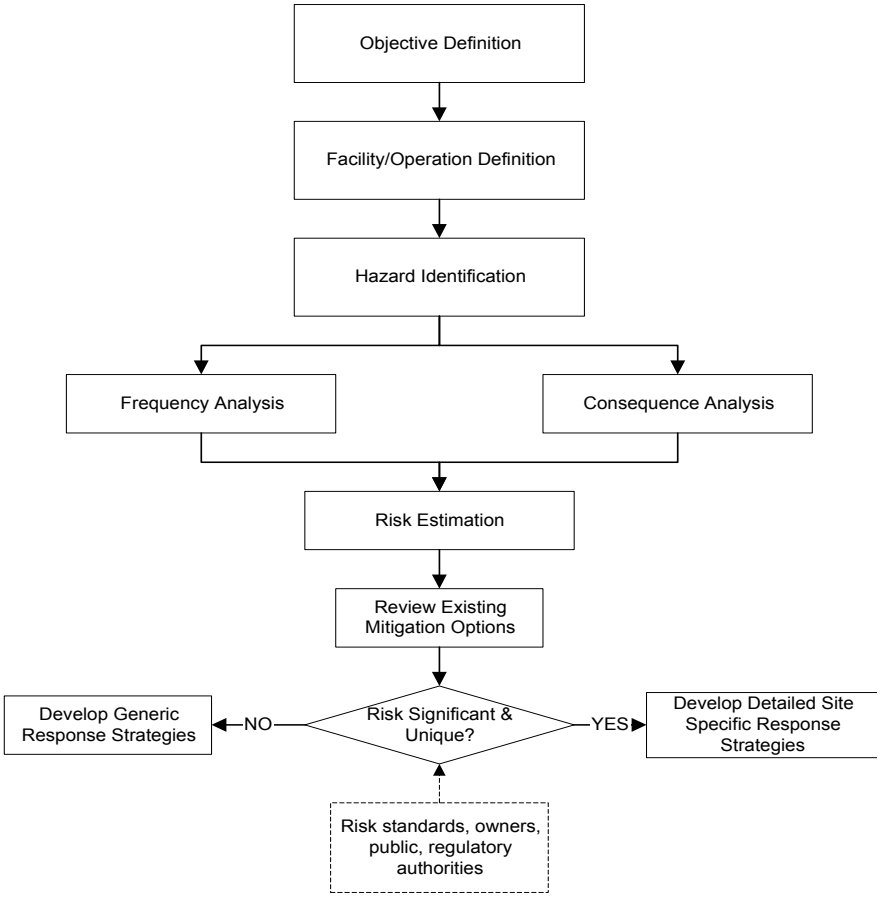
Key components of assessing risk include:

- Using a Risk Assessment Process
- Estimating Potential Frequency and Consequence

- Using a Risk Ranking Matrix

The overall risk assessment process is illustrated in Figure 3: Risk Assessment Process Flow Diagram below. Risk assessment and ranking are also supported by summaries of natural and man-made risks beginning on page 21 in Background.

Figure 3: Risk Assessment Process Flow Diagram



3.4.2 Using a Risk Assessment Process

Essential Actions

- Establish a step-wise process that enables your company to assess any type of risk at any location by:
  - defining the objectives of the risk assessment
  - describing the facility or operation being evaluated

  Tip: *Facilities and operations may not be stationery or confined to a discrete area (e.g., tank trucks, pipelines, rail cars).*

  - identifying risks that exist at the facility or operation
  - identifying risks outside the facility that could threaten the facility
  - determining the potential frequency of the identified risks
  - analyzing consequences of risks
  - estimating the significance of risks
  - mitigating risks
  - identifying those risks that require response organization and strategies

  See also: *Figure 4: Sample Risk Assessment Process on page 17.*
- Determine what activities, facilities and areas will be assessed and set priorities.
- Assign risk assessment activities to individuals who are competent in risk assessment and understand the areas they will be assessing.
- Establish procedures and methods for documenting and following up the results of risk assessments.

Figure 4: Sample Risk Assessment Process

Step 1: Define the Objective of the Risk Assessment	
Define risk assessment objectives including any adverse effects or concerns that may arise. Also specify the measures of risk that should be selected.	
Step 2: Describe Facility or Operation Being Evaluated	
Describe the facility using the following categories:	
• general description including purpose, capacity, location	
• physical layout, key processes, products, hazardous materials, ancillary equipment	
• estimate of condition	
• physical environment around facility	
• neighbors and others close by who may be affected by the facility or operation or who may create risks to your operation (e.g., industrial facilities, potential for civil disturbance or terrorism)	
• historical incidents at the facility or within the operation	
Step 3: Identify Risks that Exist at the Facility or Operation	
Identify potential risks that may exist at the facility or operation or could threaten the facility externally. Review applicable internal and external historical databases to assist in identifying potential risks from previous incidents at your facilities and elsewhere. Consider smaller incidents and near misses that could have created a significant impact if conditions had been different. *See also: Columns 1 and 2 in Table 1: Natural Risks on page 23, and Columns 1 and 2 in Table 2: Man-made Risks on page 25. Add other risks that may not be in these tables.* *See also: Example databases listed on page 21.*	**Identified Risks** 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. Etc.

Step 4: Determine the Potential Frequency of the Identified Risks

Determine the likelihood of the occurrence (frequency) of the identified risks. Use historical records plus expertise and experience of on-site personnel to estimate these frequencies. Review applicable internal and external historical incident databases to assist in determining potential frequency and severity of identified risks.

See also: Column 3 in Table 1: Natural Risks on page 23, and Column 3 in Table 2: Man-made Risks on page 25.

See also: Example databases listed on page 21.

Rank potential frequency as:

- 1 – Unlikely
- 2 - Seldom
- 3 - Occasional
- 4 - Frequent

See also: *3.4.3 Estimating Potential Frequency and Consequence on page 20.*

Risks	Frequencies (4,3,2,1))
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Etc.	

Step 5: Analyze Consequences of Risks

Estimate the severity of adverse effects these risks may have to people, environment, assets and reputation. Use historical records plus expertise and experience of on-site personnel to estimate these frequencies.

See also: Column 4 in Table 1: Natural Risks on page 23, and Column 4 in Table 2: Man-made Risks on page 25.

Rank potential consequences as:

- 1 – Incidental
- 2 – Minor
- 3 – Serious
- 4 - Major

See also: 3.4.3 Estimating Potential Frequency and Consequence on page 20.

Risks	Consequence (1,2,3,4)
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Etc.	

Step 6: Estimate Significance of Risk

Combine frequency and severity to determine the overall ranking of the risk. Rankings are based on the product of:

Frequency ***x*** Consequence

Risk	Score (FxC)
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
10.	
8.	
10.	
Etc.	

Step 7: Chart and prioritize risks.		
Use a matrix to chart and prioritize risks according to their ranking. ***See also:*** *Figure 6: Sample Risk Ranking Matrix on page 21.*		
Step 8: Identify risks that require response strategies.		
Select the highest priority risks identified in step 6 above that cannot be mitigated and develop risk-specific response strategies for incidents that might be caused by these risks. *See also:* *Figure 11: Sample Risk-specific Response Strategy on page 58.*	**Risk**	**Requires Risk-Specific Strategy**
	1.	
	2.	
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	10.	
	Etc.	

* The risk assessment in Figure 4 is a qualitative process. You may also want to consider using quantitative risk estimate tools (such as those described in *ARPEL Guideline on Oil Spills Risk Assessment and Management*).

3.4.3 Estimating Potential Frequency and Consequence

Essential Actions

- Develop definitions for frequency and consequence levels for different categories of risk (e.g., safety, loss and environmental risks).

  See also: *Figure 5: Sample Frequency and Consequence Definitions below.*

- Ensure consistency and comparability by using the same titles for different levels of frequency and consequence, regardless of the category of risk, such as:
  - Frequency:
    - Unlikely
    - Remote
    - Occasional
    - Frequent
  - Consequence
    - Incidental
    - Minor
    - Serious
    - Major

Figure 5: Sample Frequency and Consequence Definitions

SAFETY/LOSS			
Potential Frequency		**Potential Consequence**	
Unlikely 1	Possible but very rare (e.g., once in the life of the facility). Not likely to occur.	Incidental 1	• Minor injury, no threat to public. • Minor damage (<$10K). • Downtime <1 day.
Remote 2	Has happened within industry but not often (e.g., once every 20 years). Possibility of occurring sometime.	Minor 2	• Medical treatment or restricted duty. • Minor damage (<$50K). • Downtime <10 days.
Occasional 3	One occurrence every three years. Possibility of isolated incidents.	Serious 3	• Lost time, threat to public sector. • Extensive damage (<$500K). • Downtime >10 days.
Frequent 4	One or more occurrences every year. Possibility of repeated incidents.	Major 4	• Fatality, or harm to public sector. • Extensive damage (>$500K). • Extended downtime >90 days.
ENVIRONMENTAL			
Potential Frequency		**Potential Consequence**	
Unlikely 1	Possible but very rare (e.g., once in life of facility).	Incidental 1	Contained within facility or location, no adverse environmental impact. Release volume is below reportable levels or volumes.
Remote 2	Has happened within industry but not often (e.g., once every 20 years).	Minor 2	Contained within facility or location, minimal impact that poses no long-term threat to the environment. Regulatory reporting is required.
Occasional 3	One occurrence every three years.	Serious 3	Off-site releases, repeated non-compliance issues or one-time incidents with potential for significant adverse impact. Regulatory reporting is required.
Frequent 4	One or more occurrences every year.	Major 4	Major environmental impact to neighbouring receptors (e.g., community, streams, vegetation, air, groundwater). Regulatory reporting is required.

* Note: Potential Frequency and Consequence categories need to be assessed for different site and business situations.

3.4.4 Using a Risk Ranking Matrix

Essential Actions

- Develop a risk-ranking matrix that allows you to chart potential frequency and consequence along different axes.

  See also: *Figure 6: Sample Risk Ranking Matrix below.*
- Use numeric rankings (priorities) to each position in the matrix (e.g., from 1 for the lowest priority to 9 for the highest priority).
- Define response priorities for each ranking (e.g., a ranking of 9 requires an immediate response).
- Calculate rankings (i.e., frequency *x* consequence) and chart risks in the matrix.
- Determine response priorities for each risk according to its placement within the matrix.
- Incorporate response priorities into your response program development plans.

Figure 6: Sample Risk Ranking Matrix

POTENTIAL CONSEQUENCE				
POTENTIAL FREQUENCY	Incidental **(I)**	Minor **(M)**	Serious **(S)**	Major **(Ma)**
Unlikely **(U)**	**1**	**2**	**3**	**4**
Remote **(R)**	**2**	**4**	**6**	**7**
Occasional **(O)**	**2**	**6**	**7**	**8**
Frequent **(F)**	**3**	**7**	**8**	**9**
RESPONSE PRIORITY				
Rank 1 and 2:	Lower priority. May require further study and/or action, as resources are available.			
Rank 3 to 6:	Medium priority. Should be considered serious and appropriate response strategies should be developed.			
Rank 7 to 9:	Very high priority. Immediate action to develop response strategies should be taken to ensure the organization is prepared to respond.			

3.4.5 Background

Description of Risks

Risks that may apply to typical oil and gas operations and facilities in Latin America and the Caribbean are described in Tables 1 and 2 below as:

- Natural Risks (Table 1)
- Man-made Risks (Table 2)

For each Natural Risk in Table 1, the geographic area where these risks are most prevalent is described for Latin America and the Caribbean. The qualitative probability of the risk occurring is also stated along with the potential consequences of the risk. For each Man-made Risk in Table 2, contributing factors as well as potential consequences are described.

Example Resources and Databases

Databases that can help you in determining frequency and severity of risks as part of your risk assessment process include:

- Rand-MIPT Terrorism Incident Database
- CSB Chemical Incident Report Center
- EPA Accidental Release Information Program (ARIP)

- UK Health and Safety Executive Major Hazard Incident Data Base
- OECD Chemical Accident Risk Assessment Thesaurus
- Ility International Incident Database
- NOAA Oil Spill Case Histories
- Risk and Reliability
- Offshore Reliability Data (OREDA) Project
- Risk World – Risk Databases
- DNV Worldwide Offshore Accident Databank (WOAD)

The ARPEL *Health and Safety Guideline – Incident Classification*, describes a broad variety of incidents that companies should be documenting. This presents an opportunity to fully assess risk against an expansive database of incidents from individual organizations. This information will also be useful in continuous improvement and demonstrate the closure of the cycle.

As well the ARPEL *Guideline on Oil Spills Risk Assessment and Management* describes a variety of qualitative and quantitative methods that could be adapted as companies review methods to determine risk frequency and severity.

The full references and links are provided in the Bibliography beginning on page 74.

Table 1: Natural Risks

Type of Risk	Affected Geographic Area	Probability	Potential Consequences
Severe Weather			
Snow, ice, hail, storm, frost	Argentina Chile Nicaragua Southern Brazil Many countries at high altitudes	Occasionally during the presence of low-pressure systems	• Slick metal surfaces • Loss of vehicular traction • Damage to thermal-sensitive equipment and chemicals
Floods, tropical rains (heavy rains for long periods)	Argentina Brazil Colombia Costa Rica French Guyana Nicaragua North-eastern Bolivia Paraguay Peru Uruguay Venezuela	Seasonal, usually from January – February October - November	• Water damage to equipment • Unstable terrain, flooding may contribute to land and mudslides • Washed out roads • Injury or damage caused by debris being swept across the water • River levels can grow and jeopardize dock operations • Tank spill containment dikes may collapse or not work properly • Drains can become plugged and industrial effluents could reach springs, inner rivers, and other waterways.
Lightning	See also: Floods Note: Offshore facilities are especially vulnerable	Seasonal, lighting usually accompanies the storms of a rainy season or a hurricane	• Injury or loss of life to personnel struck by lightning, or within the vicinity of an object struck by lightning • Damage to electrical and electronic equipment (e.g., data handling devices, pulse transmitters, level gauges, etc.) due to voltage transients when struck by lightning • Damage to structures from being struck by lightning • Lightning could ignite vapors around atmospheric tanks without internal roofs holding volatile fuels, resulting in major fires
Drought	Brazil Colombia Ecuador Nicaragua Uruguay Venezuela	Periodic droughts may span several decades	• Short supply of fresh water • Unstable terrain
Wind-driven water, High Waves	See also: Hurricane	See also: Hurricane	• Injury or loss of life from being struck by waves or swept out to sea • Damage or loss of equipment from being struck by waves or swept out to sea • Unstable terrain due to water saturation
Hurricane	All countries that border the Caribbean Sea and the Pacific and Atlantic Coasts	Seasonal, mostly between June and November	• Depending upon the strength of the hurricane, equipment and facility damage can range from minor to extensive. • Injury or fatality • Flooding • Heavy or high waves

Type of Risk	Affected Geographic Area	Probability	Potential Consequences
Seismic Events			
Earthquake	Argentina Chile Colombia Costa Rica Ecuador El Salvador Guatemala (on the Caribbean Sea side) Honduras Mexico Nicaragua Peru	Frequent, especially within countries bordering the Pacific Ocean	• Damage to structures may range from minor to complete destruction • Loss of transport routes • Injury or loss of life due to collapsing structures and falling debris • Drilling equipment, storage tanks and pipelines are especially vulnerable
Tsunami	Chile Colombia Nicaragua Peru	Periodic	• Loss of life or injury from being struck by waves or swept out to sea • Damage or loss of equipment from being struck by waves or swept out to sea • Damage or loss of boats and ships that are docked
Other			
Landslide or mudslide	Brazil Colombia Costa Rica Ecuador El Salvador Guatemala Honduras Mexico Nicaragua Peru Venezuela	Frequent; land and mudslides usually accompany a heavy rain, flood, or seismic event	• Injury or loss of life due to being struck by mud or rock • Damage or destruction of equipment • Loss of land transport routes • Unstable terrain
Volcano	Chile Colombia Costa Rica Ecuador El Salvador Guatemala Martinique Mexico Montserrat Nicaragua Peru	Frequent, especially within El Salvador, Guatemala and Costa Rica	• Major explosions • Ash clouds • Altered terrain • Loss of transport routes • Acid rain • Unstable seismic activity • Presence of poisonous gasses • May cause land and rock slides

Table 2: Man-made Risks

Type of Risk	Contributing Factors	Potential Consequences
	Human Actions	
Bomb threat	• Disgruntled employees • A large media presence (e.g., official opening of a new facility, a change in corporate position such as a merger or sale) • Recent media releases that indicate significant corporate growth • The presence of high-ranking company officials	Although the majority of bomb threats turn out to be hoaxes, they must still be taken seriously and procedures must be in place to deal with them. Most bomb threats are made only to disrupt production; however, in the unlikely event that the bomb is real, the damage to equipment and loss of life could be extensive.
Civil protest, riots	• New exploration or operations (especially if done within sensitive environments) • Unrest within local governments • Perceptions of fraudulent corporate behavior acted upon personnel • Economic strife within the local population • Perceptions of corporate oppression of personnel	Most civil protest occurs as peaceful demonstrations with minimal injuries and property damage. Violence can be avoided by putting in place procedures and personnel to deal with protesters. Riots may cause extensive property damage and severe injuries and loss of life if not prevented or suppressed effectively. Management techniques during these instances will reflect positively or negatively under media scrutiny during the coverage of these events. See also: Media Scrutiny
Criminal Activity (e.g., theft, vandalism, arson)	• Lapse in inventory tracking • Long periods of inactivity for personnel (boredom) • Disgruntled employees • Insufficient personnel screening during hiring • Inadequate or unsafe work environments • Deficient training procedures	Criminal activity is a large contributor to losses of company profits. Minor criminal activity may seem insignificant when observed at the individual level, but when consolidated, the totals may reach a startling monetary value. Arson is of particular concern due to its obvious destructive qualities. Losses of vital assets may seriously impede production.
Kidnapping or hostage-taking	• A large increase in company profits • The presence of a high-ranking company officials • Economic unrest • Political ties between the company and the government or other countries • New exploration or operations (especially within guerrilla-occupied territory)	The likelihood of a kidnapping incident is fairly remote. The impacts of kidnapping include emotional and psychological stress upon personnel and staff and the families and communities of the hostages. If a company is perceived as not effectively handling a kidnapping incident, its public image can be significantly damaged, which may in turn cause a negative impact on shareholders and partners.
Media scrutiny	• A large increase or decrease in company profits • A major incident (e.g., a fatality or major environmental damage) • A change or shuffle of high-ranking company officials • A new discovery during exploration	Media scrutiny can have either a positive or negative impact upon the company. Care should be exercised when delivering public statements. Procedures must be in place to effectively manage the release of information.
Missing person	• Severe weather • Transportation incidents (e.g., plane crash) • Sudden illness • See also: Kidnapping	People can go missing for a variety of reasons. A company's public image can be significantly affected either positively or negatively depending on how it assists with the recovery of the missing person and meets the needs of the families and communities affected.

Type of Risk	Contributing Factors	Potential Consequences
Strike	• A large increase in company profits • Economic strife among personnel • Political change • Extended periods without pay increases • Deteriorating relationships between organized labor unions and management	Strikes can bring production to a standstill and seriously compromise company profits and public image. Unless properly attended to, strikes may cause long-term damage to the company in the form of ill will from personnel, regardless of personnel returning to work. See also: Media Scrutiny See also: Criminal Activity
Terrorism	• New operations within guerrilla occupied territory • New or continued operations within sensitive environments (e.g., especially areas containing endangered species of animals or fauna) • Relationships with companies that may be in conflict with terrorist organizations • Deficient screening of employees upon hiring • Poor public perception of company	Terrorism can range from a mild disruption of the workplace to make a political statement to a malicious act of devastating violence. Terrorist activities may be targeted towards equipment and transport, or involve the injury or death of personnel. See also: Bomb Threat See also: Criminal Activity
Financial Impact		
Business or economic Interruption	• Major economic disruption in local economy (e.g., substantial currency devaluation) • Political strife in operating regions • Terrorist activities that affect development and delivery of goods • Corporate scandals (e.g., fraudulent financial reporting) • Criminal or civil proceedings against the corporation for negligent or criminal behavior • Loss of key personnel • Incidents that result in the shutting down of major producing areas or facilities	Major business interruptions can substantially affect a company's ability to continue operating. In some cases, the situation can be so severe that a company must declare bankruptcy. Where companies avoid bankruptcy and continue operating under increased financial pressures, the morale of personnel can suffer, leading to even greater losses of productivity.
Medical		
Severe illness affecting many personnel, including epidemic diseases	• Unsanitary environment for food preparation and consumption • Unsanitary environment for personnel quarters • Inadequate ventilation • Inadequate climate controls • Deficient immunization programs	The occurrence of severe illness among groups of personnel can occur as an acute event (e.g., occurrence begins and ends quickly, affecting a limited number of personnel) or as a chronic, systemic condition (e.g., spread of waterborne or mosquito-borne viral or bacterial infections). In an acute event, production losses may be confined to a short period of time. In a chronic situation, losses may continue for a much longer period of time, particularly until the source of the condition is identified and controlled. Personnel may become hesitant to continue working if they believe they are at risk of becoming ill.
Serious injury or fatality	• Faulty or damaged equipment • Ageing equipment • Deficient training procedures • Faulty or damaged protective equipment • Severe weather occurrence • Insufficient risk assessment of the facility • Inadequate procedures • Failure to follow procedures • Lack of managerial leadership	The negative impact of a serious injury or fatality extends well beyond the afflicted individual. The remaining staff incurs emotional and psychological stress, and confidence within the company may be reduced. This may reduce work output by personnel. Should the injury reach the media, public perception of the company may be tarnished if the company is found to be at fault. See also: Media Scrutiny

Type of Risk	Contributing Factors	Potential Consequences
Operational Equipment Failure		
Plant equipment failure	• Ageing equipment • Inadequate maintenance programs • Use of damaged equipment • Misuse by personnel • Lack of predictive or preventive maintenance • Inadequate training • Exceeding stress threshold parameters of equipment • Failure due to environmental stress (e.g., equipment in deserts or offshore) • Inadequate procedures • Failure to follow procedures • Lack of managerial leadership	Major equipment failure can seriously impact the integrity of a facility and the company's production rate. It can also compromise the safety of personnel leading to severe injuries or loss of life and surrounding communities. It is wise to note that, in the instance of a failure, several more components of production may also be adversely affected. This branches out the area of loss significantly.
Loss of key supplies (e.g., fuel or other resource shortages)	• Severe weather incident that ruptures or disables supply lines • Economic strife • Terrorism • Unrealistic consumption requirements estimated when ordering	The loss of a key supply could, potentially, cripple production of the facility.
Facility Incident		
Loss of computerized systems (e.g., control-centre failure)	• Power failure due to severe weather or terrorist activities • Inadequate or absence of computer firewalls, introducing a virus • Lockout incurred from a third party (hackers) • Overloading the computer system (crashing the network) • Inadequate computer hardware and software for the task assigned (crashing the network)	With an ever-increasing reliance on computerized systems, the failure of these systems could be particularly devastating. This threat is increased when the volatile nature of a computer is taken into account. Computer systems are of particular interest to terrorist organizations and are usually a prime target for attack. This attack may be the physical assumption of control (e.g., extreme violence) or a more subtle method of electronic infiltration (e.g., hacking).
Communications systems hardware failure	• Poor hardware selection • Improper usage of hardware • Improper environment for hardware • Severe weather incident • Terrorist activities	The loss of communications is particularly alarming as it may seriously compromise the access to or distribution of resources, especially during an emergency. Communication disruption is a primary target for terrorists.
Utility failure or loss (e.g., water, gas, electricity, sewer)	• Severe weather incident • Terrorist activities • Overloads of equipment	Utility failure or loss can shut down production and safety systems. Significant risks can result during shutdown and the facility can become vulnerable to additional threats as safety systems are lost.
Extreme air pollution	• Process upset • Equipment failure • Terrorism • Severe weather • Seismic event • Bad design and specifications • Negligent practices in maintenance or hardware selection	Release of Air pollutants in significant amounts could cause damage to surrounding human populations and the environment.

Type of Risk	Contributing Factors	Potential Consequences
Industrial explosions	• Inadequate containment of volatile substances • Improper handling of volatile or explosive substances • Insufficient training for personnel handling volatile substances • Improperly cleaned containers that previously held explosive or flammable substances • Work areas containing ignition sources that are too close to explosive or flammable substances	Explosions may cause serious injury or loss of life to multiple personnel, as well as cause extensive damage to equipment and property. Explosions may also release toxic chemicals into the environment. In addition to the immediate damage, an explosion may cause a public spectacle that may damage the public's opinion of the company See also: Media Scrutiny See also: Chemical Release
Facility fire	• Presence of flammable or explosive materials • Buildings or facility constructed of flammable materials • Arson • Improper storage or transport of flammable materials • Inadequate training for personnel involved with flammable and explosive materials	Fires have the potential to destroy an entire facility, cause extensive injury and loss of life and severely decrease production. Facility fires may also require large-scale evacuations of surrounding communities and cause a great deal of negative publicity. See also: Criminal Activity
Hazardous Material Releases		
Oil spills	• Release during transport (e.g., tanker rupture, pipeline rupture) • Blowouts during drilling • Terrorist activities • Inadequate or improper storage vessels • Inadequate training of personnel • Severe weather incident	Oil spills may range in size from a few litres to millions of barrels. Aside from the initial loss of product during the spill, spills may cause significant environmental damage and be very expensive to clean up, especially if they occur in sensitive environments. Oil spills are subject to media coverage and public condemnation. See also: Media Scrutiny
Chemical release	• Release during transport (e.g., tanker rupture, pipeline rupture) • Terrorist activities • Inadequate or improper storage vessels • Inadequate training of personnel • Severe weather incident • Facility explosion	Chemical releases may cause injuries to personnel, and long-term damage to environments and equipment. Chemical releases may contribute to the chances of an explosion occurring. The clean up of a release may be expensive. See also: Industrial Explosions
Radiographic source radiation	• Release of radiation from radiographic equipment	Radiation leaks can create significant health hazards to personnel, particularly if exposure is chronic.
Transportation Incidents		
Vehicles incidents	• Aging vehicles • Inadequate maintenance plans • Vehicles unsuited for terrain • Improper training for operators • Operator fatigue • Unstable terrain • Terrorist activities • Faulty, inadequate or absent safety equipment (e.g., seatbelts, harnesses) • Un-maintained or deteriorating roads	Incidents involving vehicles may cause injury or loss of life as well as bring unwanted media attention. They can also result in significant increases in insurance premiums. See also: Media Scrutiny
Aircraft incidents	• Severe weather incident • Improper filing of flight plan • Inadequate maintenance plans • Terrorist activities • Overloading aircraft capacity • Operator fatigue	Incidents involving aircraft are expensive and hold a high profile in the view of media. Loss of life during an aircraft incident is common. See also: Media Scrutiny and Missing Persons

Type of Risk	Contributing Factors	Potential Consequences
Marine incidents	• Overloading floatation capacity • Severe weather incident • Use of dated or unreliable navigation charts • Operator fatigue • Terrorist activities • Poor maintenance plans	Marine transportation is largely open to environmental assault. Incidents may become very serious to the point of a hull breach causing a spill, and major injuries or loss of life. Due to the sensitive nature of marine environments, an incident may encourage media attention. See also: Media Scrutiny See also: Oil Spill
Rail incidents	• Obstructions on tracks • Terrorist activities • Seismic activity • Improper loading of containers • Poor maintenance plans	Incidents of rail vehicles are most liable to damage the items being transported, especially if the product is liquid (tanker rupture), due to the impact upon derailment. Serious injury and loss of life to persons aboard the rail vehicle is not uncommon in the event of a derailment. Surrounding communities can also be affected if an incident causes a release of hazardous chemicals.

3.5 Establishing a Response Organization

3.5.1 Objective and Scope

The primary objective in defining a response organization as well as the roles and responsibilities of the individuals involved is to ensure consistency in response throughout your organization, regardless of the type, level or location of an incident. Although there are many examples of response organizations, this element is based on the Incident Command System (ICS) to illustrate essential functions and requirements. ICS was chosen as the backbone of this element because it successfully integrates all functions and resources required during any type of emergency and is designed to grow as the impact and severity of an emergency increases.

As you develop your response organization, it is important to understand how it will function in relation to your company's risks, as described in Element 3.4 Assessing Risk on page 14, your company's definitions of emergency levels (also referred to as tiers) as described in 4.2.3 Understanding Emergency Levels on page 54 and the capabilities of the individuals assigned roles and responsibilities as discussed in 4.1 Assigning Roles and Responsibilities on page 49.

The key component of this element is described below:

3.5.2 Defining the Response Organization

Essential Actions

- Establish a response organization that provides both corporate and field level involvement.

  See also: *Incident Command System on page 30 and Understanding Corporate and Field Roles on page 37.*
- Identify and define key roles within the response organization such as the following ICS roles:
  - **Incident Commander** to establish and direct a command structure that suits the needs of the incident; notify all affected organizations and individuals; and coordinate all response activities and resources.
  - **Operations Section Chief** to direct tactical operations.
  - **Planning Section Chief** to assess the probable course of events and assemble and evaluate information needed to prepare incident action plans.
  - **Logistics Section Chief** to assemble personnel, resources and equipment needed to respond to the incident.
  - **Finance Section Chief** to manage financial documentation, provide financial planning advice to meet response requirements and handle compensation and damage claims.
  - **Deputy Incident Commander** to assist the Incident Commander in all aspects of that role.
  - **Information Officer** to provide assistance and advice to the Incident Commander in relation to all internal and external (e.g., employees, residents, media) communication needs.
  - **Safety Officer** to provide assistance and advice to the Incident Commander in relation to all safety issues.
  - **Liaison Officer** to provide assistance and advice to the Incident Commander by acting as a contact and information source for other agencies (e.g., regulatory agencies) involved in an incident.

  See also: *Typical Response Positions on page 33.*
- Clearly document the authority, responsibilities and chain of command between teams and roles in your response organization.
- Define emergency levels and how the response organization will change with each level.

  See also: *4.2.3 Understanding Emergency Levels on page 54.*

3.5.3 Background

Incident Command System Overview

The Incident Command System (ICS) provides a management system that organizes the functions, tasks and staff within the overall emergency response. It transforms the confusion of an emergency into a well-managed response by recognizing people as the primary assets and providing them the critical answers to "Who's in charge" and "What's my job". It is applicable to small-scale daily operational activities as well as major mobilizations.

ICS promotes communications and coordination; however, for ICS to work, all responders must understand the system and their roles within it. Such an understanding can only be gained through training, experience, and teamwork.

ICS is a useable, adaptable and well-tested approach to emergency management that is gaining increasing acceptance by governments and industry. The success of ICS results from its:

- modular organization
- use of common terminology
- unified command structure
- span-of-control
- resource management

ICS provides the flexibility needed to rapidly activate and establish an organizational format around the functions that need to be performed at any given time during an incident.

ICS can be used to address any emergency, small or large, such as injury incidents, spills, fires, earthquakes, weather-related incidents and kidnappings. It can also be used to plan for major events, such as international conferences that might draw large crowds or create the potential for terrorist acts. It has become a standard emergency response system and has been adopted for use by many industries and government agencies. It is an all-risk system, which means that the same structure and system can be used regardless of the type of situation or number of agencies involved. Positions within the ICS are fixed and can have specific functions, ensuring all responders know what to do and where they belong within the structure.

Incident Action Plans

All incidents need an action plan. Within the ICS structure, response activities are focused on the Incident Action Plan developed for that particular incident by the Planning Section and Incident Commander. Incident Action Plans provide the incident objectives, the overall incident strategy, specific tactical actions and supporting information for the next operational period. For simple incidents the plan may be oral or written. Large or complex incidents will require that the action plan be documented. Incident Action Plans may have a number of attachments, including incident objectives, organization assignment list, incident radio communication plan, medical plan, traffic plan, safety plan and incident map.

ICS Organization

The ICS organization is comprised of five functional sections: Command, Operations, Planning, Logistics and Finance. Examples of a "basic" and an “expanded” ICS structure are shown in Figures 7 and 8 below.

Figure 7: Basic ICS Functional Organization

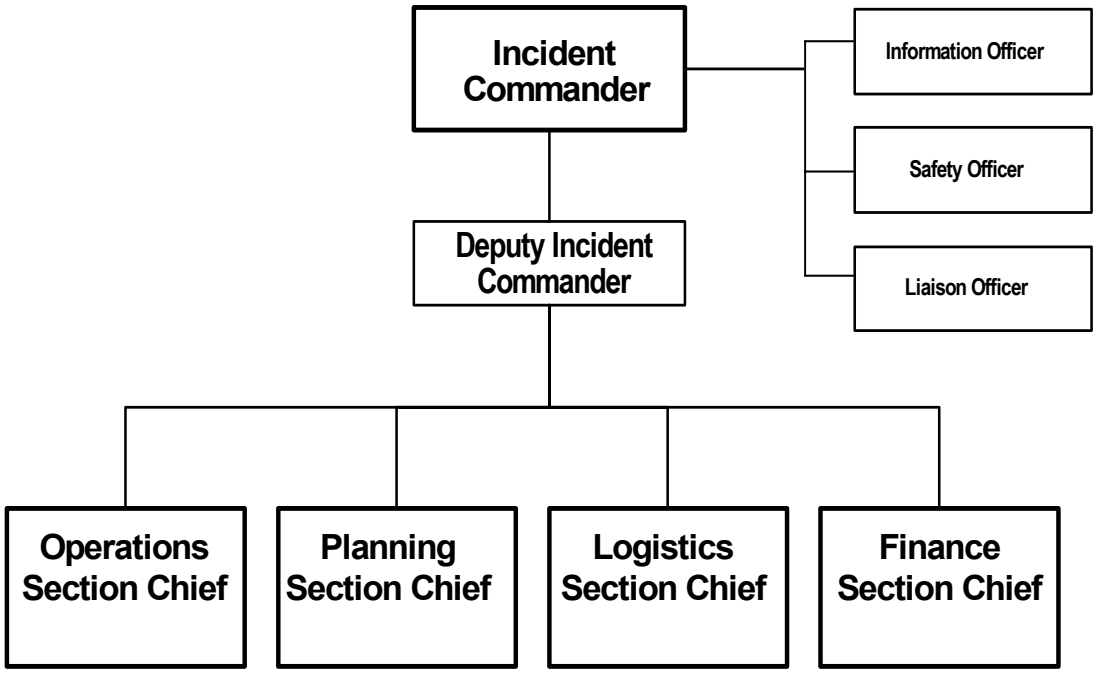
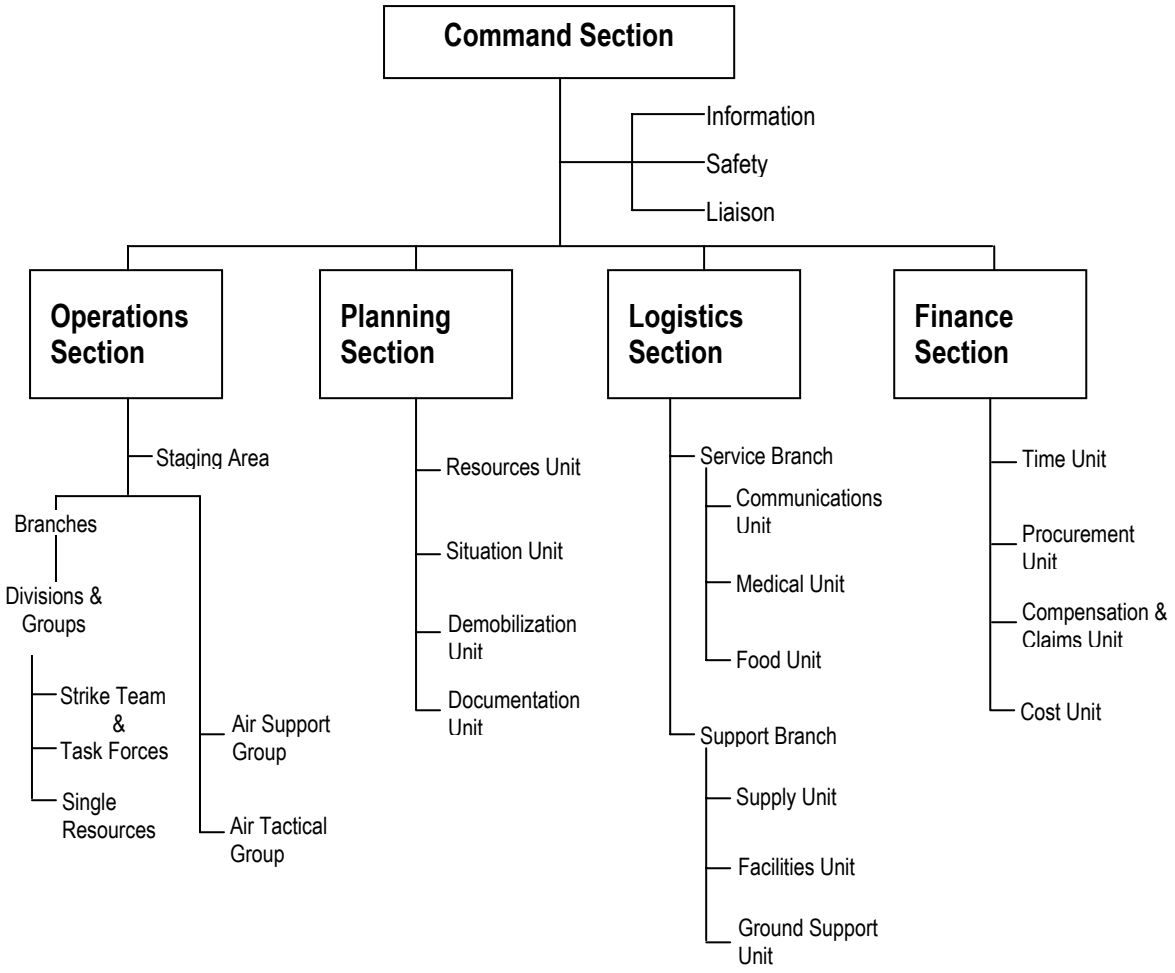


Figure 8: Expanded ICS Organization



The Command Section is led by an Incident Commander who is supported by Command Staff. Each of the other four sections is managed by a Section Chief and supported by other functional units. The Sections have specific functions, as follows:

- COMMAND sets response objectives and undertakes coordination.
- OPERATIONS undertake tactical response actions.
- PLANNING investigates the incident and establishes the technical basis for action plans.
- LOGISTICS provides equipment and services.
- FINANCE manages finances and administration.

The ICS organizational structure develops in a modular fashion based on the type and scale of incident. The organization's staff builds from the bottom up, with responsibility and performance placed initially with the fist competent responder on site. If this individual can simultaneously manage all major functional areas, no further organization is required. However, as the need exists to handle an escalating incident, an Incident Commander is designated (which may or may not be the fist responder) and separate sections, as described above, can be invoked to handle multiple functions.

ICS is capable of expanding to meet an escalating situation by invoking Sections, Groups, Branches, Units, Strike Teams, and Resources as required and by ICS protocols. This adding of functions, with staff assigned, recognizes that a small emergency need only a small organization, but a larger emergency needs a large organization. The specific organizational structure of any given incident will be based on the management needs of the incident.

Typical Response Positions

Position	Overview	Responsibilities
Incident Commander	The Incident Commander is responsible for the overall management of the incident. The Incident Commander directs incident activities including the development and implementation of strategic decisions and approves the ordering and releasing of resources. The Incident Commander may assign a Deputy Incident Commander and delegate authority as needed to assist in carrying out Incident Command responsibilities.	• Ensures that appropriate actions are taken to protect the health and safety of response personnel. • Reviews general emergency procedures, common responsibilities and action checklists. • Assesses the situation and obtains an incident briefing from the prior Incident Commander, if there was one. • Determines the incident potential and monitors for escalation or de-escalation of emergency. • Makes initial contact with other responding parties. • Establishes and maintains command. • Determines the company's role in the response. • Determines incident strategies and objectives. • Establishes response priorities. • Establishes an On-site Command Post. • Coordinates all organization actions with the appropriate agency representatives, other response organization personnel, and stakeholders as appropriate. • Coordinates with outside agencies having jurisdiction and informs stakeholders and public, as appropriate and according to company policies. • Establishes an appropriate organization and makes initial ICS assignments. • Liaises with appropriate corporate members according to company procedures. • Approves and authorizes the implementation of an Incident Action Plan. • Determines information needs and advises Command and General Staff. • Authorizes release of information to news media. • Orders the demobilization of the incident when appropriate.
COMMAND STAFF		
Deputy Incident Commander	If a Deputy Incident Commander is assigned, he may be delegated the authority to manage a functional operation or perform a specific task. In some cases, the Deputy may act as relief for a superior and therefore must be fully qualified in the position.	• Reviews general emergency response procedures and common responsibilities. • Makes initial ICS assignments. • Supervises the Section Chiefs and response operations. • Makes initial resource need projections and acquires and allocates resources to meet objectives. • Ensures adequate and open information flow, including facilitating, arbitrating and filtering. • Organizes and facilitates planning meetings and shift briefings for the Incident Commander, if so assigned. • Advises the Incident Commander of issues as appropriate.

Position	Overview	Responsibilities
Information Officer	The Information Officer is responsible for developing and releasing information about the incident to the news media, to incident personnel and to other appropriate agencies and organizations.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Determines from the Incident Commander if there are any limits on information release. • Develops material for use in media briefings. • Establishes a Joint Information Center in coordination with public information staff from other response organizations. • Obtains Incident Commander approval for media releases. • Informs media and conducts media briefings. • Liaises with appropriate corporate members according to company procedures. • Arranges for tours and other interviews or briefings that may be required. • Obtains media information that may be useful to incident planning. • Keeps the general public and stakeholders informed (e.g., through the use of a website, joint press releases, situation reports). • Collects and assembles incident information from the Situation Unit and others. • Prepares an initial information summary as soon as possible after arrival, establishes a schedule for summary updates and prepares updates. • Arranges and conducts press conferences for the Incident Commander. • Supervises media personnel activities to ensure all safety rules are followed and operations are not impacted. • Responds to special requests for information. • Provides the Incident Commander with feedback on media reporting of the incident.
Safety Officer	The Safety Officer reports to the Incident Commander and is responsible for the health and safety of all response personnel in the field. The Safety Officer is responsible for establishing safety zones, personal protective equipment requirements, and for the general overall safety, hazard identification, and preparation of on-scene Site Safety Plan(s) designed to protect the field responders.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Obtains a briefing from the Incident Commander. • Assesses the situation and identifies any existing or potential hazardous situations associated with the incident. • Verifies weather information (e.g., wind direction, wind speed, temperature, chill factor) with the Incident Commander. • Evaluates the hazards created by the incident (e.g., health, flammability, reactivity, and physical hazards). • Works with the Incident Commander to evaluate risk factors. • Establishes Hazard Control Zones (e.g., hot, warm, cold, and the isolation perimeter) as required. • Provides safety information for establishing site access. • Develops on-scene Site Safety Plan(s). • Verifies that personal protective equipment is available and adequate for the hazard(s) present. • Works with the Incident Commander to ensure personnel are not placed in an unsafe emergency

Position	Overview	Responsibilities
		situation. • Supports the Incident Commander in ensuring that the emergency scene is stabilized before clean-up operations are initiated. • Supports the Incident Commander in ensuring that a plan is established to clean up or dispose of contaminated supplies and equipment. • Provides regular and timely updates to the Incident Commander.
Liaison Officer	Incidents that are multi-jurisdiction, or have several agencies involved, may require the establishment of the Liaison Officer position on the Command Staff.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Provides a point of contact for assisting cooperating Agency Representatives. • Identifies Agency Representatives from each agency including communications link and location. • Identifies all stakeholders including affected communities, interest groups, landowners, leaseholders, non-jurisdictional government agencies and others. • Liaises with appropriate corporate members according to company procedures. • Contacts each stakeholder, maintains a list of contacts and establishes communication links. • Maintains a list of assisting and coordinating agency contacts. • Responds to requests for information from stakeholders. • Identifies current or potential concerns of stakeholders, and conveys them to the Incident Commander. • Keeps agencies that are supporting the incident aware of the incident status. • Participates in planning meetings and provides current resource status information, including limitations and capabilities of assisting agency resources. • Arranges meetings between response staff and stakeholders as required.
GENERAL STAFF		
Operations Chief	The Operations Section Chief is responsible for the management of all field operations directly applicable to the primary mission. The Operations Chief activates and supervises elements in accordance with the Incident Action Plan and directs its execution; activates and executes the Site Safety Plan; directs the preparation of unit operational plans; requests or releases resources; makes expedient changes to the Incident Action Plan as necessary; and reports such to the Incident Commander for approval.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Develops or assists in the development of the Operations input to the Incident Action Plan (e.g., strategic goals, tactical objectives and response task assignments), and provides information needed to support preparation of a General Plan (i.e., long-term strategic plan). • Briefs and assigns operations personnel in accordance with the Incident Action Plan. • Establishes and maintains communications with field operations. • Assesses the situation and determines what tasks must be undertaken to ensure the safety of response personnel, stabilize or control the source, and protect people, the environment, and property.

Position	Overview	Responsibilities
		• Supervises the execution of the Incident Action Plan for Operations. • Liaises with appropriate corporate members according to company procedures. • Requests resources needed to implement the Operations' tactics as part of the Incident Action Plan development. • Ensures a Staging Area(s) has been established, depending upon the size of the incident. • Ensures safe tactical operations.
Planning Chief	The Planning Section Chief is a responsible for supervising the work of Section personnel in organizing and managing the: (1) collection, evaluation, and display of information about an incident; (2) status of equipment and personnel resources assigned to response operations; (3) preparation of the Incident Action Plans for each operational period; (4) preparation of a General Plan (i.e., long-term strategic plan) if appropriate; (5) preparation of incident-specific plans; (6) provision of a wide range of environmental services including permitting, waste disposal, wildlife, etc.; (7) assignment of technical specialists; (8) documentation and filing of all response operations information; and (9) demobilization operations.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Receives briefing from the Incident Commander. • Activates appropriate Planning Section personnel. • Prepares documents descriptive of incident and response operations. • Establishes and maintains incident information and situation displays. • Liaises with appropriate corporate members according to company procedures. • Responds to informational requests including status reports according to company procedures and Incident Commander approval. • Supervises preparation of the Incident Action Plan. • Participates in planning and other meetings (e.g., objectives, tactical operations, planning, shift briefing) as required. • Develops the General Plan (i.e., a long-term strategic plan). • Establishes information requirements and reporting schedules for all ICS organizational elements for use in preparing the Incident Action Plan. • Ensures that resource tracking has been established. • Makes recommendations for any specialized resources needed in support of the incident. • Provides incident organizational structure including names and locations of assigned personnel. • Determines the need for and assigns technical specialists where needed to analyze and resolve technical issues. • Assists in analyzing information on alternative response technologies, as needed. • Provides periodic predictions on incident potential.
Logistics Chief	The Logistics Section Chief is responsible for providing facilities, transportation, communications, services, and material in support of the incident. The Logistics Section Chief participates in development and implementation of the Incident Action Plan and activates and supervises Branches and Units within the Logistics Section.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Plans organization of Logistics Section. • Assigns work locations and preliminary work tasks to Section personnel. • Notifies Resource Unit of Logistics Section units activated, including names and locations of assigned personnel. • Assembles and briefs Branch Directors and Unit Leaders. • Participates in preparation of the Incident Action Plan.

Position	Overview	Responsibilities
		• Identifies service and support requirements for planned and expected operations. • Provides input to and reviews Communications Plan, Medical Plan and Traffic Plan. • Coordinates and processes requests for additional resources. • Liaises with appropriate corporate members according to company procedures. • Reviews the Incident Action Plan and estimates Section needs for next operational period. • Advises on current service and support capabilities. • Prepares service and support elements of the Incident Action Plan. • Estimates future service and support requirements.
Finance Chief	The Finance Section Chief is responsible for all financial and cost analysis aspects of the incident and for supervising members of the Finance Section.	• Reviews general emergency response procedures, common responsibilities and action checklists. • Attends briefing with other Section Chiefs to gather information. • Attends planning meetings to gather information on overall strategy. • Determines resource needs. • Meets with assisting agency representatives as required. • Provides input in all planning sessions on financial and cost analysis matters. • Maintains contact with company offices on finance matters according to company policies and procedures. • Ensures all obligation documents initiated at the incident are properly prepared and completed. • Briefs administration personnel on all incident-related business management issues needing attention and follow-up prior to close of the incident.

Understanding Corporate and Field Roles

Most companies that have both corporate offices and field operations are organized into a hierarchy that places ultimate authority among management and senior executives at regional or centralized corporate offices. While this authority is essential to the day-to-day operations and development of the company, it will not always take precedence during emergency response.

Response organizations that follow ICS rely on personnel who are first at the scene to control the incident response while corporate participation will range from the need to be kept informed, to providing support as part of the ICS structure to taking on the role of Incident Commander as the emergency escalates. For example, during a level one incident, the corporate communications department may be alerted to address potential media enquiries. During a level two incident, a Finance and Administration Section Chief from head office may join the response team, while a level three incident may result in the President taking over the role of Incident Commander because the incident is so substantial, it threatens the overall integrity of the company.

Generally, the more serious the incident (e.g., the higher the incident level), the greater the involvement of corporate participants.

3.6 Identifying Emergency Resources

3.6.1 Objectives and Scope

The primary objective of identifying emergency resources is to ensure all necessary resources are available and ready to be called upon in an emergency. Emergency resources include personnel and a variety of equipment, supplies and materials.

Key components of identifying emergency resources include:

- Defining Needs and Identifying Resources
- Preparing and Maintaining Resource Inventories
- Maintaining Maps of Emergency Zones
- Preparing and Maintaining Contact Lists

3.6.2 Defining Needs and Identifying Resources

Essential Actions

- Identify needs for emergency response resources based on risk assessments for each facility or area of operation.

  See also: *3.4 Assessing Risk on page 14.*
- Prepare inventories of existing resources including:
  - equipment and capabilities of personnel on site
  - equipment and capabilities of third-parties that may assist in an emergency response (e.g., mutual aid partners, fire fighters, first aid and medical services)
- Identify gaps between existing resources and needed resources.
- Identify suppliers of remaining resources and ensure they can deliver in a reasonable time to meet emergency response needs.

  Tip: *In some cases, suppliers will be able to deliver immediately whereas others may require several days, weeks or even months to deliver. Where delivery times are excessive, consider other alternatives for obtaining the resource and maintaining it within your own inventory.*

3.6.3 Preparing and Maintaining Resource Inventories

Essential Actions

- Prepare inventories of all emergency personnel, equipment, materials and other resources available:
  - onsite

  Tip: *It may be useful to construct a map(s) depicting where all onsite resources are kept.*
  - through third-party responders (e.g., mutual aid partners)
  - from suppliers
- Ensure records of training, emergency exercises and certifications are kept for all assigned response personnel.
- Prepare maintenance schedules for company-owned response equipment based on manufacturer's recommendations.
- Ensure third-party responders and suppliers of offsite equipment meet manufacturer specifications for maintenance and replacement.
- Periodically inspect onsite equipment to ensure it is being maintained to schedule and ask to see offsite equipment and maintenance records.

3.6.4 Maintaining Maps of Emergency Zones

Essential Actions

- Obtain regional maps and nautical charts from existing sources (e.g., government departments) to be used in directing emergency services to the site of an emergency.
- Verify that maps and nautical charts are current.
- Prepare detailed planning maps and charts that plot and identify:
  - the facility location, name and access roads
  - residents' locations and reference numbers
  - other industrial facilities, such as wells and facilities in the area
  - primary, secondary, local and access roadways and dead-ends
  - environmentally sensitive areas
  - lakes, rivers, streams and other waterways which may act as barriers or landmarks
  - campgrounds, churches, schools, hospitals and other community facilities
  - railways and airports
  - corporate boundaries
  - a legend, scale and north indicator
  - roadblock locations
  - nearest urban centers
  - environmentally sensitive areas
  - basic site diagrams with hazardous areas, main storage areas, locations of emergency response equipment and access-egress routes
  - potential areas of impact
- Choose a map scale that provides a clear representation of the entire mapped area.
- Produce wall-sized maps and charts for large or complex planning areas.
- Maintain reduced copies of the wall maps and charts in emergency response plans for people who operate from vehicles or away from the main facility.
- Consider opportunities to use digitized maps (Geographical Information System) and computer-based applications (databases).
- Consider sharing maps and databases (residents) with other operators in the area.

3.6.5 Preparing and Maintaining Contact Lists

Essential Actions

- Create a list of all contacts, both internal and external, and how they can be reached (i.e., phone numbers, email, fax, and cellular numbers), such as:
  - ambulance services
  - chemical information services
  - local hospitals
  - hotels
  - travel agencies
  - car rental companies
  - transportation (e.g., surface, air, marine)
  - legal
  - management
  - security
  - financial
  - environmental
- Include with each contact a brief description of the resource, a key contact name and an auxiliary name and number in the event the key contact cannot be reached
- Ensure lists are available in all emergency response plans.
- Where applicable, post contact lists in visible areas and ensure all response personnel have of a copy.
- Make all key contact personnel aware that they are key contact personnel and on the contact list.
- Schedule regular review and updating of contact lists and ensure that all circulated copies are of the most current version.

3.6.6 Background

Emergency resources include but are not limited to:

- third-party assistance (e.g., police, fire fighters, hospitals and government agencies)
- communications equipment
- fire fighting equipment
- internal and external detection and alarm systems
- knowledgeable and trained personnel
- reference materials (e.g. MSDS sheets)
- maps (e.g., regional, detailed and sensitivity maps)
- nautical charts
- site drawings and maps
- mutual aid agreements
- risk-specific and site-specific response plans
- personal protective equipment and monitors
- shelter
- spill response equipment
- supplies (e.g., food and clothing)
- technical data
- transportation

3.7 Developing Mutual Aid Agreements

3.7.1 Objective and Scope

The primary objective in developing mutual aid agreements is to share the emergency resources and capabilities of two or more facilities or organizations. A mutual aid agreement is an agreement between two or more organizations with operations or facilities in the same area outlining how they will assist each other in responding to incidents. These agreements define each participant's responsibilities for providing aid and support during an incident. Sharing equipment, skills and other resources between companies may prove to be more cost effective than purchasing the resources entirely and may provide faster service than relying upon outside contractors.

Key components of developing mutual aid agreements include:

- Choosing Mutual Aid Partners
- Negotiating Agreements

3.7.2 Choosing Mutual Aid Partners

Essential Actions

- Assess your current operations and risks to identify where joint or adjacent operations present shared risks and opportunities to share response resources.
- Identify emergency resource needs of the company that cannot be satisfied onsite.
- Investigate the resource capacity or surplus of neighboring or similar operations or organizations.
- Contact all parties you want to include in a mutual aid agreement and address these questions:
  - Does each facility or organization have an emergency response plan?
  - What are each organization's emergency response goals and will participants work cooperatively to achieve them?
  - What is the term of the agreement and what are the conditions for terminating it?
  - What are the minimum standards for response materials, equipment and personnel?
  - What third-party contracts for emergency response services exist?
  - What financial arrangements, liability and insurance should be included?
  - How can community concerns be addressed in the proposed agreement?
  - Are there common approaches for community safety as well as common maps, charts, resources and community database information?

Tip: *Investigate associations of similar companies to find if there is already a resource pool that can be joined.*

3.7.3 Negotiating Agreements

Essential Actions

- Before creating a mutual aid agreement, work with selected partners to develop procedures for:
  - activating the agreement and mobilizing all respondents
  - assigning roles and responsibilities
  - sharing resources and equipment
  - dealing with liability issues
  - communicating with respondents during an emergency
  - communicating with the community during and after an emergency
  - training and exercises to ensure the agreement works
  - maintaining the agreement
- Identify a spokesperson to negotiate on your company's behalf.
- Negotiate the sharing of resources among all organizations involved.
- Consult the ICS Chief of Finance and Administration and the Chief of Logistics to ensure the mutual aid agreement is realistic, viable and sustainable.
- Consult legal advice to ensure that the resulting agreement is sound and mutually protective and inclusive.

  See also: *Figure 9: Example Mutual Aid Agreement on page 43.*
- Review the agreement periodically to ensure it remains valid and the resources it offers continue to be available.
- Include mutual aid partners in emergency exercises.

Figure 9: Example Mutual Aid Agreement

[3]PARTIES:

[Party One], a corporation with an office at [Place]

-and-

[Party Two]

RECITALS

A. A wide range of emergencies, natural and man made, may occur that have some impact on [Party One] or [Party Two].

B. In the event such an emergency ("Emergency") occurs, [Party One] and [Party Two] wish to provide assistance to each other as may be required.

THEREFORE, in consideration of the following terms and conditions, [Party One] and [Party Two] agree that:

1. [Party One] and [Party Two] agree to provide assistance to each other in response to an Emergency ("Emergency Assistance"). However, [Party One] and [Party Two] acknowledge and agree that this Agreement does not impose any binding obligation on either party to provide Emergency Assistance. Rather, this Agreement is a statement of the parties' intention to provide such Emergency Assistance voluntarily.
2. In this Agreement the party requesting Emergency Assistance shall be called the "Requesting Party" and the party providing the Emergency Assistance shall be called the "Providing Party".
3. Where the assistance of any of the personnel of the Providing Party is provided to the Requesting Party, such personnel shall at all times continue to be employees of the Providing party and shall at no time and for no purpose be deemed to be employees of the Requesting Party. Personnel of the Providing Party will at times, while responding to a request from the Requesting Party for Emergency Assistance, be under the control and supervision of the Requesting Party. During such time as personnel from the Providing Party are responding to a request from the Requesting Party for Emergency Assistance, such personnel will comply with all safety regulations of the Requesting Party. It shall be the responsibility of the Requesting Party to make such safety regulations known to personnel of the Providing Party.
4. Personnel of the Providing party who are providing Emergency Assistance under this agreement shall be equipped by the Providing party with working protective equipment that is normally used by personnel of the Providing Party.
5. The parties agree that the intent is to provide Emergency Assistance when requested to do so by the other party. However, at all times and in all cases the Providing Party shall be entitled, in its sole discretion, to refuse to provide any personnel or equipment to the Requesting Party or to withdraw any or all personnel or equipment previously provided to the Requesting Party.
6. The Requesting Party shall reimburse the Providing Party for all of its costs and expenses in providing the Emergency Assistance to the Requested party including, without limiting the generality of the foregoing: (a) salaries and wages; (b) use of equipment, materials, supplies, etc.; (c) transportation; and (d) other additional costs. [The Providing Party and its personnel shall not expect nor receive compensation or reward for emergency medical services or first aid assistance provided by doctors, registered nurses, or other registered health discipline members.] The Providing party shall invoice the Requesting party for all such costs and expenses. The Requesting party shall be entitled to receive from the Providing party written documentation in support of the invoice before providing any reimbursement.

[3] Mutual Aid Agreement from CAN/CSA-Z731-95 Emergency Planning for Industry, A National Standard of Canada, Major Industrial Emergencies, Canadian Standards Association and Major Industrial Accidents Council of Canada, Reaffirmed 2000.

7. The Providing Party shall keep for one (1) year all timesheets and records related to personnel or equipment provided as Emergency Assistance as may be necessary in order to verify amounts invoiced under section 6.
8. The Requesting party shall indemnify and hold harmless the Providing Party, its directors, officers, agents, contractors and employees, from and against all loss, damage, cost, expense, and liability resulting from injury to or death of any person or damage to or destruction of property, arising out of the providing of Emergency Assistance by the Providing Party, whether or not such loss, damage, cost, expense, or liability results entirely or in part from the negligence or other fault of the Providing Party or any of its directors, officers, agents, employees, contractors, or persons employed by such contractors, except such loss, damage, cost, expense, or liability as may be caused by the gross negligence or willful misconduct of the Providing Party's officers, agents, employees, contractors, or persons employed by such contractors.
9. Requests for Emergency Assistance under this Agreement shall be directed to the persons designated below:

    (a) [Party One]

    (i) Site Contact: _____

    (ii) 24-Hour Contact: _____

    (b) [Party Two]

    (i) Site Contact: _____

    (ii) 24-Hour Contact: _____

10. Either party may withdraw from this Agreement upon providing thirty (30) days prior written notice to the other party.
11. This Agreement is effective as of the last date of execution set out below.

[Party One]	[Party Two]
Per:	Per:
_____	_____
Date:	Date:
_____	_____

3.7.4 Background

In a mutual aid agreement two or more companies forge an agreement of shared resource to the benefit of all involved. Equipment, skills, response programs and personnel may be bargained for as resources that one party in the agreement is found to be deficient in.

Participating in mutual aid agreements may be more cost effective and provide faster response times than relying upon contracted companies for assistance or purchasing expensive equipment that may be rarely used. For example, trucks and heavy transport from a nearby facility may be available in the event of an incident in exchange for access to hazardous chemical spill equipment and expertise. In this instance both the bargained resource and the resource being bargained for amount to a considerable expense should one company wish to purchase them outright, but through the agreement the resources are shared at a much more affordable cost.

3.8 Establishing Emergency Communication Systems

3.8.1 Objective and Scope

The primary objective in establishing communication systems for emergency response is to ensure systems are in place and functioning and personnel are trained in their use before an incident occurs. Communication systems can include equipment (e.g., telephones, pagers, cell phones, two-way radios, computer networks and satellite phones), and communication procedures.

Key components of establishing communication systems include:

- Selecting and Installing Hardware
- Developing and Implementing Communication Procedures

3.8.2 Selecting and Installing Hardware

Essential Actions

- Assess each location to determine what communication systems are necessary, assuming that all personnel at those sites must have the means available to them to contact key personnel in an emergency.

  Tip: *In locations that are covered by standard telephone and cellular systems, satellite phones may not be necessary. In other locations, the only means of communication may be via satellite phones or two-way radios.*
- Identify communications systems available at each location and identify gaps.
- Evaluate the need for secure communication capabilities.

  Tip: *Cellular telephone signals can be interrupted by topographical changes and other cellular phones for which they are not intended can intercept them. As a result, cellular communications may not offer the most secure method of communication.*
- Obtain and install new communications hardware and software as necessary.
- Ensure systems will operate for extended periods in adverse conditions.

  Tip: *Provide backup power and replacement batteries to allow continuous, uninterrupted operation at fixed facilities or emergency sites where response team members may be isolated.*
- Identify locations of communication systems on site drawings and maps, including telephones located outdoors or at field facilities.

3.8.3 Developing and Implementing Communication Procedures

Essential Actions

- Develop standard templates for:
  - documenting and maintaining lists of key telephone numbers for each site (e.g., main control rooms and key areas of major facilities as well as telephones throughout each site)
  - documenting the types and locations of communication systems available at each site (e.g., base stations, mobile and hand-held units for radio communications)
  - identifying resources available to users (e.g., manufacturer's user guides, training, company procedures)
- Develop procedures for:
  - using communication systems as part of emergency response, including establishing priorities for use of different types of communication systems (e.g., secure versus non-secure)
  - using standard terminology in the use of the system (e.g., terms that describe successive warnings as incidents escalate in severity)
  - assigning channels and procedures for emergency radio use and traffic
  - testing, maintaining and replacing or upgrading communications equipment
- Develop and implement training programs for users.
- Post the locations of communication equipment in a visible area at each site.

  Tip: *Maps can be useful to quickly illustrate the location of the device.*
- Ensure procedures are available to users.
- Update procedures as equipment and facilities change.

3.9 Defining How to Communicate with the Public

3.9.1 Objective and Scope

The primary objectives in communicating with the public during the development of emergency response programs and during incidents are to ensure community safety and protect the image of the company. Communications with the public is a regulated requirement in many jurisdictions.

Key components of communicating with the public include:

- Identifying Publics
- Establishing Procedures for Communicating with the Public

3.9.2 Identifying Publics

Essential Actions

- Identify permanent and temporary communities near your operations that may be adversely affected by an incident.

  Tip: *Permanent communities include residential and industrial sites while temporary communities include campgrounds and sites that attract seasonal or transient residents, such as hunting, herding and trapping sites.*
- Contact with potentially affected communities and their residents to verify their needs during emergencies, such as:
  - key contacts within each residence or business
  - disabilities requiring special assistance during evacuations
  - health issues (e.g., respiratory problems such as asthma that may require early evacuation)
  - livestock and pets
- Identify other communities that will likely want to be kept informed, such as:
  - shareholders
  - partners
  - funding agencies
  - news media
  - hospitals
  - government agencies

3.9.3 Establishing Procedures for Communicating with the Public

Essential Actions

- Develop procedures for:
  - communicating with neighboring communities during the development and maintenance of emergency response programs (e.g., through mailings, open houses, town-hall meetings)
  - communicating with neighboring communities during an emergency (e.g., to conduct evacuation procedures)
  - providing information to the community through the media
  - providing information to government agencies
- Define and document minimum standards for the types of information that will be communicated to the community and media during an incident relating to:
  - release of the names of injured persons before next-of-kin have been notified
  - speculation on causes of incidents and fault
  - discussion of financial impacts
  - release of proprietary information
  - discussion of potential consequences (e.g., subsequent damages, layoffs, legal proceedings)
- Prepare procedures and provide training to ensure communication standards are met.

  See also: *the United Nations Environment Programme (UNEP) – Awareness and Preparedness for Emergencies at a Local Level (APELL). This program was developed by UNEP in conjunction with governments and industry with the purpose of minimizing the occurrence and harmful effects of technological accidents and environmental emergencies. The strategy of the APELL approach is to identify and create awareness of risks in industrialized communities, to initiate measures for risk reduction and mitigation, and develop coordinated preparedness between industry, local authorities and the local population.*

3.9.4 Background

It is essential that the community be informed of the risks they face as a result of your company's operations. Involvement of the neighboring communities in the development of facility emergency response programs will allow your company to obtain relevant information for evacuation plans and may also provide additional information about available resources. It will also assist in the implementation of response measures during emergencies because those affected will be aware of how the response will be conducted and how it will affect members of the community. The greater the level of risk in your operations, the greater the need for community involvement.

4.0 Emergency Response Plans

Overview

An effective emergency response plan is concise and well organized with sufficient detail to ensure quick access to critical information collected through the Planning and Preparedness phase. It also provides specific information to assist responders in focusing their efforts on various aspects of response (e.g., notification versus establishing emergency response centers). The primary objective of this section is to describe the key sections required to develop an appropriate emergency response plan that can be effectively used to initiate a response to an incident.

Scope

This *Guideline for Developing Emergency Response Programs* provides guidance and resources for the following elements of emergency response:

- Assigning Roles and Responsibilities
- Developing an Activation Plan
- Defining Notification and Mobilization
- Developing Risk- and Site-Specific Response Strategies
- Defining Reporting Processes
- Establishing Incident Command Posts
- Providing Security
- Establishing a Process for Damage and Claims Assessment
- Providing Critical Incident Stress Management

4.1 Assigning Roles and Responsibilities

4.1.1 Objective and Scope

The primary objective of assigning roles and responsibilities within your emergency response plans is to ensure everyone in your organization knows how they fit into response activities, who to contact for help and who is in charge. This awareness will help ensure that the members of your response teams are committed to their roles and that personnel who are not part of your response teams have a high level of trust in your company's ability to respond effectively.

Roles and responsibilities should be assigned according to the response organization your company has established. Response organizations are discussed in 3.5 Establishing a Response Organization beginning on page 29.

The key component of this element is described below.

4.1.2 Assign and Document Roles and Responsibilities

Essential Actions

- In accordance with your response organization, establish response teams in all areas of your operations, including corporate offices and field facilities, to ensure a team is available within a reasonable distance to any potential incident site.

  Tip: *In some cases incidents will occur away from company facilities (e.g., kidnapping) and should be managed from head office.*

  See also: *3.5 Establishing a Response Organization on page 29.*
- Identify roles and responsibilities that should be assigned to corporate officers and managers.

  Tip: *Risks that directly threaten or could escalate to become a direct threat to the corporation's ability to operate (e.g., kidnappings of senior personnel, financial disasters) require the direct involvement of senior management as members of the response team. Risks that are specific to a particular site or facility should not directly involve senior management but rather should rely on local responders who have direct knowledge of the location, its hazards and the site-specific response plan.*
- Identify individuals at each location who have adequate knowledge of the operations and the location to be able to participate effectively as a member of a response team.

  Tip: *It is essential that all team members are capable to act as responders (i.e., through appropriate training) and that everyone in your organization from senior management to field personnel understands that only the individuals assigned specific response roles should be directly involved in any response activities.*
- Match individuals to the roles most suited to their regular responsibilities (e.g., individuals responsible for purchasing may be appropriate as part of logistics teams while facility supervisors may be appropriate as incident commanders for level one incidents).

  Tip: *To minimize risk to responders, they should only take on roles and responsibilities for which they have been specifically trained and certified.*
- Ensure individuals are willing to accept these roles and believe they can carry them out.
- Obtain supervisory approval of team members.
- Provide training in individual and team roles.
- Conduct emergency exercises to test the training and the response assignments.
- Periodically review role assignments to determine if changes are necessary.
- Cross-train individuals in more than one role to ensure adequate backup in an emergency.

  Tip: *Cross-training may also extend across facilities so that the team members at one facility can readily back up the team members at another facility.*

4.2 Developing an Activation Plan

4.2.1 Objective and Scope

The primary objective of an activation plan is to define initial response actions that ensure the response begins as quickly and effectively as possible. Most emergency response plans will be activated by an initial alarm raised by the person discovering the incident.

Activation plans must be based on the risks identified by your company and the response organizational structure implemented within your company. Risks are discussed in Element 3.4 Assessing Risk on page 14, and response organizations are discussed in Element 3.5 Establishing a Response Organization on page 29.

Key components of developing activation plans include:

- Defining Initial Actions

- Understanding Emergency Levels

4.2.2 Defining Initial Actions

Essential Actions

- Determine how a facility may become aware of an incident, such as by:
  - alarm systems
  - calls from the neighboring residents or other members of the community
  - calls from personnel on or near the site
  - visual identification of unusual conditions
- Identify possible recipients of initial incident reports.

  Tip: *It is possible that anyone at the facility might be the first to become aware of an incident so everyone must be prepared to initiate the emergency response plan.*
- Develop procedures for:
  - handling initial emergency calls
  - verifying the incident and its level

  See also: *4.2.3 Understanding Emergency Levels on page 54.*
  - contacting appropriate individuals and teams to initiate response actions

  See also: *3.5 Establishing a Response Organization on page 29.*
  - calling for help from external emergency response services
  - documenting appropriate information about the incident

  See also*: Figure 10: Sample Initial Incident Report Form on page 52.*
  - submitting completed initial incident reports to appropriate personnel

Figure 10: Sample Initial Incident Report Form

SAMPLE INCIDENT REPORT

Date of Incident: _____ Time: _____ ☐ Actual ☐ Near Miss
Year Month Day *2400 clock*

Incident Location _____ Area _____

Phase of Operation ☐ Normal ☐ Shutdown Employee/ Contractor _____

Visibility Condition ☐ Clear ☐ Fog ☐ Rain ☐ Snow ☐ Bright ☐ Dim ☐ Dark
Road/Surface Conditions ☐ Dry ☐ Wet ☐ Slippery

INCIDENT TYPE *(check)*	**INCIDENT CHARACTER** *(check)*			
☐ Injury	☐ Struck By or Against	☐ Caught on or Between	☐ Exposure	☐ Slip
	☐ Trip	☐ Fall	☐ Contact With	☐ Over Exertion
	☐ Foreign Body	☐ Other		
☐ Occupational Illness				
☐ Safety	☐ Arson	☐ Theft	☐ Vandalism	☐ Lost
	☐ Other			
☐ Environmental	☐ Spills	☐ Flaring	☐ Emission	☐ Pollution
	☐ Land Disturbances	☐ Leak	☐ Other	
☐ Damage	☐ Malfunction	☐ Fire	☐ Explosion	☐ Procedural
	☐ Struck by or Against	☐ Leak	☐ Other	
☐ Production	☐ Product Loss	☐ Spills	☐ Flaring	☐ Interruption
	☐ Other			

Incident Description (Include who, what, where, how, part, components, unit)

_____

_____

_____

_____

Equipment No.: _____ Vehicle No.: _____

Name of Injured: _____ _____ _____ _____
Surname *Given Name* *Initial* *Employee No.*

Employees Involved: _____

_____
Name(s) and Employee No.(s)

Contractors Involved: _____
Company Name and Employee Name(s) and No.(s)

Reported By: _____ Date Reported: _____
Year Month Day

To be completed by Supervisor:

Figure 10: Sample Incident Report - Page 2

SEVERITY

Actual Severity

☐ Minor ☐ Serious ☐ Major ☐ Catastrophic

Potential Severity

☐ Minor ☐ Serious ☐ Major ☐ Catastrophic

Frequency

☐ Rare ☐ Occasional ☐ Frequent

Formal Investigation

☐ Yes ☐ No

Potential For Recurrence

☐ Low ☐ Medium ☐ High

***For Injuries/Illness Only Classification*:** ☐ First Aid ☐ Medical Aid ☐ Medical Treatment

Body Parts Injured - (circle one ore more of the following parts listed)

☐01	Eyes	☐02	Head (includes face, neck)	☐03	Fingers (includes thumb)	☐04	Hands (includes wrist)
☐05	Arms (includes elbow)	☐06	Back	☐07	Knees	☐08	Legs
☐09	Trunk (includes chest, hips, shoulders)	☐10	Feet (includes toes, ankles)	☐11	Internal	☐99	Other

Nature of Injury – (circle one or more)

☐01	Cut	☐02	Fracture	☐03	Allergy	☐04	Sprain	☐05	Scrape
☐06	Shock	☐07	Welder's Flash	☐08	Bruise	☐09	Crush	☐10	Foreign Body
☐11	Burn	☐12	Exposure	☐13	Puncture	☐14	Amputation	☐15	Dermatitis
☐99	Other								

Incident Cost: Estimated cost of repair or replacement: _____

Causes: (Immediate and Basic) _____

SPECIFIC ACTIONS TO BE CARRIED OUT

ACTION / WORK TO CONTROL LOSS	BY WHOM	DATE DUE	DATE COMPLETE

Signed _____ _____ Date: _____ _____ _____

Team Leader *Employee No.* *Year* *Month* *Day*

Comments:

_____

_____

_____

_____

_____

Signed Off by: _____ Date: _____ _____ _____

Safety Advisor *Year* *Month* *Day*

_____ Date: _____ _____ _____

Manager / Representative *Year* *Month* *Day*

4.2.3 Understanding Emergency Levels

Essential Actions

- Establish emergency levels that are appropriate to your company's facilities, areas of operations and regulatory requirements.

  See also: *Table 3: Emergency Levels on page 55.*
- Define emergency levels according to their potential to cause damage within and beyond company boundaries.
- Incorporate emergency levels into initial activation procedures to ensure adequate measures are instigated at the right times.

  See also: *4.4 Developing Risk- and Site-Specific Response Strategies on page 56.*
- Include emergency levels in training programs for response teams and others workers at your company facilities.

  See also: *5.3 Training Response Teams on page 66.*

4.2.4 Background

Emergency Levels

The purpose of classifying incidents into level designations is to provide clarity and enable companies to quickly and clearly communicate the severity of the incident.

The most common approach to incident classification is to use three levels to establish the complexity, nature, risks and extent of the incident as well as the level of response organization and types of strategies required. These three levels are briefly defined as:

- Level one – least serious, precautionary - LOW
- Level two – confirmed incident, outside support required, threat to life - MODERATE
- Level three – most serious, major impact, great deal of support required - HIGH

Color designations can also be associated with these levels.

- Level one – **GREEN**
- Level two – **YELLOW**
- Level three – **RED**

Emergency levels indicate the potential an incident has for causing injury or damages on company sites and beyond the boundaries of company sites. For response teams, emergency levels help define the magnitude of response required. Emergency levels also provide the basis for a tiered response to any type of incident.

Descriptions and examples of emergency levels common to oil and gas operations are provided in Table 3: Emergency Levels on page 55.

Table 3: Emergency Levels

Criteria	Description	Summary	Examples
Level 1: Low (Green)	Level 1 Incidents are the least serious and are typically handled entirely by local facility staff and contractor support.	Meets ALL of the following Criteria: • Hazard can be controlled immediately. • Public safety not threatened. • Environmental impacts negligible – confined to company property or lease. • Company reputation not impacted. • Little or no interest by local media.	• System alarm or notification of a problem sufficient to cause concern and dispatch personnel to investigate • Any situation that affects well control and has the potential to escalate in severity. • Minor injury of company or contract personnel. • Minor damage of company property. • Trespassers on company property. • Spot fire that can quickly be controlled. • Community concern, complaint or observation of an incident. • Preliminary weather reports that indicate potentially threatening conditions are developing.
Level 2: Medium (Yellow)	Level 2 Incidents are more serious and result in or have the potential to result in: • detrimental health effects; or injury or death of workers, responders or the public • damage to the environment • damage to company, private or community property • damage to the company's reputation or shareholder value	Meets ANY of the following Criteria: • Definite risk to life. • Imminent control of the hazard probable. • Public safety threatened. • Environmental impacts moderate – that extend or may extend off company property. • Local reputation of company impacted. • Local and regional media interest. • Use of external resources for assistance.	• Verified alarm or credible notification of any situation that has a definite risk to life. • Public evacuation or sheltering. • Oil or salt water spill that extends beyond company property or lease. • Any situation that has the potential for loss of well control or failure of essential well-control equipment. • Threatening telephone call. • Serious injury of company or contract personnel. • Any incidents involving the public. • Fire, explosion, release with threat to life, where imminent control of the hazard is probable. • Overdue aircraft that air-traffic control cannot contact. • Severe weather threatens operations and personnel.
Level 3: High (Red)	Level 3 Incidents are the most serious and result in or have the potential to result in: • serious health effects; multiple injuries or death of workers, responders or public • major environmental impact • extensive damage to company, private or public property • potential to significantly damage the company's reputation or shareholder value	Meets ANY of the following Criteria: • Operational control lost, uncontrolled hazard • Public safety jeopardized • Environmental impacts significant and ongoing • Corporate reputation impacted • Regional, state, national media interest • Governmental involvement immediate and extensive • Great deal of assistance needed from outside parties	• Fatality or life threatening injury to an employee, contractor or the public • Monitored hydrogen sulphide levels reach ignition criteria • Explosion with extensive damage to community facilities • Major spill extending beyond company property • Act of terrorism such as bombing of a company facility • Loss or crash of company aircraft • Unexplained disappearance of key company personnel

4.3 Defining Notification and Mobilization

4.3.1 Objective and Scope

The primary objective of notification and mobilization is to ensure emergency resources are contacted and put into service as quickly as possible during an emergency. Certain government agencies must also be notified as part of regulatory compliance.

Notification and mobilization activities need to be documented in concise procedures for notifying and mobilizing key company personnel, mutual aid partners, third parties and equipment.

The key component of this element is described below.

4.3.2 Developing Notification and Mobilization Procedures

Essential Actions

- Develop procedures that clearly describe:
  - who must be contacted, when and how (both internal and external)
  - who should be making those contacts
  - what forms are available to assist with initial notification
  - how personnel and other resources are to be assembled in an orderly, coordinated manner (e.g., transportation)

  Tip: *Often these procedures are tied to the emergency levels in a tiered approach that shows how notifications change as the level increases. For example, the lower the incident level, the fewer people who have to be notified.*
- Designate a person or position responsible for mobilizing people, equipment and materials from within the organization.
- Assign specific personnel to organize resources according to need and resource constraints (e.g., size, storage requirements, cost).
- Provide guidance for requesting and obtaining mutual aid and resources outside the organization.

  See also: *3.7 Developing Mutual Aid Agreements on page 41.*
- Define logistics for moving resources to emergency sites and equipment staging areas.
- Define authorities for spending (e.g., limits) and procedures for getting expenditures approved.
- Ensure funding for emergency resources is available and adequate for emergency response.
- Assign the monitoring of resource expenditures to specific personnel (e.g., Finance and Administration Chief).

4.4 Developing Risk- and Site-Specific Response Strategies

4.4.1 Objectives and Scope

The primary objective of risk- and site-specific emergency response strategies is to ensure response actions are appropriate to the risk and the sites for which they are implemented.

Risk- and site-specific strategies are key elements of Incident Action Plans discussed on page 31 and rely on risk assessments as well as response organizations and incident levels to be effective. Risks are discussed in 3.4 Assessing Risk on page 14, response organizations are discussed in 3.5 Establishing a Response Organization on page 29, and incident levels are described in

4.2.3 Understanding Emergency Levels on page 54.

Key components of this element include:

- Developing Risk-specific Strategies
- Developing Site-specific Strategies

4.4.2 Developing Risk-specific Response Strategies

Essential Actions

- Review risk assessments to determine which risks require specific response strategies.
- Consider risks created as a result of the response effort (e.g., contaminated fire water, risk to responders in a hazardous chemical environment, exposure to responders) and where appropriate, refer to existing corporate environment, health and safety plans or procedures that address these risks and mitigation measures.
- Develop detailed procedures for each of the risks that describes:
  - the type of incident and its hazards
  - roles and responsibilities of the individuals and agencies that will participate in response
  - regulated notification requirements
  - equipment and training necessary to effectively respond to the incident
  - contacts for support and additional materials
  - government and other emergency contacts

  See also:

  Figure 11: Sample Risk-specific Response Strategy on page 58.
- Appoint an individual or team to be responsible for documenting and maintaining written procedures.
- Ensure an Incident Commander or equivalent is assigned responsibility for approving procedures.
- Distribute finished procedures to field and office personnel as appropriate as well as regulators and other government agencies as necessary.
- Keep records of every distributed copy so you know where to send updates.
- Maintain the procedures on a regular schedule (e.g., yearly).

4.4.3 Developing Site-specific Response Strategies

Essential Actions

- Compile into site-specific strategies the following information:
  - Description of the local ICS team members and how they interact with the corporate members and other contacts.

  See also: *3.5 Establishing a Response Organization on page 29.*
  - Inventories of local emergency resources and contacts.

  See also: *3.6 Identifying Emergency Resources on page 38.*
  - Details of mutual aid agreements for the site.

  See also: *3.7 Developing Mutual Aid Agreements on page 41.*
  - Descriptions of emergency communication systems at the site.

  See also: *3.8 Establishing Emergency Communication Systems on page 45.*
  - Communication procedures specific to the site.

  See also: *3.9 Defining How to Communicate with the Public on page 46.*
  - Risk-specific response plans for the risks at the site.

  See also: *4.4.2 Developing Risk-specific Response Strategies on page 57.*

- Procedures for reporting incidents at the site.

See also: *4.5 Defining Reporting Processes on page 59.*

Figure 11: Sample Risk-specific Response Strategy

Suspicious Package

Isolate the Area and Package

- Do not touch the package.
- If you accidentally picked up the package, gently place it on the nearest flat, stable surface (e.g., a desk top or the floor).
- Evacuate the area.
- Prevent others from approaching or handling the package or from coming into contact with any substances that might have spilled from the package.
- If possible and safe to do so, post personnel near entrances to the area to ensure no one re-enters before emergency services (e.g., police) arrive.
- If it is safe to do so, secure the area directly surrounding the package to:
  - Remove hazards (e.g., lit cigarettes, hot lamps, power cords).
  - Prevent any spills from further movement (e.g., close open windows and vents that might cause powdery substances to become airborne).
- Do not try to clean it up.
- Put on respiratory protective equipment if you have any available.
- Use clothing, paper, a trashcan or other material to cover the spill.
- Apply the cover gently so as not to further disturb the spilled material (e.g., cause powdery substances to become airborne).

Stop Potential Contamination

- Remove any clothing and other items that may have come into contact with the package or any substance that spilled from it.
- Place all contaminated items inside plastic bags (e.g., including clothing, desk pads, keyboards, pens, papers) and seal the bags tightly.
- Do not discard the bags – keep them so the contents can be analyzed.
- Wash your hands and face with anti-bacterial soap immediately (or any soap if you don't have antibacterial soap).
- If it is possible to shower completely at the site, then do so.

Call for Help

- Phone local Emergency Contacts (e.g., police).
- Provide as much information as possible about the location and type of suspicious package.
- Indicate where you will be and how Emergency Services can contact you when they reach the area.
- Notify Maintenance to turn off circulating fans, air conditioning and heaters.
- Notify Building Security of the situation.

Document the Event

- Make a list of all the people who were in the area when the suspicious package arrived.
- Provide this list to emergency services when they arrive.
- Record the details of the package and why you are suspicious of it, such as:
  - strange odor
  - lop-sided packaging or protruding item(s)
  - stains on wrapping
  - unusual contents (e.g., powdery, rigid or bulky contents)
  - post-marking from a foreign country

- post mark office that is different from return address
- excessive postage
- misspelled words
- addressed to a position title only (e.g., Manager) without the individual's name
- addressed to an employee who is no longer with Company
- wrong title with name
- badly typed or hand-written address
- no return address
- restrictive markings such as "To be opened by…Confidential, Urgent or Personal."

- Record actions taken in response to discovery of the package.

4.5 Defining Reporting Processes

4.5.1 Objective and Scope

The primary objective of reporting processes is to ensure all internal as well as regulatory requirements for reporting incidents are met.

The key component of this element is described below.

4.5.2 Developing Reporting Procedures

Essential Actions

- Document procedures for notification and reporting to include:
  - who is responsible for notification and reporting
  - to whom notifications and reports are to be made:
    - internally (e.g., management)
    - externally (e.g., police, fire, regulatory agencies, other public authorities)
  - when notifications and reports are to be made (e.g., immediately, within 24 hours)
  - how the notifications and reports are made (e.g., written, oral)
  - where and for how long copies of reports are to be maintained
- Develop templates or provide copies of existing internal report forms as part of procedures.
- Establish a process for managing internal forms.
- Include in internal procedures copies of government report forms as well as names of contacts for assistance in completing the forms and requesting additional copies of forms.

4.6 Establishing Incident Command Posts

4.6.1 Objective and Scope

The primary objective of Incident Command Posts is to provide centralized response coordination and management during an emergency. These posts should be located in highly visible areas that are easily accessed. They should act as hubs for information collection and dissemination, task assignment and response coordination and monitoring.

Key components of this element include:

- Establishing an On-site Command Post
- Establishing an Incident Command Post

4.6.2 Establishing an On-site Command Post

Essential Actions

- Establish an On-site Command Post to coordinate and direct all response and mitigation efforts inside the perimeter of the incident site and to carry out the objectives set by the individual in charge (e.g., the Incident Commander).

  Tip: *A On-site Command Post can be established in many types of structures including existing buildings, self-contained mobile facilities, trailers, skid-mounted buildings, modular kits or tents.*
- Select personnel to work in the Incident Command Post from your response organization.

  See also: *3.5 Establishing a Response Organization on page 29.*
- Ensure the On-site Command Post contains the equipment, materials and resources to support the functions of your response plan and organization, including:
  - power supply (e.g., power generator)
  - furnishings (e.g., desks, map storage, meeting tables, chairs, fire extinguishers ad other safety equipment, kitchen, exterior and interior lighting, sleeping facilities)
  - communications and computing equipment (e.g., conventional, mobile, cellular or satellite phones; fax machines; public address system; mobile radios; television)

4.6.3 Establishing an Incident Command Post

Essential Actions

- Establish an Incident Command Post to manage all issues related to the emergency that can be addressed outside the perimeter established by the Incident Commander and to provide support to the On-site Command Post as requested.
- Select personnel to work in the Incident Command Post from your response organization.

  See also: *3.5 Establishing a Response Organization on page 29.*
- Assign the following roles to the personnel within the Incident Command Post:
  - supporting the ICS team in making key decisions
  - providing technical information as required
  - facilitating mobilization of emergency resources
  - monitoring the response
  - liaising with authorities and other organizations as required by the ICS team
  - gathering information and keeping records (e.g., logs and financial records) in relation to the emergency

4.6.4 Background

The On-site Command Post is best located in a safe, secure area near the incident scene and is the base for control operations. There can be only one Incident On-site Command Post to provide a safe, central location to manage the emergency. Appropriate government agencies and other resources may also work from the On-site Command Post. It can be activated by anyone who takes command and control of the emergency scene (e.g., Incident Commander).

The Incident Command Post normally provides support to the On-site Command Post. The Incident Command Post is usually located at the company's head office or a local field plant.

4.7 Providing Security

4.7.1 Objective and Scope

The primary objective in providing security at emergency sites is to ensure protection of the public and to prevent unauthorized access. Response plans should identify the needs for security and provide the procedures and responsibilities of security during an incident.

The key component of this element is described below.

4.7.2 Establishing Security Procedures

Essential Actions

- Appoint security personnel and alternatives.
- Define their roles in securing emergency sites.
- Prepare written procedures for providing security during incidents that include steps for:
  - identifying personnel with emergency responsibilities
  - preventing or minimizing personal injury by maintaining a security perimeter
  - preventing unauthorized access
  - preserving evidence for investigation
  - restoring the mode of operations as quickly as possible
- Train personnel as necessary.
- Add security personnel to key contact lists within site-specific response strategies.

4.7.3 Background

In most emergencies, security personnel are assigned to preserve evidence for investigation and follow-up, and prevent unauthorized access to the scene. Although local police forces often assist in emergencies, never assume they will always be available. In cases of widespread disaster, they may not be able to respond due to conditions or other demands for their services. Train personnel to handle security needs or to plan for outside resources to handle these duties.

4.8 Establishing a Process for Damage and Claims Assessment

4.8.1 Objective and Scope

The primary objective of damage and claims assessment is to ensure your company is adequately protected from the liabilities resulting from incidents.

Claims may include losses incurred:

- due to response costs
- resulting from business interruption
- through damaged or destroyed property or equipment
- by impacted community (e.g., evacuation costs, out-of-pocket costs, etc)

The key component of this element is described below.

4.8.2 Developing Damage Claims and Assessment Procedures

Essential Actions

- Identify individuals capable of assessing damages accurately and assign responsibility for this task.
- Prepare procedures and forms for assessing damages and preparing claims that address:
  - documentation of all losses prior to any claim submissions
  - assessment of losses requiring immediate attention and repairs
  - investigations by government departments

  Tip: *Significant emergencies may be investigated by government departments and will require an industry liaison to assist with their investigation.*

  - damages to:
    - contractors' equipment
    - community residential and commercial property
    - livestock
    - surface water and groundwater
  - claims of nuisance or inconvenience imposed on the community as a result of the emergency

4.8.3 Background

In the event of an emergency, damage may cover a broad field and may require some expertise in damage assessment above and beyond the capabilities of a company or corporation. Resources for damage assessment should be investigated and selected as part of the emergency response program development.

Emergency response programs should identify how claims will be assessed and addressed. This assessment may involve insurance claims adjusters or specialists.

Damage assessment after an emergency is essential for a facility of any size. Your company may or may not be liable for damage caused by its operations, whether or not specific negligence can be proven. If your company depends on outside insurance, the premium will be reflected by your company's operations and loss claims record.

4.9 Providing Critical Incident Stress Management

4.9.1 Objective and Scope

The primary objective of critical incident stress management is to assist responders in dealing effectively with the stress they may encounter through the course of responding to an emergency. Critical incident stress management programs provide appropriate stress management interventions by qualified personnel to help reduce or eliminate negative impacts to a responder's personal and professional life.

The key component of this element is described below.

4.9.2 Establishing Critical Incident Stress Management Programs

Essential Actions

- Develop programs to provide critical incident stress management that will:
  - facilitate the expression of feelings and thoughts
  - offer education on stress management and post-traumatic stress syndromes
  - facilitate fitness-to-work assessments
  - return the responder to his or her working pattern as soon as possible
  - develop a follow-up and plan where necessary for individual and group consultation
  - restore group cohesiveness
- Look for assistance from qualified mental health professionals in developing these programs.

4.9.3 Background

Emergency response personnel can be placed under enormous stress during critical incidents. The effect of this stress may manifest itself immediately or it can be delayed. When this happens, the emotions and the functional capability of the person may be negatively impacted. Physical and psychological symptoms may appear and normal life may be disrupted until the problem is recognized and resolved.

Critical Incident Stress Management Teams offer a partnership between mental health professionals and emergency or other high-risk workers who are interested in preventing and mitigating the negative impact of acute stress. They are also interested in accelerating the recovery process once an emergency responder or team has been seriously stressed or traumatized.

Critical Incident Stress Debriefing programs (CISD) are structured group meetings between the people directly involved in an emergency and the CISD professional within 24 to 72 hours after the incident. These meetings are confidential and serve to mitigate stress impacts through open, non-judgemental discussions of feelings as well as education on stress management.

A well-planned and timely CISD can accelerate the recovery process in people suffering normal affects in response to an abnormal situation.

5.0 Implementation and Continuous Improvement

Overview

The success of emergency management programs depends greatly on how well they are implemented and maintained. As new programs and components are developed, it is essential to ensure they are integrated into the overall management of company operations. It is also important to constantly re-evaluate response programs to ensure they are current, relevant and effective.

Scope

This *Guideline for Developing Emergency Response Programs* provides guidance and resources for the following elements of implementation and continuous improvement:

- Obtaining Approval of the Emergency Response Program
- Distributing Emergency Response Plans
- Training Response Teams
- Inspecting and Maintaining Emergency Resources
- Conducting Emergency Exercises
- Consulting with Stakeholders
- Updating Program Components
- Auditing the Emergency Response Program

5.1 Obtaining Approval of the Emergency Response Program

5.1.1 Objective and Scope

The primary objective in having the emergency response program and its components approved by line management is to ensure management understands and is committed to the program. While the individuals and teams that developed the program may be committed to implementing it, they will not get very far if line management isn't aware of their work or hasn't set aside appropriate resources for implementation and continuous improvement. An important part of obtaining management and facility level support for emergency planning is to ensure management is aware of and understands the business benefits discussed in the 1.3 Business Sustainability on page 2.

Key components of this element are:

- Identifying Who Will Be Part of the Approval Process
- Implementing an Approval Process

5.1.2 Identifying Who Will Be Part of the Approval Process

Essential Actions

- Establish an approval process that will ensure management support of your organization's emergency response activities and plans.
- Determine who should be involved in the approval process including:
  - line management
  - managers of operations and facilities affected by the program
  - government agencies
  - mutual aid partners
  - third parties that will participate in the response (e.g., police, fire)

  Tip: *The Planning Committee is typically responsible for identifying who should approve the plan and how approval should be obtained and documented.*

  See also:

  3.2 Appointing a Planning Coordinator and Establishing a Planning Committee on page 11.
- Contact these groups during the development of emergency response programs to ensure they are aware their approval and support will be requested.

5.1.3 Implementing an Approval Process

Essential Actions

- Ensure emergency response program components comply with the company emergency policy, industrial emergency planning standards, and industrial codes of practice, before seeking formal plan approval.
- Ensure company, municipal, and other emergency response plans are compatible and complementary, and include the parties responsible for those plans in the approval process.
- Develop and use a checklist or other tool for documenting the company policies, industry standards, third party plans, codes of practice and regulations against which your program has been compared.
- Record and follow up results from the comparison before pursuing approvals.
- Develop an approval form or other means of documenting approvals and comments that result from the approval process.
- Request approval from the appointed line manager and other parties as necessary.
- Establish a means for following up all comments received during the approval process.

5.1.4 Background

Management responsible for facilities or operations should approve emergency response programs relevant to their areas. Their approval should be sought when programs are first developed and when significant changes are made.

The emergency response plans for all organizations that may interact during an emergency should be compatible and complementary to one another, and the parties responsible for those plans should be part of the approval process. Where emergency response plans must comply with regulatory requirements, they may also have to be submitted to relevant government agencies for formal review and approval.

5.2 Distributing Emergency Response Plans

5.2.1 Objective and Scope

The primary objective in distributing emergency response plans is to ensure the individuals who need them have access to them. Emergency response plans and other program components must be accessible to all employees, departments or agencies having responsibilities for emergency response.

The key component of this element is described below.

5.2.2 Establishing a Distribution Process

Essential Actions

- Retain at least one controlled copy of the plan as the master.
- Ensure electronic files for the master copy are only accessible to individuals with the authority to make changes to the plan.
- If possible, make the plan accessible on the company intranet site.
- Prepare and number copies of the plan.
- Prepare a distribution list that includes:
  - the Planning Coordinator
  - members of the Planning Committee
  - members of ICS teams
  - key employees and internal departments involved in emergency response
  - key representatives of senior management
  - external agencies such as fire and spill response agencies
  - government agencies
  - mutual aid partners
  - contractors
- Assign copy numbers to everyone on the list.
- Maintain a record of the distribution and update it as the plans and the people change.
- Distribute the original document and amendments as soon as possible after preparation.

5.2.3 Background

All personnel and third parties involved in emergency response should be in possession of a current version of the emergency response plan. Distribution is an important part of communicating and managing an emergency response plan. A formal process for maintaining up-to-date lists and distributing updates in a timely manner is essential to ensure everyone follows the same directions during an incident. Some government agencies may require full copies while others may only want contact lists and facility notification phone numbers.

5.3 Training Response Teams

5.3.1 Objective and Scope

The primary objective of emergency response training is to ensure teams have the skills and the confidence to perform effectively during an emergency. It is essential to provide training to everyone with a role in emergency response. The amount and frequency of training depends on the type and size of your operation.

The key component of this element is described below.

5.3.2 Developing Training Programs

Essential Actions

- Ensure employees are thoroughly familiar with company policy and procedures for responding to emergencies.
- Provide training for all emergency response roles through recognized industry training programs in areas such as:
  - fire fighting
  - oil spill response
  - hydrogen sulfide response
  - hazardous chemical response
  - Incident Command System
- Reinforce emergency training through on-the-job training and discussions at regular safety meetings
- Maintain detailed records of all training provided.
- Schedule regular refresher training for emergency response personnel.

5.3.3 Background

An emergency can create an unfamiliar atmosphere that can be disorienting to personnel that are not completely familiar emergency response procedures. The more familiar personnel are with the facility, procedures and use of emergency equipment, the more effective and efficient the emergency response will be. Familiarity will also reduce the amount of stress and anxiety personnel experience and reduce the amount of secondary incidents (caused by panic or failure to follow emergency instruction) that may be encountered during an emergency.

The amount and the frequency of training will vary depending on the:

- procedures
- roles and responsibilities
- equipment
- hazards and risks
- regulatory requirements
- lessons learned from previous response activities (real and simulated)

5.4 Inspecting and Maintaining Emergency Resources

5.4.1 Objective and Scope

The primary objective of regular inspections and maintenance of emergency response equipment is to ensure the equipment is available and in good working order in the event of an emergency. Emergency response equipment, whether owned, contracted or leased, must be regularly inspected and maintained in a state of readiness.

The key component of this element is described below.

5.4.2 Establishing Inspection and Maintenance Programs

Essential Actions

- Determine for each site or facility which equipment will be inspected and maintained as part of the emergency response program.

  See also: *3.6 Identifying Emergency Resources on page 38.*
- Check the manufacturer's recommendations for inspection frequency and type.
- Establish a schedule for inspections that is consistent with manufacturer recommendations and fits within other site and facility management activities.
- Develop inspection forms to ensure consistency in how inspections are conducted and the results are documented.
- Develop maintenance schedules and programs in compliance with manufacturer recommendations and any unique conditions of the site (e.g., high humidity may require increased corrosion protection of some equipment).
- Develop forms for documenting all maintenance activities and results.
- Develop a procedure for distributing and filing inspection and maintenance documents.
- Ensure third-party suppliers (e.g., mutual aid partners, emergency services) meet the same inspection and maintenance standards set for your company-owned equipment.
- Monitor inspection and maintenance programs to ensure they are being implemented.

5.5 Conducting Emergency Exercises

5.5.1 Objective and Scope

The primary objective in conducting emergency exercises is to determine how well emergency response plans and responders work together to manage an incident. Results from exercises are very useful in identifying gaps and problem areas that need improvement.

The key component of this element is described below.

5.5.2 Planning Emergency Exercises

Essential Actions

- Set an annual schedule for testing plans.
- Test the plan by conducting emergency exercises such as:
  - orientation seminars
  - drills
  - tabletop exercises
  - functional exercises
  - full-scale exercises

  See also: *Background below for descriptions of each type of exercise.*
- Discuss the results of the exercises and drills and document the feedback.
- Use the feedback to improve the plan.

5.5.3 Background

An exercise is an organized activity that requires people to take action, to solve problems or to make decisions in a team structure as if they were responding to an actual emergency.

Exercises are designed to promote emergency preparedness; test or evaluate emergency operations, policies, plans, procedures or facilities, train personnel in emergency duties, and demonstrate operational capabilities. Essential elements, inter-related elements or the entire emergency response program should be exercised at least annually to ensure that it is current, comprehensive and effective. This may be accomplished by one or more of the exercises described below.

Your company is responsible for setting standards to test your emergency response plans. Testing should reflect regulatory and company requirements. The Planning Coordinator is usually responsible for ensuring the emergency response plans are tested to keep them current, comprehensive and effective.

Orientation Seminar

An orientation seminar is an informal discussion designed to familiarize participants with roles, plans, and procedures, and answer questions of coordination and assignment of responsibilities. It is usually undertaken during the rollout or introduction of an emergency response plan or updates.

Drills

A drill is a supervised activity that tests, develops, or maintains skills in a single response procedure (e.g., communications, notification, lockdown, fire) and the possible or probable interaction with local government agency functions (e.g., incident command posts, rescue squad entry, hazard perimeter control), which will involve actual field response. Drills help to prepare for more complex exercises in which several functions are coordinated and tested.

Tabletop Exercises

A tabletop exercise is an activity in which personnel and individuals with emergency responsibilities are gathered together to discuss planned responses to various simulated emergency situations. Using existing plans, the exercise is designed to elicit constructive discussion by the participants as they examine and attempt to resolve response problems. The purpose is for participants to evaluate plans and to resolve questions of coordination and assignment of responsibilities throughout the exercise.

Tabletop exercises are used to provide an opportunity for participants to practice and discuss emergency response issues. This type of exercise is best suited to meet objectives such as:

- familiarize personnel with a new or revised emergency response plan
- familiarize personnel with assigned roles and responsibilities under the plan
- maintain an awareness of the plan requirements
- increase confidence in the plan and its application in emergency situations
- develop working relationships with other emergency response organizations
- identify changes which are required to the emergency response plan

A tabletop exercise is conducted over a two- to three-hour timeline. It involves an open forum discussion on the scenario presented. A facilitator who is familiar with the plan and the operations involved guides the discussion. It is the least complex exercise to plan and conduct.

Functional Exercises

A functional exercise is an activity designed to test or evaluate the operational capability of an individual function or complex activities within a function of emergency response. This is a fully simulated interactive exercise that tests one or more functions in a time-pressured realistic simulation. This type of exercise is applicable where the response activity is capable of being evaluated in isolation from other emergency management activities. A functional exercise fully tests specific functions of the emergency response and preparedness plan. An Incident Command Post or On-site Command Post is activated and used to demonstrate the use of command structure. This type of exercise is best suited with a focus on policies, procedures, roles and responsibilities.

Full Scale Exercises

A full-scale exercise is an activity intended to evaluate the operational capability of the overall emergency management system in an interactive manner. A full-scale exercise involves the testing of a majority of the

functions of the Emergency Response Plan. A full-scale exercise requires actual field play that includes mobilization and actual deployment of emergency personnel and resources required to demonstrate coordination and response capabilities. The full-scale exercise tests total response capability as close to a real emergency as possible. An On-site Command Post or Incident Command Post is activated to coordinate operational field capabilities.

Full-scale exercises are used to test the overall response capability of an organization. It gives the first responders a chance to work together and to practice using ICS. The Incident Command Post is mobilized and communications both internally and externally are tested. In a full simulation, the media relations component is also fully tested.

5.6 Consulting with Stakeholders

5.6.1 Objective and Scope

The primary objective of consulting with stakeholders, as part of continuous improvement, is to ensure everyone who may directly or indirectly affect the outcome of response activities has an opportunity to provide input. Stakeholders such as the communities in which your company operates, regulatory agencies and external response agencies can provide valuable information that might otherwise go unnoticed. In addition, the process of consultation helps to maintain trust among your stakeholders in your company's ability to respond effectively to incidents.

The key component of this element is discussed below.

5.6.2 Consulting with Stakeholders for Continuous Improvement

Essential Actions

- Identify who among your stakeholders should participate in the continuous improvement of your emergency response plans, such as:
  - representatives from the communities in which you operate
  - regulatory agencies
  - external response agencies (e.g., police and fire services, medical facilities, suppliers of equipment and materials)
  - media
- Determine how to best involve stakeholders in the continuous improvement process, such as by participating in:
  - annual reviews of site-specific emergency response plans
  - exercises
  - surveys to verify stakeholder information (e.g., contact information, health risks of individuals who may need to be evacuated during an incident, changes to materials available from suppliers)
- Maintain continuous contact with stakeholders by providing a resource within your organization that can accept feedback and answer questions as needed.
- Document all information collected from stakeholder consultations and ensure it is incorporated into emergency response plan updates.
- Follow up with stakeholders to let them know how their feedback was used in the continuous improvement process.

5.7 Updating Program Components

5.7.1 Objective and Scope

The primary objective of updating emergency response programs is to ensure the programs remain active and maintain a consistent profile within the organization. Emergency response is a process that requires continuous adjustment and amendment because of changes in operations, organizational structure, personnel, regulations and lessons learned from real-life events or exercises.

The key component of this element is described below.

5.7.2 Implementing Regular Updates

Essential Actions

- Establish a regular review period (at least once a year) to perform a risk assessment and ensure the emergency response programs remain current.

  See also: *3.4 Assessing Risk on page 14.*
- Establish a set of key indicators to evaluate the effectiveness of your company's emergency response programs, such as:
  - number of emergency response training sessions conducted within a specified period
  - number of emergency response exercises conducted within a specified period
  - number of senior executives trained in emergency response
  - number of pre-identified people on regional response teams
- Regularly update emergency contact lists and notification lists.
- Notify plan holders immediately of key changes, regardless of the regular review period.

  See also:

  5.2 Distributing Emergency Response Plans on page 66.
- Ask users to provide input on the plan by including a revision request form or contact number in each copy of the plan.
- Use safety or other meetings as an opportunity to encourage comments on ways the program can be improved.
- Number each updated page to correspond with the original pagination.
- Send updates with specific instructions for insertion, e.g., "Replace page 10 with the attached new page."
- Reissue the entire plan periodically to ensure it is complete and up to date.

5.8 Auditing the Emergency Response Program

5.8.1 Objective and Scope

The primary objective in auditing the emergency response program is to periodically determine the program's overall effectiveness and usefulness within the company. Audits also identify gaps and problem areas that can be addressed as continuous improvements. The frequency of audits varies according to organizational policy and regulatory requirements.

Key components of auditing are:

- Managing the Audit Process
- Conducting Effective Audits
- Scoring Audits and Assessing Results

The audits discussed in this section do not specifically include quality audits. For information on quality audits, refer to international guidelines such as *ISO 19011:2002, Guidelines for Quality and/or Environmental Management Systems Auditing.*

5.8.2 Managing the Audit Process

Essential Actions

- Choose an auditor.

  Tip: *The audit may be performed by staff, external third-party auditors or a regulatory authority.*
- Plan the audit to ensure the company's state of emergency preparedness will be audited against defined criteria (e.g., legislative requirements, organizational policy, emergency planning standards, codes of practice).
- Gather all written materials that are part of the emergency response program including:
  - emergency manuals, policies and procedures
  - job descriptions or lists of emergency responsibilities
  - hazard and incident report forms
  - risk assessments
  - risk-specific and site-specific strategies and any other related work procedures
  - training and maintenance records related to personal protective equipment
  - checklist and records of emergency orientations, on-the-job training, investigations, inspections, maintenance, previous audits and performance assessments
  - emergency response procedures
  - relevant legislation
- Inform other employees that an audit is to take place and how they will participate (*e.g.*, through interviews).
- Conduct the audit.

  See also: *5.8.3 Conducting Effective Audits on page 72.*
- Ensure gaps or deficiencies identified in the audit are:
  - documented
  - reviewed with management
  - corrected
- Analyze audit results and prepare recommendations for follow-up.

  See also: *5.8.4 Scoring Audits and Assessing Results on page 73.*
- Report audit results and recommendations to the Emergency Coordinator and file copies of the audit at head office.

5.8.3 Conducting Effective Audits

Essential Actions

- Assure individuals being interviewed that their comments are confidential so that they will provide accurate and true information.

  Tip: *It's important to protect the rights of individuals to express their opinions freely without experiencing negative consequences. Do not include names or sources on the audit form. If you want to keep track of sources for future reference, ask the individuals you've interviewed permission to keep such records confidential and separate from the audit form.*
- In addition to scheduled audits, conduct audits whenever there is:
  - significant change in business operations
  - high staff turnover or increases
  - significant increase in the number and degree of work hazards
  - a previous audit that shows poor results

- an increase in incident frequency
- Mark questions as not applicable only if the company does not legitimately need to fulfill the requirement cited in the question.

5.8.4 Scoring Audits and Assessing Results

Essential Actions

- Give full marks for questions that can be answered with a yes.
- Give no marks for questions that are answered with a no.
- Give partial marks only where auditor judgment in scoring is indicated.
- If questions are not applicable to a particular audit, mark them with as not applicable (NA).
  Tip: *On the Audit Form, clearly indicate why the question is not applicable.*
- Deduct from the total score the highest possible marks for any questions marked NA.
- Total all marks and compare them to the total possible.
- Define a range of acceptable and unacceptable marks.
- Develop recommendations for improving areas of the program that received low marks

5.8.5 Background

It is recommended that key elements of emergency response programs be assessed annually. Unless otherwise specified, comprehensive emergency preparedness audits should be performed at least every five years.

Auditing an emergency response plan requires a formal approach to determine its adequacy and completeness. It may consist of an internal review by the emergency response team or an external review by peers and community members.

Regulators may also audit emergency response programs. In a formal audit, regulatory officials will look for concrete evidence that specific planning elements have been adequately addressed. As an auditor may require physical verification, those elements that support the written plan should be carefully documented (e.g., risk assessment records of response equipment maintenance and repair work, or training records).

6.0 Bibliography

6.1 Resources Used in Development of this Guideline

This section identifies the sources of information that were used to construct this Guideline as follows:

- Online Resources (e.g., websites and databases)
- Additional Industry Documents
- Existing ARPEL Guidelines

The documents and sources identified below were reviewed by the authors for information related to this Guideline. In most cases, the information obtained from these sources was generally supportive of concepts already developed by the authors in previous work and modified for this Guideline. Readers are encouraged to review the sources listed below for additional and in some cases more detailed or specific information related to emergency response planning.

6.2 Online Resources

The web addresses provided below were active during initial research. Some may have changed.

- *A Comprehensive Glossary of Weather Terms for Storm Spotters – NOAA Technical Memorandum,* Michael Branick, National Weather Service, *NWS SR-145,* nd, <http://www.srh.noaa.gov/oun/severewx/branick2.html#Glossary>.
- *API Risk-Based Software,* American Petroleum Institute, nd, <http://api-ep.api.org/committees/index.cfm?objectid=9B9B7D73-4B00-42D8-B624E06440AB29AE&method=display_body&er=1&bitmask=002009000000000000>.
- *B.C. Provincial Emergency Program, An Introduction to the Incident Command System*, < http://wlapwww.gov.bc.ca/eeeb/ENVSITRPT1/icsintro/icsintr.htm>
- *Beyond Compliance: Creating a Responsible Regulatory Environment that Promotes Excellence, Innovation and Efficiency*, Office of Pipeline Safety, American Petroleum Institute, Interstate National Gas Association of America, May 1999, http://www.aopl.org/pubs/pdf/RiskDemoProgress.pdf>).
- *Catalogue of OGP Publications,* Oil and Gas Producers Association, nd, <http://www.ogp.org.uk/publications/index.html>.
- CDMHA (Center for Disaster Management and Humanitarian Assistance), nd., <http://www.cdmha.org/products.htm>.
- *Chemical Accident Prevention and Risk Management Programs*, United States Environmental Protection Agency, 1 May 2002, <http://www.epa.gov/ceppo/acc-pre.html>.
- *Chemical Accident Prevention: Site Security*, United States Environmental Protection Agency, February 2000, nd, <http://www.npradc.org/pdf/environmental/secale-f.pdf>.
- CIDI (Center for International Disaster Information), and., <http://www.cidi.org/>.
- *Code of Practice for Community Awareness and Emergency Response (CAER), Responsible Care*, Canadian Chemical Producer's Association, nd, <http://www.ccpa.ca/english/position/enviro/index.html>.
- *Contingency Planning for Flood Related Emergencies at Retail and Wholesale Petroleum Facilities*, Canadian Petroleum Products Institutes, 27 August 2001, <http://www.cppi.ca/tech/FloodProcedures.pdf>.
- Crisis Navigator, <http://www.crisisnavigator.de/index2.html>.
- *CSB Chemical Incident Report Center*, nd, < http://www.chemsafety.gov/circ/>.
- *Disaster Preparedness,* Canadian Red Cross, nd, <http://www.redcross.ca/english/disaster/prepare/index.html>.
- *Disaster Response, Dr. Erik Auf der Heide*, http://216.202.128.19/dr/DisasterResponse.nsf/section/07?opendocument&home=html
- *DNV Worldwide Offshore Accident Databank (WOAD)*, nd, < http://www.dnv.com/technologyservices/handbooks/WOAD/woad.asp>

- *Earthquakes in Canada?,* Government of Canada – Safe Guard, nd, <http://www.safeguard.ca/earthquakes/en_can.html>.
- *Electronic Documents*, Regional Disaster Information Center: Latin America and the Caribbean, nd, <http://www.crid.or.cr/crid/Indexen.htm>.
- *Emergency Response Management Consulting (ERMC) Exercise Descriptions,* Partnerships Toward Safety Communities, nd, <http://www.ptsc-program.org/>
- *Emergency Response-Western Canada,* Lori Steine, Gord Tidmarsh, Canadian Association of Petroleum Producers, June 2000, <http://www.capp.ca/default.asp?V_DOC_ID=763&PubID=24958>.
- *EPA Accidental Release Information Program (ARIP)*, nd, < http://yosemite.epa.gov/oswer/CeppoWeb.nsf/content/ds-epds.htm>.
- *Fact Sheet: Hurricanes,* FEMA (Federal Emergency Management Agency), 14 January 1998, <http://www.fema.gov/library/hurricaf.htm>.
- *Fact Sheet: Medical Response to Chemical Warfare and Terrorism,* FEMA (Federal Emergency Management Agency), 13 September 2001, <http://www.fema.gov/emanagers/sasb.htm>.
- *FEMA Emergency Management Institute, IS-195 Basic Incident Command System,* < http://training.fema.gov/EMIWeb/IS/is195.asp>
- *Floods: What to do before and after*, Government of Canada – Safe Guard, 24 May 2001, <http://www.epc-pcc.gc.ca/publicinfo/self_help_ad/self_help/floods.html>.
- *Glossary,* Canadian Association of Petroleum Producers, nd, <http://www.capp.ca/default.asp?V_DOC_ID=733>.
- *Glossary,* Transport Canada, 28 May 2002, <http://www.tc.gc.ca/canutec/erg_gmu/en/Glossary.htm>.
- *Guide for All Hazard Emergency Operations Planning,* FEMA (Federal Emergency Management Agency), 14 May 2001, <http://www.fema.gov/pte/gaheop.htm>.
- *Guidelines for Producing a Community Risk Map,* International Strategy for Disaster Reduction, nd, <http://www.eird.org/ing/varios/folletocomunidades/mapascomunidades.htm>,
- *How to Plan for Workplace Emergencies and Evacuations*, U.S. Department of Labour: Occupational Health and Safety Administration, 2001, <www.osha-slc.ov/SLTC/ emergency response/index.html>.
- *Ility International Incident Database*, nd, < http://www.saunalahti.fi/ility/IncidentHistory.htm>
- *Incident Command System in Oil Spill Response,* Region I Regional Response Team, U.S. Coast Guard, August 1998, <http://www.uscg.mil/d1/staff/m/rrt/ics.html>
- *Introduction to NBC Terrorism: An Awareness Primer and Preparedness Guide for Emergency Responders,* Robert J. Heyer, D.Sc., 15 October 2001, <www.disaster.org>.
- *Mitigating Risk/Threat of Terrorism and Other Risks,* The Disaster Center, 21 January 2002, <http://www.disastercenter.com/terror/0_risk.htm>.
- *Natural Disasters and Sustainable Development: Understanding the links between development, environment and natural disasters – Background Paper No.5,* United Nations Department of Economic and Social Affairs, 8 February 2002, <http://www.unisdr.org/>.
- *Natural Disasters in Latin America and the Caribbean: An Overview of Risk*, Inter-American Development Bank, Céline Charvériat, October 2000, <http://www.iadb.org/RES/pdf/434.pdf>.
- *New York State Incident Command System,* < http://www.nysemo.state.ny.us/training/ics/explain.htm>
- *NFPA Codes and Standards,* NFPA (National Fire Prevention Association), nd, <http://www.nfpa.org/Codes/NFPA_Codes_and_Standards/List_of_NFPA_documents/list_of_folders.asp>.
- *NOAA, Electronic ICS Forms*, http://response.restoration.noaa.gov/oilaids/ICS/intro.html
- *NOAA, Historical Incidents Database*, nd, < http://response.restoration.noaa.gov/oilaids/reports.html>
- *NOAA, Oil Spill Case Histories*, nd, < http://response.restoration.noaa.gov/oilaids/reports.html>
- OECD Chemical Accident Risk Assessment Thesaurus (CARAT), nd, < http://www.oecd.org/document/19/0,2340,en_2649_34369_2371411_119656_1_1_1,00.html>.

- *Offshore Emergency Planning and Response*, Gillian Crowley, Canadian Association of Petroleum Producers, April 2001, <http://www.capp.ca/default.asp?V_DOC_ID=763&PubID=25592>.
- *Oil Spill Removal Organization Classification Program,* United States Coast Guard, 27 April 2001, <www.uscg.mil/>.
- *Oil Spill Response Planning and Implementation*, Allegro Energy Group, January 2000, <http://www.aopl.org/pubs/pdf/Anatomy1.pdf>.
- *OREDA Offshore Reliability Data Project*, nd, < http://www.sintef.no/static/TL/projects/oreda/>.
- *Pollution Prevention and Abatement Handbook,* World Bank Group, July 1998, < http://lnweb18.worldbank.org/essd/essd.nsf/Docs/TOC?OpenDocument>.
- Public entity Risk Institute, nd.,<http://www.riskinstitute.org/ch.asp>.
- *Public Safety and Sour Gas Homepage*, Advisory Committee on Public Safety and Sour Gas, nd, <http://www.publicsafetyandsourgas.org>.
- *Publications: Oil Spill Preparedness and Response,* International Petroleum Industry Environmental Conservation Association, nd, <http://www.ipieca.org/publications/oilspill.html>.
- *Rand-MIPT Terrorism Incident Database.* nd, < http://db.mipt.org/mipt_rand.cfm >.
- *Raising Employee Safety Awareness,* Canadian Association of Petroleum Producers, nd, <http://www.capp.ca/default.asp?V_DOC_ID=785 >.
- *Response Strategies,* International Tanker Owners Pollution Federation Limited, 28 May 2002, <http://www.itopf.com/response.html>.
- *Risk and Reliability*, nd, < http://www.riskandreliability.com/first_main.htm>.
- *Risk World – Risk Databases,* nd, < http://www.riskworld.com/websites/webfiles/ws6aa003.htm>.
- *Severe Storms,* Government of Canada – Safe Guard, *nd*, <http://www.safeguard.ca/Storms/en_storms.html#TORN>.
- *Strategic Plan: A Framework for Action – Summary,* CNC IDNDR (Canadian National Committee for the International Decade of Natural Disaster Reduction), July 1997, <http://www.rsc.ca/idndr/reports/strategy/plan.htm>.
- *Sustainable Development Department Publications Page,* Inter-American Development Bank, 22 May 2002, <http://www.iadb.org/sds/env/publication_2530_e.htm>.
- *The Environmental and Safety Programs for Oil Pipeline Companies: A Prevention Ethic,* Cheryl J Trench, Charlene A Sturbitts, July 1999, http://www.aopl.org/pubs/pdf/programs.pdf>.
- *The Incident Command System and the Concept of Unified Command at a Terrorist Incident,* Lt. John Kane, Sacramento, Calif. Police Department, nd, <http://www.pep.bc.ca/hazard_preparedness/symposium_paper_unified_command.pdf>
- U.S. National Response Team, 18 October 1996, < http://www.nrt.org/>.
- *Understanding Your Risks: identifying hazards and estimating hazards,* FEMA (Federal Emergency Management Agency), 1 October 2001, <http://www.fema.gov/mit/planning_toc3.htm>.
- UK Health and Safety Executive, MHIDAS (Major Hazard Incident Data Service), nd, < http://www.hse.gov.uk/infoserv/mhidas.htm>.
- United Nations Environment Programme – Awareness and Preparedness for Emergencies at a Local Level (APELL), nd, < http://www.unepie.org/pc/apell/>.
- *Useful Links,* International Petroleum Industry Environmental Conservation Association, nd, <http://www.ipieca.org/intro/links.html>.
- *What is the Incident Command System,* Dispatch Monthly Magazine, September 18, 2003 http://www.911dispatch.com/ics/ics_describe.html.
- *Winter Power Failure*, Government of Canada – Safe Guard, 18 April 2001, <http://www.epc-pcc.gc.ca/publicinfo/self_help_ad/self_help/self_winter.html>.

6.3 Additional Industry Documents

- *Risk Analysis Requirements and Guidelines*, Canadian Standards Association, November 1991.
- *Emergency Preparedness and Response,* CAN/CSA-Z731-03, Canadian Standards Association, 2003.
- *Risk Assessment Techniques for Pipeline Systems*, Canadian Association of Petroleum Producers, May 1993.
- *Risk Assessment Process/Guidelines*, TransAlta Emergency Management System, TransAlta Corporation, September 2001.
- *Awareness and Preparedness for Emergencies at Local Level: a Process for Responding to Technological Accidents, United Nations Environment Programme, 1988.*
- *Hazard Identification and Evaluation in a Local Community (TR 12), United Nations Environment Programme, 1992.*
- *APELL for Port Areas: Preparedness and Response to Chemical Accidents in Ports, United Nations Environment Programme, 1996.*
- *TransAPELL, Guidance for Dangerous Goods Transport Emergency Planning in a Local Community (TR 35), United Nations Environment Programme, 2000.*
- *CRAIM Guidelines Risk Management Guide for Major Industrial Accidents intended for Municipalities and Industries, United Nations Environment Programme, 2002.*
- *Guiding Principles for Chemical Accident Prevention, Preparedness and Response - Second Edition, OECD, 2003*
- *Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas, United Nations Environment Programme, 1998.*

6.4 Existing ARPEL Guidelines

- ARPEL Guideline on “Oil Spills Risk Assessment and Management”, May 1999
- ARPEL Guideline on “Regionalizing Oil Spill Contingency Planning in Latin America and the Caribbean, June 2000
- ARPEL Guideline on “Oil Spill Management and Contingency Planning”, December 1997
- ARPEL Health and Safety Guideline – Incident Classification, December 2003

ARPEL MEMBERS

COMPANIES

Administración Nacional de Combustibles Alcohol y Portland (ANCAP) - BP Exploration Company Ltda. - ChevronTexaco - Empresa Colombiana de Petróleos (ECOPETROL) - Empresa Nacional del Petróleo (ENAP) - EnCana Corporation - ExxonMobil - Petroleum Corporation of Jamaica (PCJ) - Petróleos de Venezuela S.A.(PDVSA) - Petróleos Mexicanos (PEMEX) - Petróleo Brasileiro S.A. (PETROBRAS) - Petróleos del Ecuador (PETROECUADOR) - Petróleos Paraguayos (PETROPAR) - Petróleos del Perú (PETROPERU) - Petroleum Company of Trinidad and Tobago Limited (PETROTRIN) - Refinadora Costarricense de Petróleo S.A. (RECOPE) - RepsolYPF - State Oil Companie Suriname N.V. (STAATSOLIE) - Den Norske State Oljeselskap A.S. (Statoil) - Total - Yacimientos Petrolíferos Fiscales Bolivianos (YPFB)

INSTITUTIONS

Instituto Argentino del Petróleo y del Gas (IAPG) - Instituto Brasileiro de Petróleo e Gás (IBP) - Instituto Mexicano del Petróleo (IMP)

Regional Association of Oil and Natural Gas Companies in Latin America and the Caribbean

ARPEL is the only Regional Organization of Oil and Natural Gas Companies in Latin America and the Caribbean. It was created in 1965 and its 24 Member Companies (local, regional and international) represent more than 90% of the regional upstream and downstream operations. It is a business forum for debating on the strategic issues concerning the Oil and Gas Industry, working pro-actively to anticipate the effects of trends, policies and regulations, which may affect the industry's activities.

The ARPEL Mission

ARPEL's mission is to promote and facilitate the development, integration and optimization of the Oil and Natural Gas Industry in Latin America and the Caribbean, being a forum for all key issues of interest to its Member Companies.

The ARPEL Vision

To be the focal point of the Latin American and the Caribbean Region for all issues related to the oil and natural gas industry: environment, legislation, integration, technology and society.

The ARPEL Values

- *Knowledge*
- *Cooperation*
- *Social Responsibility*

REGIONAL ASSOCIATION OF OIL AND NATURAL GAS COMPANIES IN LATIN AMERICA AND THE CARIBBEAN
Javier de Viana 2345 - P.O. Box 1006 - CP 11.200 Montevideo - URUGUAY
Telephone: (598 2) 410 6993* - Fax: (598 2) 410 9207*
E-mail: arpel@arpel.org.uy Internet: http://www.arpel.org