Critical Infrastructure Emergency Risk Management and Assurance

Handbook

2nd Edition
November 2003

Emergency Management Australia

A Division of the Attorney-General's Department

Emergency Management Australia

Mt Macedon Road
Mt Macedon VIC 3441

Tel: 03 5421 5100
Fax: 03 5421 5272
Email: emamtm@ema.gov.au

Copyright

Disclaimer

Foreword

This document is based on AS/NZS 4360: 1999 *Risk Management.* The following interests are represented on Joint Technical Committee OB/7 – Risk Management:

- Australian Computer Society
- Australian Customs Service
- Australian Institute of Risk Management
- Centrelink
- CSIRO
- Department of Administrative Services, Australia
- Department of Defence, Australia
- Environmental Risk Management Authority, New Zealand
- Institution of Engineers, Australia
- Institution of Professional Engineers, New Zealand
- Insurance Council of Australia
- Insurance Institute of New Zealand
- Local Government New Zealand
- Ministry of Agriculture and Forestries, New Zealand
- Ministry of Commerce, New Zealand
- Ministry of Emergency Management, New Zealand
- NSW Department of Urban Affairs and Planning
- NSW Treasury Managed Fund
- National Insurance Brokers Association of Australia
- Securities Institute of Australia
- The Association of Risk and Insurance Managers of Australasia
- University of New South Wales

Standards Australia and Standards New Zealand published AS/NZS 4360:1995 *Risk Management* in 1995. The standard was developed "with the objectives of providing a generic framework for identification, analysis, assessment, treatment and monitoring of risk".

The applicability of the standard to emergency risk management (ERM) was immediately apparent. An ERM workshop was conducted by Emergency Management Australia in 1996[1]. The outcome of the workshop was the development of the *Emergency Risk Management Applications Guide.* The National Emergency Management Committee, Australia's peak emergency management body, endorsed that guide in October 1998.[2]

In November 2002, an EMA sponsored ERM workshop expressed the need for a handbook that complimented the standard and *Emergency Risk Management Applications Guide*. Practitioners dealing with critical infrastructure noted that their degree-of-readiness to meet the challenges presented by extreme risk events was dependent upon addressing both internal sources of risks, and the sources of risk associated with infrastructure interdependencies and externalities.

1 Emergency Management Australia (1996) record of Emergency Risk Management Workshop, 19-21 March 1996, Mt Macedon Paper Number 5 / 1996, Mt Macedon.

2 *ibid*

4 AS/NZS 4360:1999 Risk Management, Standards Australia (1999).

The materials for this handbook are based on the outcomes of the 2002 workshop and the content of the *Emergency Risk Management Applications Guide*. The handbook is an additional resource and will be continually refined to become a repository of the collective knowledge and wisdom of the emergency risk managers in the infrastructure sector. A second workshop was held in April 2003 at EMA to review the draft and provide comment.

The Steering Committee members for the handbook were:

- Mr. Mike Tarrant – EMA (Chair)
- Mr. David Parsons – Sydney Water (Project Proposer)
- Mr. Bruce Angus – Sydney Water
- Mr. Rodney Cade – EnergyAustralia
- Mr. Peter Garland – NSW Critical Infrastructure Review Group
- Mr. Gavin Love – Melbourne Water Corporation
- Mr. Rod Stewart – EnergyAustralia

The Committee would also particularly like to acknowledge the contributions of:

- Erik Maranik, Res Eng (Aust)
- Prof Jean Cross, University of New South Wales
- Ross Pagram, Community IKS Planning

The following organisations were represented in the development of the Handbook:

Agility Management Electricity (AGL)

AlintaGas

ARIMA

Aust. Social and Ethical Accountability Centre

Australian National Audit Office

Australian Water Association

Barwon Water

Brisbane City Council

Brisbane Water

Cardno MBK Pty Ltd

City West Water Vic

Coliban Water

Community IKS Planning

Country Energy NSW

Delta Electricity

Dept of Human Services, Public Health, Vic

Dept. Natural Resources and Environment Vic

Dept. of Premier and Cabinet, Qld

Emergency Management Australia

Energy SA

EnergyAustralia

Ergon Energy

Far North District Council NZ

Four C's Consulting

Hunter Water Corporation

Institution of Engineers

Integral Energy

Johnstone McGee and Gandy

Marsh Pty Ltd

Melbourne Water

Melbourne Water Corporation

Network Performance CitiPower

NSW Agriculture

NSW Critical Infrastructure Review Group

NSW Dept. of Public Works and Services

NSW DLWC

NSW Police

NT Power Water

Office of Emergency Services, NSW

Office of Energy Qld

Powerlink Qld

Protective Security Coordination Centre

Res Eng (Australia) Pty Ltd

SA Dept. of Administrative Services

SA Water Corporation

Santos Ltd

School of Safety Science, Uni of NSW

Scott Cromwell Pty Ltd

Southern Rural Water

Sydney Catchment Authority

Sydney Water

TAS State Emergency Service

Telstra Corporation Ltd

Transend Networks

Transport NSW

TXU Networks Pty Ltd

United Energy Ltd

University of Melbourne

Vic Office of Gas Safety

Vic Workcover Authority

Victoria Police

Victoria SES

Victorian Workcover Authority

Water Corporation WA

Water Services Australia

Western Power Corporation

Yarra Valley Water Vic

Contents

List of tables

Handbook Definitions

Administrative area

The Australian jurisdictions use various terms to describe administrative areas; including precinct, district, region, local government area etc. These should be defined in ERM.

Assurance indicators

Generic characteristics of ERM that allow emergency risk managers to assess their degree-of-readiness for extreme risk events.

Community

A group of people with a commonality of association, generally defined by location, shared experience, or function.

Critical infrastructure

A service, facility, or a group of services or facilities, the loss of which will have severe adverse effects on the physical, social, economic or environmental well being or safety of the community.

Consequence

The outcome of a situation or event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. In the ERM context, consequences are generally described as the effects on persons, stakeholders, communities, the economy and the environment.

Delphi technique

The use of a group of knowledgeable individuals to arrive independently at an estimate of the outcome of an uncertain situation.

Emergency

An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response. In the ERM context for critical infrastructure, it is an event that extends an organisation beyond routine processes.

Enabling Resource

Expertise, staff, finance or other support or aid that makes risk treatments possible.

Environment

Conditions or influences comprising built, natural and social elements, which surround or interact with stakeholders and communities.

Environmental Scanning

The observation of changes in circumstances and context. It can be achieved by processes such as monitoring the news and other media and establishing and maintaining a network of information-sharing peers.

ERM - Emergency Risk Management

A systematic process that produces a range of risk treatments that reduce the likelihood or consequences of events.

Essential Service

An indispensable supply or activity. The various Australian jurisdictions have a range of legislative instruments in place to either define or constitute essential services, their roles and responsibilities. These should be properly researched and understood as part of ERM.

Event

An incident or situation which occurs in a particular place, system or network during a particular time interval.

Externality

Influences exerted by others or the environment, either real or perceived, on an organisation's ability to operate.

Interdependency

The essential external organisational, systems or technical connectivity associated with critical infrastructure operations.

Latent risk

A risk that is present but not yet apparent.

Likelihood

Used as a qualitative description of probability and frequency.

Mitigation

Acts or efforts to lesson the consequences of an event. These may be carried out before, during or after an event.

Monitor

To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Physical resource

Tool, equipment, plant, asset or thing.

Planning and proving

The process of engaging stakeholders and communities by analysing and documenting courses of action and testing them for efficiency and effectiveness.

Preparedness

Measures to ensure that communities and organisations are capable of coping with the effects of emergencies.

Prevention

Measures to eliminate or reduce the likelihood or consequences of an event. This also includes reducing the severity or intensity of an event so that it does not become an emergency.

Recovery

The coordinated process of supporting disaster affected persons in the reconstruction of the physical infrastructure and restoration of emotional, social, economic, and physical well-being. *[AEM Disaster Recovery, 1996]*

Relief

A critical control that avoids people over-stressing themselves during emergencies.

Residual risk

The remaining level of risk after risk treatment measures have been taken.

Resilience

The ability to maintain function. Factors contributing to resilience include existing control measures, duplicated or redundant assets or systems, knowledge of alternatives and the ability to implement them.

Response

Measures taken in anticipation of, during and immediately after, emergencies to ensure the adverse consequences are minimised.

Risk

The chance of an event that will have an undesirable impact. It is measured in terms of consequences and likelihood. In ERM - a concept used to describe the likelihood of harmful consequences arising from the interaction of sources of risk, communities and the environment.

Risk acceptance

An informed decision to accept a particular residual risk.

Risk analysis

A systematic use of information to determine the likelihood and consequences of events.

Risk avoidance

An informed decision to either completely eliminate the sources of a particular risk or not become involved in a particular risk.

Risk control

The implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse consequences.

Risk evaluation

The process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined standards, targets or other criteria.

Risk financing

The methods applied to fund risk treatment and financial consequences of risk.

Risk identification

The process of determining what can happen, why and how.

Risk level

The relative measure of risk as defined by the combination of likelihood and consequence. Usually expressed in terms of extreme, high, moderate and low.

Risk management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk reduction

The application of techniques to reduce the likelihood or consequences of risk.

Risk retention

Intentionally or unintentionally retaining the consequences of risk within the organisation.

Risk sharing

The equitable apportionment of risk among stakeholders and communities.

Risk treatments

Measures that modify the characteristics of organisations, sources of risks, communities and environments to reduce risk, for example, prevention, preparedness, response and recovery.

Robustness

The ability of critical infrastructure to withstand, or recover from, an event.

Source of risk

A real or perceived event, situation or condition with a real or perceived potential to cause harm or loss to stakeholders, communities or the environment.

Stakeholders

Those who may affect, be affected by, or perceive themselves to be affected by, ERM.

Substitutability

The characteristics of a resource that allows it to act or serve in place of another. For example, it may be possible to use other equipment or expertise when local resources are unavailable.

Susceptibility

The degree of exposure to loss.

Vulnerability

The susceptibility of stakeholders, communities and the environment to consequences of events and their resilience to the loss of services or facilities.

1.0 Introduction

1.1 Scope

This handbook provides information for senior emergency risk managers dealing with critical infrastructure. The handbook complements and supports *AS/NZS 4360:1999 Risk Management*[4] and Emergency Management Australia's *Emergency Risk Management Application Guide*[5].

It is assumed in the drafting of this handbook that qualified and experienced emergency risk managers are the audience and that these managers have an understanding of, and experience with implementing, *AS/NZS 4360:1999 Risk Management*.

The focus of this handbook is emergency risk management[6] (ERM) for those events identified by emergency risk managers while assessing risks to critical infrastructure as having **extreme risk** consequences. Extreme risk consequences depend on context, what is an extreme risk for a small regional town is very different to an urban area. The key concept is that an organisation or a community has to operate in a non-routine manner.

Extreme risk consequences may be characterised by:

- long-term inability to deliver the services or facilities of critical infrastructure (loss of control);
- the transition from routine processes to emergency processes;
- the need for multi-agency / jurisdiction (State / Federal / International) response;
- extensive use of external resources;
- possibly large number of fatalities / loss-of-life and/or severe injuries requiring extended hospitalisation;
- general and widespread displacement of people for extended durations;
- extensive property damage;
- severe environmental impact with long-term or permanent damage; and,
- extensive and widespread financial loss.

When considering the strategic importance of these events, it is not prudent to ignore the potential impact on stakeholders or communities of being unprepared.

ERM can be considered to be a means of treating extreme risk. However it is more than just one step in a wider risk management process. Each of the steps in the risk management process is applied during ERM in the new context of assuming an emergency could occur.

---

5 *Emergency Risk Management Applications Guide*, Emergency Management Australia (2000).

6 Emergency risk management (ERM) is a systematic process that produces a range of measures that contribute to the well being of communities and the environment. The philosophy and methods of emergency risk management are a blend of traditional emergency management and the risk management approaches outlined in AS/NZS 4360:1999 *Risk Management*.

Over fifty (50) assurance indicators[7] are provided in this handbook to allow emergency risk managers to qualitatively assess their degree-of-readiness for extreme risk events. For each assurance indicator a range of evidence is suggested to enhance the approach and encourage benchmarking. The assurance indicators are listed at the end of each section with suggested evidence; they are also summarised in Appendix A as a checklist.

What event was it and could it happen to you?

- What happened in **October 1970** that took 35 lives?
- **January 1977**: 83 dead, 213 injured. How would you manage?
- **December 1989**: 13 dead, approx 160 injured. Could you deliver your critical infrastructure services or facilities?
- **September 1998**: 2 dead, eight injured, residents across Victoria left without cooking and/or heating appliances… Does your emergency management plan deal with residual risk?

1.2 Benefits

Critical Infrastructure Emergency Risk Management provides the analysis and planning which enables the services and facilities provided by critical infrastructure to be maintained. ERM is also of considerable value to stakeholders and communities because planning and engagement establishes dialogue, personal networks and relationships between a wide-range of individuals and organisations. Proving and testing plans further develops these relationships and creates trust and confidence.

A major benefit of engaging stakeholders in this process is building the relationships and trust so necessary for managing under uncertain circumstances.

ERM, through a systematic and critical examination, provides a tool for highlighting areas of vulnerability. Importantly, a systematic and critical examination prompts other approaches and challenges established priorities.

From a corporate governance perspective, a systematic and critical examination demonstrates commitment, provides evidence that systems are in place, and encourages a positive approach to performance evaluation.

7 The assurance indicators may be used to qualitatively assess the organisation's ERM approach for catastrophic events.

Can your organisation answer "YES" to these questions?

- Does your Emergency Risk Management project address the risk posed by external factors?
- Do you have working relationships with government and emergency services that include risk treatments other than response plans?
- Do you have mutual support arrangements with others in your sector?
- Would your sector's emergency response be effective?
- Have you established agreed protocols for recovery of your critical infrastructure services or facilities?

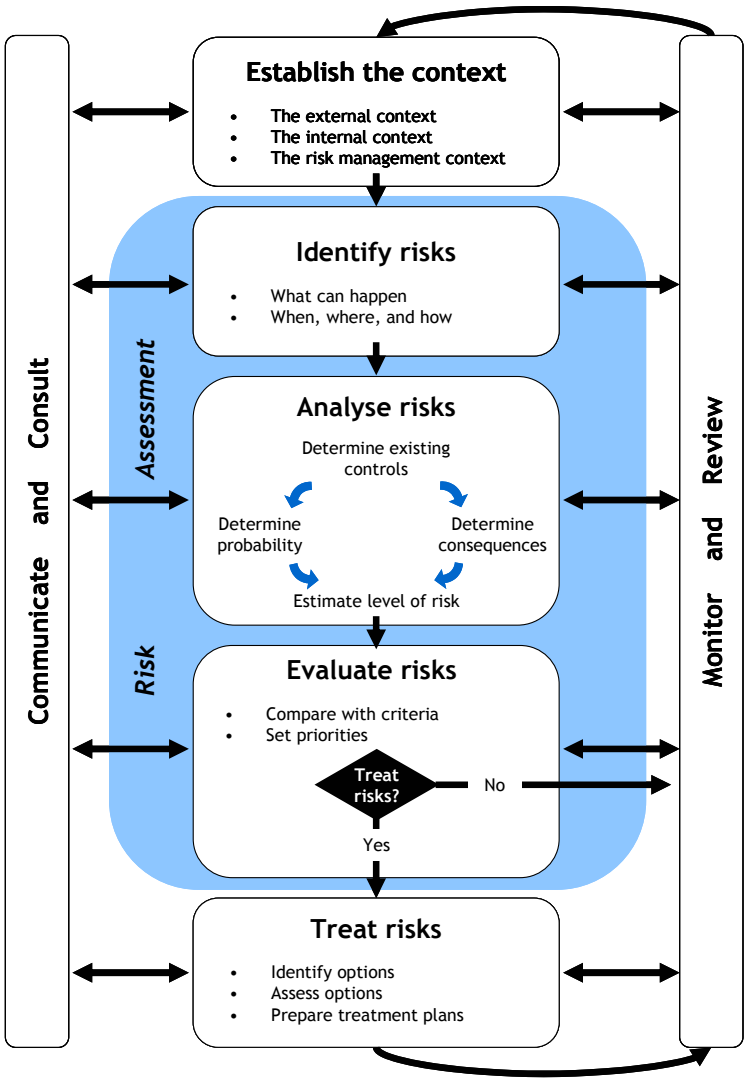
2.0 ERM Overview

This handbook is based on the structure of *AS/NZS 4360:1999 Risk Management.* Each element of ERM is discussed in relation to critical infrastructure. It is important to understand that ERM is not sequential, it is an on-going iterative process that often results in elements being constantly reviewed or modified to accommodate real and changing circumstances.

For example, the processes of risk analysis often identify additional aspects of context which need to be considered, or new risks. Risk treatments often introduce new risks which must be identified and analysed.

2.1 The ERM Process Elements

The main elements of the emergency risk management process are described in the diagram below.



2.2 ERM Terms

The terms associated with each of the ERM elements are explained below.

Communication and consultation

Identify stakeholders and communities, and establish paths of communication. Where stakeholders and communities contribute to the decision making process there is a much larger pool of information and expertise to enable appropriate solutions to be developed. For extreme risk events which have high levels of uncertainty, communication and consultation is considered extremely important. Communication and consultation develop resilience amongst stakeholders and communities and is invaluable in regaining control of critical infrastructure during extreme risk events.

Newcastle

NSW
DECEMBER 1989
In Australia, an earthquake of Richter magnitude 5.5 (almost that of the Newcastle earthquake) occurs, on average, every 13 months.

Establish the context

Explore the background to the organisation and the community it supports and the environment in which it operates. Define objectives and problems for which decisions are required and the scope of studies needed.

Define the problem. Establish a management framework that takes account of the nature and scope of the problem and how the ERM process will be undertaken. Define the stakeholders and the various communities.

Define measures that will be used to establish levels of acceptable risk using tools such as consultative groups, and develop risk evaluation criteria. Review the applicability of legislation, operating licences or similar instruments which define the level of risk to extreme risk scenarios. If inadequate, modify them to be appropriate for the nature and scope of the problem.

Establish processes to ensure that the nature and scope of the problem, and levels of risk, are reviewed regularly.

Identify risks

Identify and describe the sources of risk, stakeholders, communities and environments. Scope the vulnerabilities and describe the risks.

Analyse risks

Analyse the risks associated with the problem by determining the likelihood and consequence of the identified risks.

Evaluate risks

Compare risks against risk evaluation criteria to decide whether they require action, and prioritise the risks.

Treat risks

Identify and evaluate treatment options. Respond to the level of risk by deciding which source of risk can be addressed either by reducing susceptibility and increasing resilience of the community, or by increasing the robustness of critical infrastructure. Model changes to determine the new level of risk. Select, plan and implement treatments. Define mechanisms for monitoring treatments.

Monitor and review

Establish and maintain systems that monitor and review risk and its management. Latent and residual risks are ever-present. Conduct on-going ERM to ensure that change and uncertainty can be accommodated.

Documentation

Maintain appropriate documentation at all stages to retain knowledge and satisfy audit requirements.

Gas Pipeline

Tennant Creek Earthquake
1988

The pipeline which supplied Darwin's electricity system was damaged during this Earthquake.

3.0 Getting Started

ERM, like any management process, requires leadership at the highest levels of the organisation and the community. Appropriate training, resources, supporting policy and procedures all must be properly established at the outset because of the high levels of complexity and uncertainty associated with ERM.

CIERM is a social process as much as it is a technical and political process. The primary objective is continuity of services and facilities to the community. Meaningful participation with the community and effective collaboration with a wide range of organisations is required. Communication and consultation are essential means for ensuring participation and collaboration. They will be the first step of the risk management process.

3.1 Assurance Indicators and Typical Evidence

- Organisational policies for ERM have been proclaimed.

  Typical Evidence: *Policy documentation endorsed by the CEO / Board, or statements concerning ERM as part of other risk management policies. These should include statements of the operating environment and services or facilities.*

- An ERM framework has been established.

  Typical Evidence: *Organisational structure includes emergency, risk and/or incident management responsibilities at a senior level.*

- An ERM Committee has been identified and established.

  Typical Evidence: *Meeting agendas, actions, contact details etc.*

- Required expertise and training needs have been considered

  Typical Evidence: *Records of training needs analysis and training provided.*

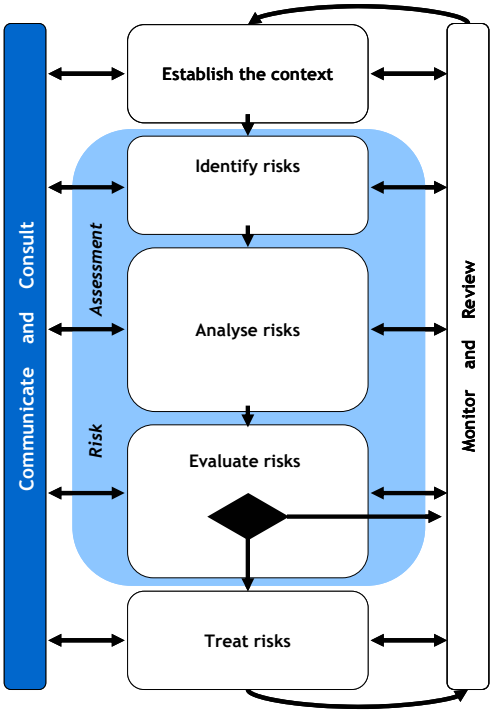
- An appropriate project management structure to develop ERM, together with a process for continually improving the process, is established.

  Typical Evidence: *Project management plans including work breakdown structures, estimates, schedules, documented roles and responsibilities exist and have been formally approved. Processes have been developed to ensure that once ERM is established it becomes a continual process.*

4.0 Communication and Consultation

4.1 General

Successful critical infrastructure ERM requires the effective engagement of stakeholders and communities. Effective engagement enables the strategic management of uncertainty and develops resilience amongst those involved. ERM goes far beyond being simply a technical or political process - it is also a social process.



Communication and consultation are an important consideration at each step of the ERM process. It is critical to identify stakeholders and develop a communication strategy that will engage stakeholders and communities at the earliest stage. Some stakeholders include the community, customers and suppliers, government and government departments, and other infrastructure operators, including competitors.

Effective communication and consultation is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which certain decisions are made and why particular actions are required.

Intra / inter-relationships need to be identified, acknowledged and appropriate processes put in place. For example, members of the community and staff may have multiple roles and responsibilities that could contribute to ERM. Because of the inherent uncertainty and complexity in ERM it is important to acknowledge that values and experience play a fundamental role in people's thinking and decision-making. Stakeholders and communities are likely to make judgements on the acceptability of a risk based on their beliefs, perceptions and ability to implement mitigation strategies.

Participation is the first step towards developing partnerships and their supporting relationships of trust. In times of actual emergency, when routine processes are unable to address the consequences of an event, well-developed partnerships and relationships improve the likelihood of a timely, considered and measured response.

Stakeholders can provide valuable input at each step of the process, providing information about context and background from different perspectives, helping to identify risks, and providing information for their analysis. Engaging stakeholders helps ensure that multiple perspectives can be brought to ERM.

Perceptions of risk vary and critical infrastructure operators must be careful when communicating with stakeholders and communities. Organisations that operate critical infrastructure are often monopolies and interface with stakeholders and communities at various levels.

Conflicting corporate messages impact significantly on trust. This could happen when the business arm of the operator is talking up the reliability of the systems and the operational arm is highlighting the range of system vulnerabilities that exist on a day-to-day basis. Confusion can arise for critical infrastructure operators when the levels of risk prescribed by operating licences do not align with the views of the majority of stakeholders and communities.

The process of communication should consider:

- audience (primary, secondary and opportunistic);
- content (simple, technical or non-technical, clear, unambiguous)
- assumptions (social, religious, cultural, technical); and
- mode (radio, television, journals, person-to-person, consultative committee etc.);

In relation to the audience it should also consider:

- needs (language, readability, vision impaired, etc.);
- political and social sensitivities; and
- boundaries (legal, political, social, technical, etc.).

The nature and timing of an extreme risk event will dictate many elements of a communication strategy. Table 1 lists a number of elements that are suggested.

4.2 Assurance Indicators and Typical Evidence

- A Communication and consultation strategy exists.

  Typical Evidence: *Documentation outlining responsibilities, communication and consultation access points, contact details, media messages etc.*

- Communication and consultation protocols have been developed and implemented with the participation of stakeholders and communities.

  Typical Evidence: *Internal newsletters, web sites / pages, training materials, meetings, minutes, etc. The existence of appropriate committees, media strategies, stakeholders and community groups, supporting structures etc.*

- Stakeholders and communities have been engaged in the development of the communication and consultation strategy and had input to ERM.

  Typical Evidence: *Meeting minutes, working groups, brainstorming sessions etc.*

- Stakeholder and community views are monitored and where necessary, communication strategy is amended.

  Typical Evidence: *Surveys, questionnaires, meetings etc.*

- Media spokespeople have been identified and trained.

  Typical Evidence: *Training records, responsibility charts, videotapes of practice etc.*

- Stakeholder and community liaison officers have been identified and trained.
  Typical Evidence: *Training records, responsibility charts etc.*

Table 1. Suggested elements of a communication strategy

Pre-event	Post-event
Ensure that the communication strategy has considered stakeholders and organisations with which there are inter-relationships.	Review stakeholders and inter-relationships to ensure communication channels are appropriate and that strategies are in place to recognise and work with emergent groups.
Engage stakeholders and communities (including community representatives, politicians, etc.)	Review stakeholder and community views. Brief stakeholders and communities.
Provide opportunities for stakeholders and communities to express their views.	Provide opportunities for stakeholders and communities to express their views.
Provide basic emergency hints.	Monitor spokesperson's performance – beware of unintended messages.
Communicate the nature of emergencies and qualify guarantees in these cases. Don't build expectations that can't be fulfilled.	Establish media "centre" – invite media to command centres, provide access, provide opportunities for good vision etc.
Liaise and brief / educate media on issues.	Brief own staff as soon as possible, ideally before the media.
Be aware of legal constraints.	Confirm what can be disclosed with interests such as police, security organisations, insurers, lawyers etc.
Ensure effective internal communications.	Understand the media agenda, develop appropriate approaches (positive news, honesty, public interest, etc.)
Be cautious with public meetings, use skilled and knowledgeable facilitators.	Analyse the issues from a variety of perspectives. Engage the media.
Explain the context of the problem before proposing solutions.	Be aware of "technical truth" versus "public fact" issues.
Establish a stakeholder and community management plan.	Avoid appearing devious or "high and mighty".
Establish a media strategy, core messages, and materials.	Review communication assumptions.
Train spokespersons.	Use credible and articulate spokespersons ("talent").
Develop regulator / jurisdiction protocols.	Implement regulator / jurisdiction protocols. Recognise that an extreme risk event may result in control being vested in another jurisdiction or authority.

Communication

- The **ability to communicate appropriately with stakeholders** is a key skill for Emergency Risk Managers. If emergency risk managers are not able to communicate, problems will arise. Some common communication traps include:
- The **application of inappropriate techniques** or language leading to the development of misinformation and consequently poor decision making. Examples include poorly run meetings, trying to manipulate the media, and playing politics.
- **Incorrect information** leading to direct decision-making mistakes.
- **Poor content** sending wrong messages and dispersing effort.
- **Slow communication of identified problems** causing delays and indicating poor management commitment, understanding and leadership.

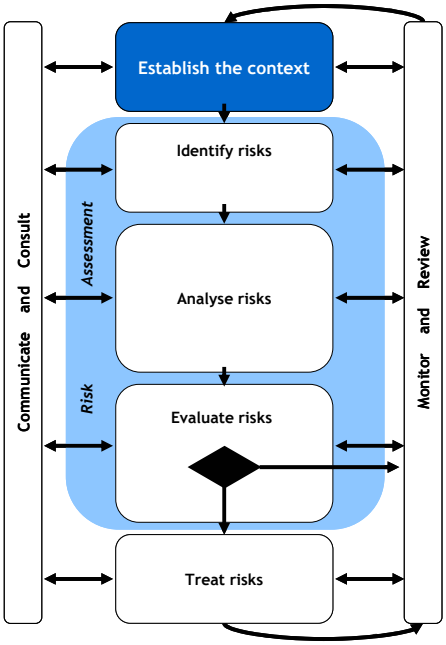
Storm, Brisbane

Qld
1985

Major damage to a range of infrastructure was sustained during this extreme event.

5.0 Establish the Context

5.1 Gather Information



Establishing the context involves using experience and judgement and a range of information sources to set the scope and boundaries of the particular risk management study being undertaken.

Risk relates to things that might happen that will impact on desired objectives. Therefore, a key part of establishing the context is to identify the organisation's objectives and those of other stakeholders. In the context of ERM it must be recognised that objectives of the organisation and of stakeholders post-event may differ from operational objectives under normal circumstances and may mean changes in priorities and criteria for acceptability. In most cases regaining the ability to deliver the service or facility becomes the primary objective of the critical infrastructure operator post event.

The capabilities and limitations of the critical infrastructure organisation and its people need to be understood as this will affect the way in which emergencies can be managed.

The way in which ERM fits within other risk management activities in the organisation should be defined. ERM will require resources and responsibilities to be allocated. Often an ERM committee will be established to ensure good internal coordination and involvement of internal stakeholders. A framework which ensures accountability for ERM at senior levels in the organisation is required as well as an effective project management structure to ensure that ERM is managed effectively. The systems and framework that are put in place should ensure that ERM is monitored and reviewed and that the results of review activities feed into continuous improvement.

The inability to deliver a critical infrastructure service or facility, in line with an organisation's social and ethical accountability, represents the single most significant characteristic of an extreme risk event. The inability to deliver the service or facility may be considered to be a loss of control.

Loss of control may be partially compensated by the degree of resilience of the various stakeholders and communities. The degree of resilience will strongly depend on the effectiveness of prior engagement, particularly if alternative delivery systems are deployed with which the user may have had little or no experience. This again stresses the need for effective communication channels with stakeholders.

Regaining control may include recovery of the infrastructure, or it may include deploying alternatives, or a combination of both, to ensure that stakeholder needs and their key

objectives are met. While treatment options are not considered in this step, community and stakeholder objectives and needs should be identified and conflicting needs and objectives rationalised.

Two primary groups of stakeholders to be considered are:

- those involved with addressing the resilience of the stakeholders (such as local government, media and hospitals) and communities; and
- those involved with activities needed to restore or provide alternatives to the delivery of the service or facility, including other infrastructure organisations and key or alternative suppliers.

The capabilities and limitations of these groups need to be established. A high degree of coordination will be required and the mechanisms to achieve this will need to be established early. Those that contribute most to improving resilience and regaining control should be afforded priority.

Table 2. Examples of stakeholder groupings

Stakeholder and community resilience		
	local communities and media	welfare
	business and industry	regional communities
	safety providers	cyber communities
	local authorities / government agencies	aid providers
	residential property owners	non-government organisations
	direct and indirect customers	investment property owners
	local representatives	welfare and Church groups
	hospitals / medical practitioners	shareholders
Regaining control *(Restoring the ability to deliver the critical infrastructure service or facility)*		
	energy (electricity, gas, etc.)	regulators
	water and sewage	insurers
	telecommunications	legal advisors
	transport	auditors
	emergency services	peak industry bodies
	personnel unions	professional advisors
	decision makers	internal experts
	key suppliers	intelligence organisations

5.2 Evaluation Criteria

In relation to critical infrastructure, evaluation criteria may be prescribed through legislation, operating licences or other statutory instruments. The relevance of these acceptability criteria to situations following an extreme risk event needs to be defined and new criteria may need to be established.

Consultative group processes can be used to help develop risk evaluation criteria and levels of acceptable risk if they are not prescribed. These processes may also be used to review the prescribed criteria or levels of acceptable risk. Evaluation criteria and levels of acceptable risk may also be driven by organisational policy or the regulatory and political environments in which the critical infrastructure operator functions.

When developing risk treatments for extreme risk events it is important to consider the potential for severe adverse effects on the physical, social or economic well-being or safety of the community. The evaluation criteria and levels of acceptable risk should reflect these considerations.

As the nature and scope of the problem changes, the evaluation criteria may be further developed and refined. For critical infrastructure, specific evaluation criteria may need to be developed that correspond to particular sources of risk or anticipated risk treatments. For example, where a risk treatment calls for the development of excess capacity, it may be necessary to develop technical evaluation criteria for each possible alternative approach.

Coode Island
Melbourne
Victoria 1991

A fire on Wed. 21 August 1991 at the bulk chemical storage tank facility, comprising over 200 tanks containing flammable and toxic chemicals.

5.3 Assurance Indicators and Typical Evidence

- Stakeholders and communities have been identified, characterised, and engaged.

  Typical Evidence: *Stakeholder and community registers / databases containing contact details, documentation indicating that demographic or other data has been considered, meeting schedules etc., minutes of meetings and associated action sheets / files, documentation outlining rationale for engagement.*

- Objectives of the organisation, the community, and other stakeholders in the context of an extreme risk event having occurred, have been defined.

Typical Evidence: *Documented objectives for different groups rationalised to overall objectives for ERM. Evidence of the objectives' use in the risk identification process.*

- Stakeholder and community expectations and perceptions have been recognised.

  Typical Evidence: *Records of public meetings, surveys etc. are available. Documentation exists which indicates consideration of what is acceptable to the stakeholders and communities in terms of loss of life, health, economic loss, environmental harm, infrastructure damage, and heritage loss.*

- Inter-relationships have been identified and communication channels established.

  Typical Evidence: *Methods used to establish interdependencies, records of meetings to work out relationships.*

- The legislative context has been reviewed particularly in relation to criteria for acceptable risk.

  Typical Evidence: *Review of legislation, operating licences, statutory instruments etc.*

- Risk evaluation criteria are available.

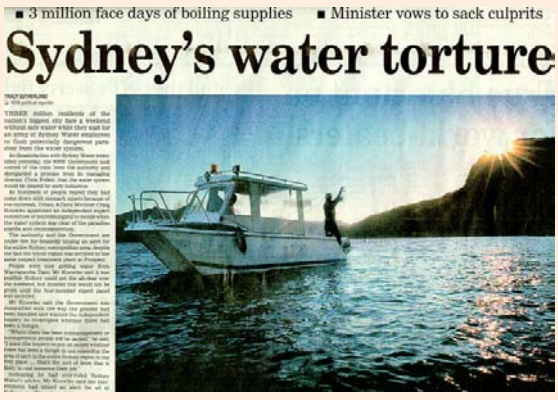
  Typical Evidence: *Documentation indicating that criteria have been developed by the organisation taking the input of stakeholders and communities into consideration. Factors to which these criteria relate include: technical, economic, legal, social, and humanitarian.*

- Risk evaluation criteria have been reviewed throughout the ERM process.

  Typical Evidence: *Documentation indicating that monitoring and review has taken place: project plan amendments, executive minutes, project management minutes etc.*

- Prioritisation tools, such as ranking systems, have been developed and endorsed by the CEO / Board of the organisation.

  Typical Evidence: *Documentation of the development process: board minutes, meeting minutes etc.*



■ 3 million face days of boiling supplies ■ Minister vows to sack culprits

Sydney's water torture

Sydney Water Crisis

NSW, October 1998
Cryptosporidium and giardia contamination

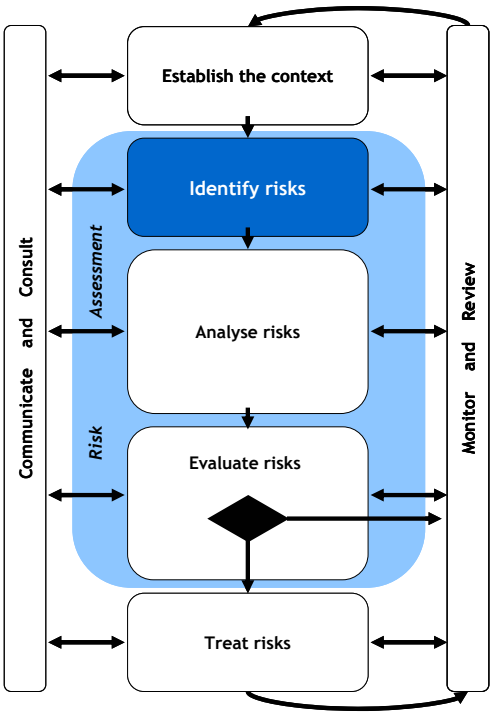
6.0 Identify risks

6.1 General

Identifying risks involves identifying what can happen and how.

In Australia critical infrastructure is generally geographically dispersed, difficult to secure, may have low levels of redundancy, and is often co-located with other organisations' assets.

Identifying risk requires a detailed investigation of the characteristics of the source of risk and how it interacts with the critical infrastructure and with stakeholders, communities, and the environment. It also involves examining the robustness of the critical infrastructure, and the vulnerability and/or resilience of the community and environment.



6.2 Identify Sources of Risk

A source of risk presents the potential for loss or harm to stakeholders, communities and/or environment through the failure of critical infrastructure to deliver its services or facilities. Sources of risk may come from natural, technological, biological or civil / political origins. The following table provides some examples that may be relevant to ERM.

Floods, Nyngan

NSW
1990

Extensive and prolonged damage to transport, supply, and power networks. Power, water and sewerage were disabled for approximately two weeks

Table 3. Sources of Risk[9]

Primary	May also consider …
aeronautical	carcinogens / mutagens / pathogens
biological, including pandemics	climate change
chemical	economic recession / depression
civil disturbance / riot	electromagnetic radiation
electronic / cyber-attack	epidemic (human, animal, plant)
explosion / incendiary / fire (residential, industrial, bush, etc.)	erosion (soil, coastal)
hazardous materials	fog
human acts (terrorism / vandalism / wilful damage / retribution / sabotage)	frost / extreme cold management
industrial accident (chemical, mine, plant, smelter etc.)	organisational failure
infrastructure failure (power, water, telecommunications, gas, etc.)	exotic disease (animal and plant)
market failure	resource shortage / depletion
manipulation (deliberate or forced misuse of controls)	salinisation
pollution (chemical, oil, waste, etc.)	space debris
radiological / nuclear	subsidence
seismic (earthquake, tsunami, volcano)	supply chain failure
slope failure (landslide, rock fall, mudflow)	
storm surge	
structure failure / collapse (bridge, building, dam etc.)	
transport accident (air, rail, road, sea)	
warfare	
weather (electrical storm, cyclone, tornado, torrential rain, flood, hail, blizzard, heat-wave, etc.)	

For an extreme risk event, it is likely for a combination of a number of sources of risk to interact.

The ERM process for critical infrastructure should identify and describe sources of risk and their effects in terms of spatial distribution, temporal distribution, intensity, and manageability. These four primary characteristics are further described below.

9 Adapted from *Emergency Risk Management Applications Guide*, Emergency Management Australia (2000).

Techniques for identifying sources of risk include:

- researching the history of emergencies;
- inspecting for evidence of previous emergencies, sources of risk and vulnerability;
- examining literature or interviewing people about, or from, similar circumstances;
- requesting information from State / Territory or Federal governments;
- mapping communities and environmental characteristics; and
- using groups (internal and external) to identify possible sources of risk.

6.3 Describe Risks

Describing the risk involves describing the source of risk and how it affects infrastructure. It also involves identifying how the inability of the critical infrastructure to deliver services and facilities may impact on stakeholders and communities. This is not always straightforward as people may have different perceptions on what is a significant source of risk.

It is therefore important to engage the stakeholders and communities to consider:

- their own needs (for example, potable water, shelter, sustenance, energy, hygiene etc)
- the impact of the loss of critical infrastructure services or facilities on their needs;
- the possible extent of damage resulting from loss of critical infrastructure;
- alternative services and facilities that fulfil their basic needs;
- the probable time for restoration; and,
- the cost of repairs.

The four primary characteristics that are considered in relation to describing sources of risk which may lead to extreme risk events are:

- spatial distribution (the area that a source of risk may impact);
- temporal distribution (warning time, duration, time of day / week / year, frequency);
- intensity (how big, fast, powerful); and,
- manageability (what can be done about it).

For each source of risk these characteristics may mean quite different things. For example, in a cyclone, intensity relates to wind speed and air pressure, whereas in an earthquake intensity refers to the number and strength of earth tremors. Each source of risk should be briefly described using appropriate characteristics.

When dealing with the risk of human interference, such as terrorism, vandalism, wilful damage, retribution or sabotage, the risks can be further described in terms of the perpetrator's desire, confidence and experience, knowledge, and resources. An understanding of these, and the various resources available to the perpetrator, will provide important information for developing risk treatments.

Risk statements systematically record elements and sources of risk. One method, based on a scenario approach is illustrated in the table below. Alternative formats list the elements at risk as the specific needs of the community. Importantly, documented risk statements may be used to facilitate discussions with stakeholders and communities and promote effective engagement.

The following fictitious example explores an electrical storm scenario.

Table 3. Example of mapping source and element at risk

Scenario

An electrical storm causes a transmission outage due to lightning discharge. The response to this event is routine, however at around the same time generation control is lost. The combination of these events impact on stability of the network. Ultimately a system restart is required which is not routine.

Source of risk		**Element at risk** – example stakeholders and communities *(repeat for environment and other defined elements at risk)*				
Electrical storm	Intensity / Impact ↓	Cyber	Local	Regional	State	National
Sub-station damage		✓	✓	✗	✗	✗
+ transmission outage		✓	✓	✗	✗	✗
+ lost generation control		✓	✓	✓	✓	✗
+ lost frequency control		✓	✓	✓	✓	✗
= system restart		✓	✓	✓	✓	✓

6.4 Scope Vulnerability of Infrastructure

In identifying what might happen and how, the robustness of the infrastructure needs to be considered. This includes the susceptibility to failure and the speed and effectiveness with which the services and facilities can be restored. Scoping vulnerability involves identifying critical components in the system, interdependencies and system-specific weaknesses. Critical infrastructure may also be vulnerable through proximity to the source of risk, and co-location of infrastructure.

6.5 Scope vulnerability of stakeholders and communities

For an extreme risk event, it is certain that a combination of a number and different types of stakeholders, communities and environments will be impacted. The vulnerability of stakeholders and communities is defined by their susceptibility to harm and their resilience or ability to recover. Scoping vulnerability involves looking for elements that are noticeably less resilient or more susceptible than others to the loss of infrastructure. For some communities and stakeholders there may be a wider range of alternatives available than for others.

The stakeholder groups and communities may be divided into groupings based on a range of factors, for example shared experience, sector or function. Individuals may belong to several groupings.

The process of identifying and describing stakeholders and communities requires examining characteristics or information relating to them. Characteristics may include: population size, spatial distribution, remoteness, prior experience or perception, degree of exposure, capacity, access to resources, and susceptibility or resilience.

Without detailed knowledge of the stakeholders, communities and environment, it is impossible to determine the elements at risk and to describe their vulnerability, and therefore impossible to develop appropriate risk treatments. Table 4 contains characteristics that may be used as prompts.

Table 4. Some stakeholders, communities and environmental characteristics

Demography	Culture	Economy	Infrastructure	Environment
population	traditions	trade	communication	land forms
age distribution	ethnicity	agriculture livestock	transportation networks	geology
mobility	social values	investments	services	waterways
skills	politics	industries	assets	climate
health status	religion	wealth	government	flora
education	attitudes		resource base	fauna
	risk awareness			

6.6 Revisit risk evaluation criteria

It may be necessary to revisit risk evaluation criteria to check that all identified risks have evaluation criteria or that the underlying objectives have been effectively distilled.

Table 5. Critical infrastructure emergency risk managers may need to consider.

Vulnerability indicators for stakeholders and communities		
	Less vulnerable	**More vulnerable**
Special needs / health	Healthy stakeholders and communities	Frail, infirm, dependent on medical support / systems
Critical infrastructure	Alternative sources of supply or substitution possible Robust, protected	No alternatives Frail, exposed, concentrated
Employment	Low unemployment	Substantial unemployment
Ethnicity	Groups with sufficient knowledge of English; socially cohesive members of supporting groups	Groups with no, or insufficient, English; socially not cohesive; non-members of supporting groups
External government financial support and policies	In place and effective	Not in place or not effective
Government planning processes including mitigation policies and programs	In place and effective	Not in place or not effective
Items of environmental and cultural significance	Robust, protected	Frail, exposed
Local economic production and employment opportunities	Robust, protected	Frail, exposed
Medical and emergency services	Robust, resilient	Frail, not resilient
Response and recovery capability	Tested and adequate	Untested or inadequate
Social structure	Strong and robust	Fragile
Stakeholders and communities planning process including mitigation measures	Stakeholders and communities participate in planning process; effective mitigation strategies	Stakeholders and communities not involved in planning process; no or ineffective mitigation strategies

6.7 Assurance Indicators and Typical Evidence

- The sources of risk have been identified and described.

  Typical Evidence: *Documentation such as risk registers or databases of sources of risk. A range of methods by which risks have been identified are described.*

- The communities have been identified and described.

  Typical Evidence: *Documentation, supporting surveys, demographic information.*

- The environments have been identified and described.

  Typical Evidence: *Documentation of environmental factors, impact statements.*

- The vulnerability of the identified communities have been scoped.

  Typical Evidence: *Documentation indicating appropriate research and analysis of vulnerability in terms of the ability to cope with and recover from an extreme risk event.*

- The vulnerability of the identified environments has been scoped.

  Typical Evidence: *Documentation indicating appropriate research and analysis of vulnerability in terms of the ability to cope with and recover from an extreme risk event.*

- The effect of sources of risk on critical infrastructure has been identified.

  Typical Evidence: *Documentation indicating that sources of risk to critical infrastructure have been reviewed to include qualitative descriptions and the rationale behind declaring a risk.*

- The vulnerability of critical infrastructure has been described.

  Typical Evidence: *Documentation indicating appropriate research and modelling of vulnerability in terms of criticality, exposure and restoration.*

- Risk statements have been generated.

  Typical Evidence: *Risk matrices or similar analysis tools such as databases .*

- Risk evaluation criteria have been revisited.

  Typical Evidence: *Minutes of meetings, action sheets, project documentation .*

- Stakeholders and communities have been involved in the identification of risks.

  Typical Evidence: *The presence of, and documentation for, consultative groups, public meetings, correspondence .*

- Monitoring and review processes have been established to capture future sources of risk.

  Typical Evidence: *Quality / project management systems, project meetings, feedback protocols .*

SCENARIO ANALYSIS

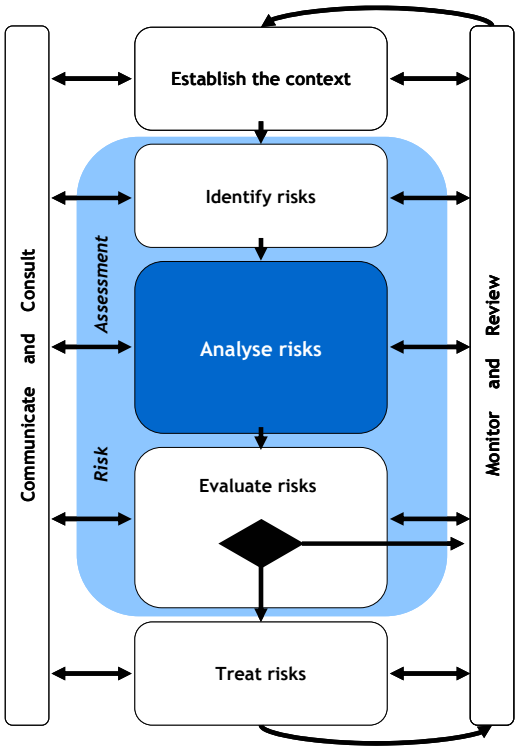
What is the cause? What is the likely effect?

Scenario analysis can be used to determine cause-effect relationships for complex situations at all stages of ERM but is particularly helpful at identifying and analysing risks. Risk scenarios can describe sources of risk in a manner that will help with the generation and selection of risk treatments.

A scenario can be constructed by combining a number of possible conditions and cause-effect relationships. Importantly, any scenario analysis must examine the relationship between the immediate, residual, and latent risks and how these may combine to trigger, contribute to, or escalate, an event.

7.0 Analyse Risk

7.1 General



The purpose of analysing risks is to provide information to assist in the evaluation and treatment of risks. Methods of analysis should therefore match the criteria which will be used to decide whether the risk is acceptable and should explore the factors needed to define appropriate treatment. Within the broad area of ERM a number of different analyses are likely to be carried out. The objectives and scope of each should be defined.

With respect to extreme risk events for critical infrastructure significant analysis is required in relation to:

- the development of the extreme risk event
- existing controls and systems
- vulnerabilities
- infrastructure interdependencies within and external to the organisation;
- physical resource availability, prioritisation and substitutability; and,
- enabling resource availability, prioritisation and substitutability.

Analysis will require considered and experienced judgements and assumptions. These will involve uncertainty and be based on incomplete information. Where possible the confidence of the risk analysis should be included. This may be determined by such parameters as; the quality of information used, the type of studies conducted, and the depth to which scenarios have been explored.

7.2 Determine Likelihood and Consequence

The predicted likelihood and expected consequences of risk should be estimated either qualitatively or quantitatively based on the description of the source of risk and the robustness of infrastructure and the vulnerabilities of the communities and environment.

The outcome of an event depends on the effectiveness of the systems already in place to treat risk, for example on existing response arrangements for infrastructure failure. In analysing possible consequences and their likelihood the effectiveness of existing controls should be reviewed in the context of extreme risk event.

Experience of extreme risk events is usually limited. To overcome this, experienced emergency risk managers need to source a range of information and apply a variety of techniques. To avoid bias the best available information and techniques should be applied. These may include the use of:

- past records;
- experience and judgement;
- industry practice;
- appropriate journals and literature;
- scenarios, experiments and prototypes;
- peer reviews and audits; and
- modelling.

Scenario Exercises

Scenario exercises for critical infrastructure have proven invaluable. They help to explore the complexities of the various modes of critical infrastructure loss of control. Scenarios can be basic, simply representing an experienced risk manager's judgement, or they can be further developed by paper-based studies or large and complex exercises which may include quantitative modelling. Scenarios can be extended to enable the likely merit of risk treatments to be explored.

The development of scenarios allows for either qualitative or quantitative risk assessment, predictive analysis and modelling based on the description of sources of risks, and the degree of vulnerability of the stakeholders, communities and environment.

Modelling

Predictive analysis and modelling may be used to accommodate uncertainty and to investigate the impact of various selected assumptions. Modelling can be physical, virtual, mathematical or intuitive. Outputs may provide valuable information for determining effective treatments.

Other Tools

There is a range of different formal analysis tools that may be used to explore the impacts of rare extreme risk events, for example the routes to unwanted outcomes, the effectiveness of controls or the different paths an unfolding disaster may follow. Reliability engineering analysis tools (used in normal critical infrastructure management) may be extended to cover rare extreme risk events.

Quantifying Likelihood

The likelihood of a particular outcome depends on:

- the likelihood of the initiating event (for example, fire, flood, terrorist attack etc),
- the likelihood that this will lead to a major failure in critical infrastructure, and
- the likelihood that particular sectors of the community, particular elements of the environment, or particular stakeholders will be affected by that loss.

It may not be possible to produce a quantitative estimate of the likelihood of each outcome for each risk. Using quantitative information to explore factors which influence the magnitude of the risk, however, can substantially assist decision-making and understanding. Judgements about whether the risk is acceptable and what treatment is required become both more transparent and more reliable

Limitations on Level of Risk

To estimate a level of risk, a single descriptor or measure for consequence is combined in some way with an estimate of the likelihood that the consequence will occur. However, in the case of Critical Infrastructure Emergency Risk Management, producing a single "level of risk", whether qualitative or quantitative, is limited in a number of ways:

- There is a high level of uncertainty in the way a source of risk may affect critical infrastructure and in the way in which a major loss of infrastructure will affect stakeholders and communities;
- Many different types of consequence arise from the loss of critical services and facilities for example, economic, social, environmental etc. These have different impacts on different stakeholders and there will be both real and perceived differences in the magnitude of the consequences to different stakeholders and communities. This makes it extremely difficult to produce a single quantitative measure or even qualitative description of consequence; and
- Emergencies are by definition highly unlikely. There is little reliable data, therefore, on which to base likelihood estimates of failure from many of the potential and considered sources of risk.

Any estimate of a single level of risk will generally be extremely uncertain and useful only for broad based decisions on priorities.

7.3 Analysis Outcome

The main outcome of the analysis process is a greater understanding among the stakeholders and communities of the consequences and likelihood of the extreme risk event. This understanding may be used to decide whether a risk is acceptable and to define the additional treatment required.

7.4 Assurance Indicators and Typical Evidence

- Critical infrastructure interdependencies have been identified and described.

  Typical Evidence: *Documentation or databases of interdependencies such as network or systems links with internal or external providers, network diagrams, network models, systems architecture etc.*

- Physical resource availability has been identified and described.

  Typical Evidence: *Documentation or databases of essential plant and equipment, substitute and substitutable equipment, supplies, chemicals, spare parts etc.*

- Enabling resources have been identified and described.

Typical Evidence: *Up-to-date documentation or databases of key staff, consultants, substitutable expertise etc. available. Documentation indicating that financial analysis has occurred, identification of emergency sources of funds etc.*

- Scenarios have been explored and have considered a range of sources of risk and the vulnerabilities of critical infrastructure, of stakeholders, and of the community.

  Typical Evidence: *Documentation relating to the analysis.*

- Consequences have been explored and described using data and quantitative methods where appropriate.

  Typical Evidence: *Documentation relating the analysis of consequences which records the methods used, sources of data and outcomes.*

- Estimates of the likelihood of different consequences have been made

  Typical Evidence: *Documentation relating the analysis of likelihood, which records methods were used, sources of data and outcomes.*

- Risk statements have been expanded to include information on likelihood and consequences and, where appropriate, a level of risk.

  Typical Evidence: *Review of the risk statements.*

- The views of stakeholders and communities have been included in the analysis and the results discussed with them.

  Typical Evidence: *Documentation indicating meetings, correspondence, liaison etc.*

- The outcome of analyses have be verified where possible.

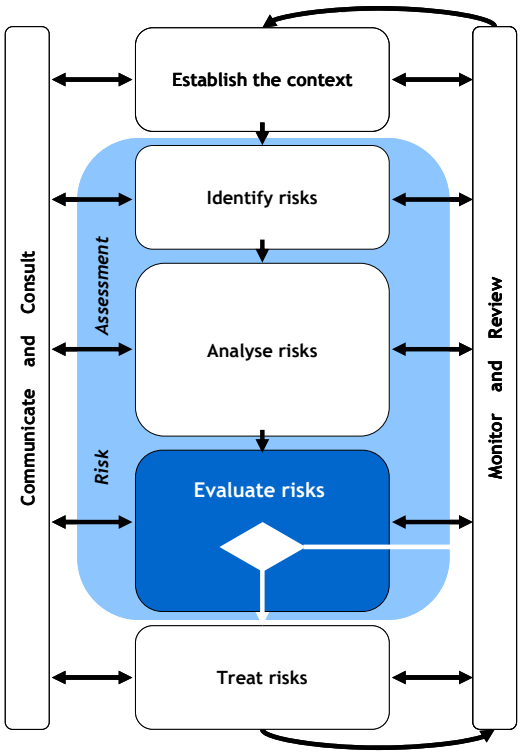
  Typical Evidence: *Documentation of verification.*

Derwent River

Tasmania
January 1975
The vessel SS Lake Illawarra collided with the Tasman Bridge on 5 January 1975. The loss of the bridge section impacted n the people in southern Tasmania.

8.0 Evaluate Risks

8.1 General



Given limited resources, it is necessary to determine which risks will be treated and those that will be treated first. This is achieved by comparing levels of risk estimated during analysis with risk evaluation criteria.

The evaluation criteria defined earlier may need to be revisited as a result of the analysis and further consultation with communities and stakeholders.

One of the outputs of a risk evaluation is a prioritised list of risks for further action. The prioritisation tools must be logical, documented, and based on likelihood and consequence. In deciding whether and with what priority to treat a risk, the level of risk, uncertainties in the analysis, the views of communities and stakeholders and perceptions of risk should all be considered.

Importantly, the level of confidence in the evaluation should be discussed. The level of confidence will depend on the quality of analysis. For example, the information used and the type of evaluation (desk-top or full investigation) will greatly impact the overall quality of the evaluation and prioritisation processes.

The implications of prioritisation and the level of confidence associated with them should be made clear to stakeholders and communities.

8.2 Assurance Indicators and Typical Evidence

- Likelihood and consequence have been used to undertake the evaluation.

  Typical Evidence: *Documentation of the process.*

- Risks have been subjected to the prioritisation tools and the results documented.

  Typical Evidence: *Documentation or databases of the application of the prioritisation tools.*

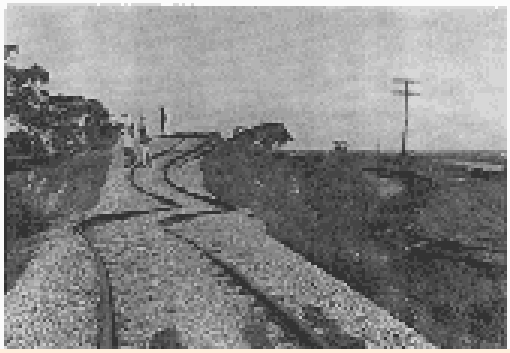
- Risk acceptability criteria have been reviewed and consultation has occurred about priorities for treatment.

  Typical Evidence: *Documentation outlining the risk acceptability criteria, the decision making process, the acceptable and unacceptable risks. Documentation*

of meetings with stakeholders and communities with regard to decisions about risk acceptability and priorities. Legislation / operating licences etc.

- Risk statements are in place with a monitoring and review process established to ensure they remain current. These risk statements describe consequences, vulnerability, likelihood, risk levels, confidence limits, and priorities.

  Typical Evidence: *Risk statements describing risks and their priorities contained in a risk registry.*

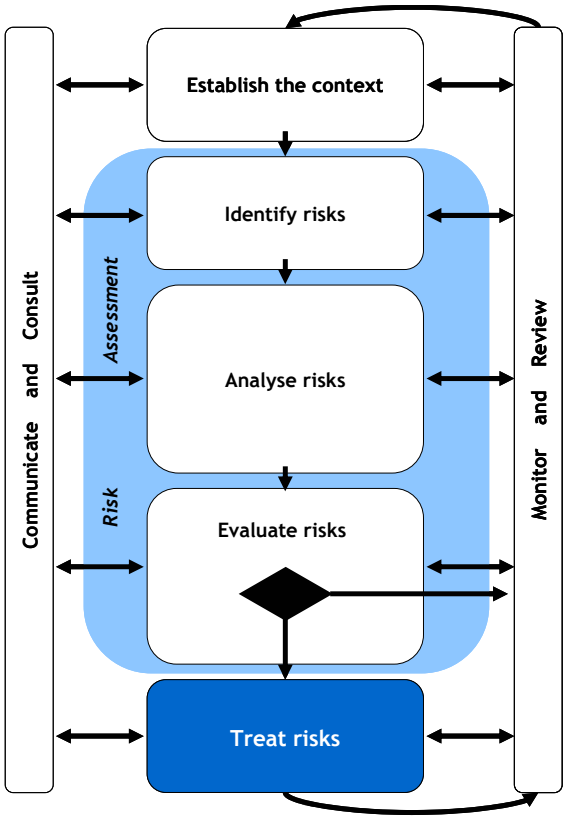


Meckering Earthquake

Western Australia
Month, Year
Text text text text text text text text text

9.0 Treat Risks

9.1 General



The purpose of treating risks is to reduce risks by:

- modifying the source of risk,
- improving the robustness of infrastructure, and/or
- reducing the vulnerability of stakeholders, the community and the environment as well as enhancing their resilience.

Risk treatment also considers how residual risks will be shared and paid for.

Options for risk treatment include

- Reducing the consequences and/or likelihood of an event by addressing the source of risk;
- Implementing engineering design or administrative arrangements to reduce the consequences or likelihood of critical infrastructure failure (given an existing source of risk);
- Adjusting engineering or administrative processes to improve the robustness of critical infrastructure (ie its ability to withstand impact and to restore services and facilities);
- Duplicating or substituting critical infrastructure services;
- Reducing the susceptibility of stakeholders, the community and the environment to critical infrastructure loss or improving their resilience;
- Sharing residual risk so it is borne by those most able to cope;
- Risk financing through insurance or other means *[this is outside the scope of this document]*; and
- Arranging alternatives to critical infrastructure that supplies the community's and stakeholders' critical needs

For critical infrastructure, practical engineering or structural modification for extreme risk events are the best risk treatments. They are most cost effectively addressed during the design, planning and commissioning phases as part of the infrastructure's initial risk assessment.

9.2 Choosing the Risk Treatments

It will usually be neither economical nor possible to implement all possible risk treatments. It is necessary to choose, prioritise and implement the most appropriate mix of risk treatments. Complicating factors such as legal, social, political and economic considerations also exist.

Care should be taken to ensure that in reducing one risk others are not inadvertently increased, or even created.

There are a number of ways of thinking about risk treatments. They may be:

- expected to include a mix of actions and activities focussed on maintaining services and facilities to the community during extreme risk events.
- defined for each component / element / aspect of an emergency including prevention, preparation, response and recovery.

Other ways of thinking about risk treatment are encouraged. For example, it may be possible to categorise risk treatments into those that address the susceptibility and resilience of stakeholders and communities, and those that address the robustness of critical infrastructure.

It is wise to be flexible and consult broadly with the various stakeholders and communities as well as peers and ERM specialists. In some cases the more innovative treatments may be less costly and more effective.

Each risk treatment should be considered in terms of (1) the priorities established during the evaluation, and (2) the objectives of stakeholders and the community defined while establishing the context. Those treatments rated as the most appropriate with the highest priority should be implemented.

Table-top and operational exercises may be employed to test and assure the effectiveness of treatment measures.

Risk treatment plans need to be worked through to refine details and to document:

- who is going to do what,
- where resources will be found,
- how the chosen treatments will be implemented,
- agreed responsibilities and schedules,
- the expected outcome of treatments,
- budgeting and performance measures, and
- the monitoring and review process to be used.

Table 6. Some criteria for assessing risk treatments[10]

Criteria	Questions
Administrative efficiency	Is it easily administered? or will its application be neglected because of administration difficulty or lack of expertise?
Compatibility	How compatible is this option with others that may be adopted?
Continuity of effects	Will the effects of this option be continuous or short term?
Cost / Efficiency	Is it cost-effective? Could results be had by cheaper means?
Effects on stakeholders and communities	Are reactions to this option likely to be adverse or positive?
Effects on the economy	What will be the economic impacts of this option?
Effects on the environment	What will be the environmental impacts of this option?
Equity	Do those responsible for creating the risk pay for its reduction? When the risk is not man-made, is the cost fairly distributed?
Individual freedom	Does this option deny basic rights?
Jurisdictional authority	Does this level of Government have the authority to apply this option? If not, can higher levels be encouraged to do so?
Leverage	Will this option lead to further risk-reducing actions by others?
Political acceptability	Is it likely to be endorsed by the relevant governments?
Latent Risks	What are the latent risks and how can they be managed?
Risk creation	Will this option itself introduce new risks?
Risk reduction potential	What proportion of the potential losses will this option prevent?
Timing	Will the beneficial effects of this option be quickly realised?

10 Adapted from Foster, H. D. (1980*) Disaster planning,* Springer-Veriag New York Inc.

9.3 Suggested Risk Treatments

A range of risk treatments may be available. These may address resilience or robustness. Depending upon the context risk treatments may be equally important to the resilience of the community and the robustness of the infrastructure.

Table 7. Documentation of risk treatment impact

Example risk treatments	To address …	
	Community resilience	Infrastructure robustness
Awareness and vigilance of infrastructure staff	Secondary	Primary
Community consultation, awareness, and preparation	Primary	Secondary
Engineering options	Secondary	Primary
Monitoring and review	Primary	Primary
Resource management	Primary	Primary
Security and surveillance	Secondary	Primary
Community capability and self-sufficiency	Primary	Secondary

Risk treatments may then be further categorised as illustrated in Table 6.

Table 8. Categorisation of Risk Treatments

Treatments	Prevention Mitigation	Preparedness	Response	Recovery
Awareness and vigilance	General staff training include ERM issues Implementing management controls Implementing incident reporting systems	Specific ERM training Leadership training Preparing response plans	Developing relationships	Debriefing and review
Communi-cation and consultation	Community and stakeholder awareness raising and briefing Liaising with the media Broad awareness raising and consultation	Engaging stakeholders and communities in risk assessments, drills and scenario testing Briefing media and preparing media plans around possible scenarios	Communicating effectively with stakeholders, communities and media Implementing media strategy, such as providing media access to command centre	Debriefing stakeholders and communities Extracting lessons learned Reporting on incident to stakeholders and communities
Engineering options	Designing features to minimise risk Reviewing design standards Designing processes consider emergency risks	Modifying or adding / supplementing infrastructure to reduce risk	Implementing emergency repairs and coping mechanisms, including substitute services	Restoring infrastructure and, where necessary, redesigning
Monitoring and review	Reviewing ERM process and risk treatments Monitoring to detect problems early Assessing assurance indicator achievement	Monitoring and reviewing state of preparedness	Monitoring and reviewing emergency response progress	Monitoring and reviewing recovery progress and organisational performance
Resource management	Assigning necessary resources to deal with Emergency Risk Management Evaluating investment in prevention vs response	Conducting drills and scenario exercises involving stakeholders, communities, staff, contractors, and consultants Ensuring contractor agreements include catastrophe action clauses	Implementing emergency command structure Deploying resources and implementing plans	Mobilising resources Providing supplementary crews for relief
Security and surveillance	Implementing physical security, surveillance and monitoring system Identifying staff, contractors, etc.	Testing security and surveillance systems. Conducting drills and tests	Deploying supporting surveillance and physical security	Conducting performance reviews of security and surveillance systems
Community capability and self reliance	Develop alternative supplies for needs	Build capacity in the community	Community assistance with emergency	Managed demand and reduced service expectations

The following discussion highlights some of the issues that each risk treatment may present.

Awareness and vigilance

By engaging stakeholders and communities, internal and external to the organisation, awareness of risks can be increased, and stakeholders and communities can be empowered to be vigilant.

Such risk treatments imply that appropriate technical advice is used, comprehensive competency and risk assessments of staff and contractors are conducted, and that appropriate processes are followed.

Management controls can be established to reduce the likelihood or consequences of a variety of risks. For example, checks and rechecks associated with received chemicals such as those used in water treatment. That is, a risk treatment option employed may be one which confirms that the chemical ordered is the one received and used.

When dealing with extreme risk events, the executive decision makers of the organisation will be involved. It is common that they are not involved with day-to-day ERM activities of lesser consequence, and as a result may be least prepared for the operational requirements of dealing with an event. Awareness training must address these issues.

It should also be recognised that contractors and consultants may have broader responsibility to provide expertise during extreme risk events than the specific wording of their contracts.

A variety of plans and strategies should be developed to educate, and in some cases train, stakeholders and communities with respect to the mode and impact of extreme risk events. These plans may address issues associated with mutual aid and service or facility shedding and restoration priorities.

Communication and consultation

A variety of plans and strategies should be developed for communication and consultation. These could involve tools such as consultative committees and media strategies.

The use of scenario exercises and drills provides an excellent mechanism for communication and consultation. They further develop partnerships and relationships and allow testing of risk treatments.

Debriefing is a powerful tool for improving ERM. Plans, and trained staff, should be available to conduct and analyse outputs from ERM debriefs.

Engineering options

Infrastructure can often be manipulated with engineering or procedural controls, e.g. electricity networks can manipulate load, gas networks can use en-route storage, telecommunication providers can shed or re-route congestion. A variety of plans may be developed that outline the ways that infrastructure can be configured to reduce the likelihood and consequences of extreme risk events.

Risk treatments may also consider options such as substitution,

improvement or redesign. This could include aspects such as increasing redundancy, designing alternative delivery mechanisms, or simply enhancing facilities.

A variety of plans may be developed that outline the ways that an organisation can begin to provide its critical infrastructure service or facility in the event of significant or critical asset loss. This may involve actions other than repairs to the existing infrastructure. e.g. It may include the provision of community watering points if water reticulation infrastructure is not available; or include the provision of wireless communications if PSTN networks are unavailable etc.

A variety of plans may be developed that outline the ways that infrastructure can be repaired or recovered. These plans may consider elements of mutual aid whereby prior arrangements are made with others in the sector for sharing critical spare components, expertise or resources etc.

Monitoring and review

A variety of plans and strategies may be developed for monitoring and review. These could involve tools such as peer group review or third party audit. Communication and monitoring activities relating to ERM across a sector, within a State, or more widely, can be useful in determining benchmarks that are likely to be considered post-event.

Resource management

During extreme risk events others may have control of the organisation's resources. This may be the case when a Responsible Officer or other assignment of authority is invoked by way of legislative process or prior arrangement.

If legislative processes are not in place, organisations should establish escalation procedures and protocols. These should outline roles and responsibilities. Importantly, they should also outline the changes to the roles and responsibilities as situations escalate and tools such as emergency services legislation are invoked. Of particular note is the need for cross-jurisdictional protocols where the potential exists for confusion, such as extreme risk flooding along State borders.

Mechanisms for deploying expertise should be considered. It should be remembered that in extreme risk events there may be competing demands for in-house expertise. It is also essential in ERM that controls are established to relieve people during emergencies.

The mobilisation and deployment of resources requires planning and attention to detail. Others may be prioritising the availability of resources such as transporters, helicopters, troops, expertise, and funds.

The legitimate activities of others may impact upon the organisation's ERM plans.

For example, if the organisation has army reservists, bushfire volunteers, etc., it is likely that in an extreme risk event these resources may be in use by others and be unavailable.

Security and surveillance	Much of Australia's critical infrastructure is geographically dispersed, and is often remote and exposed. Physical security and surveillance, with associated response, may be a possible risk treatment to a variety of sources of risk. Examples include remote monitoring, security patrols, as well as ingress and egress *[or access and departure]* controls.

9.4 Assurance Indicators and Typical Evidence

- A range of risk treatments have been generated.
  Typical Evidence: *Documentation of the risk treatments.*

- Risk treatments have been reviewed against the assessment criteria.
  Typical Evidence: *Documentation of the review process.*

- Risk treatments have undergone a prioritisation process.
  Typical Evidence: *Documentation of the prioritisation process including involvement and endorsement of the organisation's executive.*

- Risk treatment plans have been developed.
  Typical Evidence: *Plans exist and identify responsibilities, schedules, expected outcomes of treatments, budgeting, performance measures, and the review process to be set in place.*

- Risk treatment implementation schedules developed and endorsed by CEO / Board.
  Typical Evidence: *Project schedules, Gantt charts etc., documentation indicating executive endorsement.*

- Roles and responsibilities have been assigned to the risk treatments.
  Typical Evidence: *Responsibilities have been communicated and agreed.*

- Resource profiles have been developed for the risk treatments.
  Typical Evidence: *Documentation and databases indicating resource characteristics such as availability, substitutability, alternatives, priorities etc. are in place.*

- Agreed performance measures have been established to assess the risk treatments.
  Typical Evidence: *Documentation of performance measures and the means by which these will be collected, analysed and reported.*

- Relevant stakeholders and communities have been consulted when deciding between options and provided with details of the risk treatment plans.

  Typical Evidence: *Documentation of meetings, consultative groups, etc.*

- Risk treatments have been subjected to a validation process.

  Typical Evidence: *Evidence that scenarios or other appropriate proving and testing activities have been undertaken.*

Longford Gas Explosion

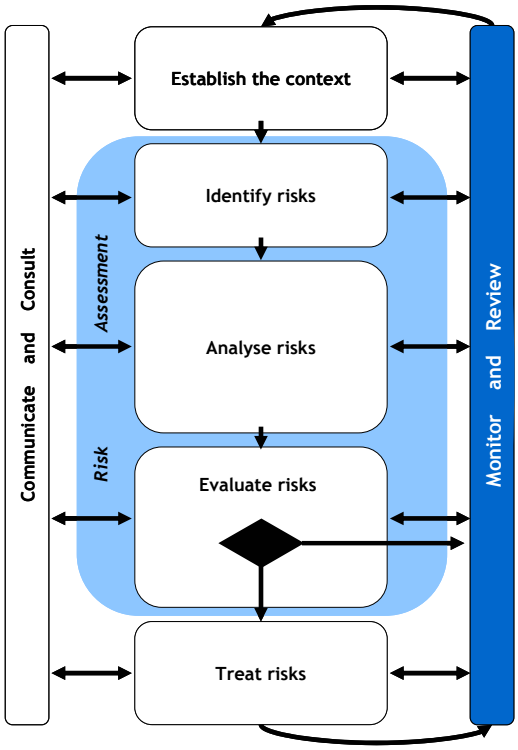
Victoria
Month, Year

The privately-owned gas installation in Longford, Victoria exploded. 1 life was lost and gas supplies to Victoria and NSW were lost for several weeks.

NSW declared a state of emergency.

10.0 Monitor and Review

10.1 Purpose



The purpose of monitoring and reviewing the ERM process is to ensure it remains relevant. It also helps to recognise and exploit opportunities to improve risk treatments. Review of ERM may be based on monitoring changes to:

- context;
- sources of risk;
- critical infrastructure;
- stakeholders;
- communities;
- environment; and
- events.

Risks, and the effectiveness of the risk treatments, need to be monitored to ensure changing circumstances do not alter priorities. Ongoing review of the context, such as environmental scanning[11], may be used.

New data may be produced either following incidents or through an increase in knowledge or experience elsewhere. This needs to be fed back into risk identification and risk assessment processes.

Once risk treatments have been recommended or implemented the new level of risk needs to be analysed and evaluated to see whether it is now acceptable or more needs to be done. Residual risks need to be monitored to ensure they remain acceptable

In ERM risk treatment plans include arrangements for responding to an emergency situation. Times of emergency often require people to act in ways outside their normal job role, and at a time of crisis when they may be overloaded with information and not thinking clearly. It is therefore important that emergency plans are practiced and tested to ensure that people are familiar with what they need to do and that the plans work in practice.

Any adverse event, involving the same or similar elements or issues to those being considered by the ERM study, should be evaluated to determine whether there are lessons to be learned.

Risk management is a process of continual improvement. It is a process that should be applied regularly and whenever situations change or there are new decisions to be made.

11 *Emergency Risk Management Applications Guide*, Emergency Management Australia (2000), p.23.

Documentation of ERM should be managed as part of a document control system and include details of assumptions, methods, data sources, reasons for decisions and recommendations and results. The documentation should provide[12]:

- assurance that the process has been conducted;
- evidence of a systematic approach;
- a record of risks;
- a means of retaining the organisation's knowledge;
- planning tools;
- accountability mechanisms and tools;
- opportunities for incremental improvement;
- training of personnel;
- an audit trail; and
- a means to share and communicate information.

Mt Stromlo Observatory

Canberra
February, 2003

The original telescope at the Mt Stromlo Observatroy was lost to bushfire in the Canberra blazes of 2003.

10.2 Assurance Indicators and Typical Evidence

- The context of the ERM and the plans developed from it is regularly reviewed to account for changes in circumstances.

  Typical Evidence: *Review documents regularly re consultation.*

- Risks are monitored to see if they change and to verify risk assessments.

  Typical Evidence: *Recent data concerning risks, risk statements that are regularly updated and reviewed.*

- Risk treatments are monitored for effectiveness.

  Typical Evidence: *Review procedures specified in risk treatment plans are carried out. Current and relevant statements concerning the effectiveness of treatment.*

- Emergency plans are tested, reviewed and improved.

  Typical Evidence: *Debriefing documents from regular desk-top or other exercises. Plans indicating dates reviewed.*

[12] Adapted from Standards Australia (1999) AS/NZS 4360:1999 *Risk Management.*

- The ERM project is subject to routine audit.

  Typical Evidence: *Audit schedule, results etc.*

- A system is established to assimilate knowledge and experience from other emergency events (internal and external), and from modelling and analysis carried out elsewhere.

  Typical Evidence: *Evidence that management seeks, records, shares and applies new knowledge. Incremental improvement techniques etc. have been used.*

- Regular progress and status reports are provided to the organisation's executive.

  Typical Evidence: *Executive minutes, project progress reports etc.*

- A documentation control system is established and operating.

  Typical Evidence: *Quality management / file system, archive and back-up systems, project control files etc. are in place.*

APPENDIX A – ASSURANCE SUMMARY

The systematic and critical examination of ERM provides a tool for highlighting areas of vulnerability and determining degree-of-readiness.

Over fifty (50) assurance indicators are provided to allow the emergency risk manager to qualitatively assess their degree-of-readiness for extreme risk events.

It is recognised that organisations involved with critical infrastructure vary considerably in terms of size, structure, resources and sources of risk. This handbook suggests a range of evidence that is generic and indicative. The evidence should be used in conjunction with the content of the handbook to ensure that the elements of ERM have been addressed.

The assurance indicators may be used to provide an assessment of the current state of emergency risk management or to identify broad areas of concern. Importantly, they may prompt for other approaches and challenge established priorities.

From a corporate governance perspective, a systematic and critical examination demonstrates commitment to ERM and provides evidence that systems are in place and that a positive approach is employed to evaluate performance.

Assurance processes, including audit, can be implemented using a variety of systems or techniques. Internal, peer or external auditors may be used.

Getting Started

- Organisational policies for ERM have been proclaimed.
- An ERM framework has been established.
- An ERM Committee has been identified and established.
- Required expertise and training needs have been considered
- An appropriate project management structure to develop ERM, and a process for continual improvement of the process, is established.

Communication and Consultation

- A communication and consultation strategy exists.
- Communication and consultation protocols have been developed and implemented with the participation of stakeholders and communities.
- Stakeholders and communities have been engaged in the development of the communication and consultation strategy and had input to ERM.
- Stakeholder and community views are monitored and where necessary changes addressed.
- Media spokespeople have been identified and trained.
- Stakeholder and community liaison officers have been identified and trained.

- Establish Context
- Stakeholders and communities have been identified, characterised, and engaged.
- Objectives of the organisation the community and other stakeholders in the context of an extreme risk event having occurred have been defined.
- Stakeholder and community expectations and perceptions have been recognised.
- Inter-relationships have been identified and communication channels established.
- The legislative context has been reviewed particularly in relation to criteria for acceptable risk.
- Risk evaluation criteria are available.
- Risk evaluation criteria have been reviewed throughout the ERM process.
- Prioritisation tools, such as ranking systems, have been developed and endorsed by the CEO / Board of the organisation.

NorthEast Floods

Victoria
1993

Highways were cut, stranding supply vehicles during the unseasonal floods in 1993.

Identify Risks

- The sources of risk have been identified and described.
- The communities have been identified and described.
- The environments have been identified and described.
- The vulnerability of the identified communities have been scoped.
- The vulnerability of the identified environments has been scoped.
- The effect of sources of risk on critical infrastructure has been identified.
- The vulnerability of critical infrastructure has been described.
- Risk statements have been generated.
- Risk evaluation criteria have been revisited.
- Stakeholders and communities have been involved in the identification of risks.
- Monitoring and review processes have been established to capture future sources of risk.

Analyse Risks

- Critical infrastructure interdependencies have been identified and described.
- Physical resource availability has been identified and described.
- Enabling resources have been identified and described.
- Scenarios have been explored considering a range of sources of risk and the vulnerabilities of critical infrastructure and of stakeholders and the community
- Consequences have been explored and described using data and quantitative methods where appropriate.
- Estimates of likelihood of different consequences have been made
- Risk statements have been expanded to include information on likelihood and consequences and where appropriate, a level of risk
- The views of stakeholders and communities have been included in the analysis and the results discussed with them.
- The outcome of analyses have been verified where possible.

Evaluate Risks

- Likelihood and consequence have been used to undertake the evaluation.
- Risks have been subjected to the prioritisation tools and the results documented.
- Risk acceptability criteria have been reviewed and consultation has occurred about priorities for treatment.
- Risk statements describing consequences, vulnerability, likelihood, risk levels, confidence limits, and priorities are in place with a monitoring and review process established to ensure they remain current.

Treat Risks

- A range of risk treatments have been generated.
- Risk treatments have been reviewed against the assessment criteria.
- Risk treatments have undergone a prioritisation process.
- Risk treatment plans have been developed.
- Risk treatment implementation schedules developed and endorsed by CEO / Board.
- Roles and responsibilities have been assigned to the risk treatments.
- Resource profiles have been developed for the risk treatments.
- Agreed performance measures have been established to assess the risk treatments.
- Relevant stakeholders and communities have been consulted when deciding between options and provided with details of the risk treatment plans.
- Risk treatments have been subjected to a validation process.

Monitor and Review

- The context of the ERM and the plans developed from it is regularly reviewed to account for changes in circumstances.
- Risks are monitored to see if they change and to verify risk assessments.
- Risk treatments are monitored for effectiveness.
- Emergency plans are tested, reviewed and improved.
- The ERM project is subject to routine audit.
- A system is established to assimilate knowledge and experience from other emergency events (internal and external), and from modelling and analysis carried out elsewhere.
- Regular progress and status reports are provided to the organisation's executive.
- A documentation control system is established and operating.