CRITICAL INFRASTRUCTURE EMERGENCY RISK MANAGEMENT AND ASSURANCE

Handbook

January 2003

EMERGENCY
MANAGEMENT
AUSTRALIA

www.ema.gov.au

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

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 Application Guide*. The National Emergency Management Committee, Australia's peak emergency management body, endorsed that guide in October 1998.[2]

In November 2002, a EMA sponsored ERM workshop[3] expressed the need for a handbook that complimented the standard and applications guide. Practitioners dealing with critical infrastructure noted that their degree-of-readiness to meet the challenges presented by catastrophic events was dependent upon addressing both internal sources of risks, as well as the sources of risk associated with infrastructure interdependencies and externalities.

The materials for this handbook are based on the outcomes of the 2002 workshop and the content of the *Emergency Risk Management Application Guide.* The handbook is an additional resource and will be continually refined to become a repository of collective knowledge and wisdom of the emergency risk managers in the infrastructure sector.

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 following organisations were represented on the Working Group:

Agility Management (AGL)
AlintaGas
Aust. Social & Ethical Accountability Centre
Australian National Audit Office
Australian Water Association
Brisbane Water
Cardno MBK Pty Ltd
City West Water VIC
Country Energy NSW
Dept. Natural Resources & Environment VIC
Emergency Management Australia
EnergyAustralia
Energy SA
Ergon Energy
Far North District Council NZ
Four C's Consulting
Integral Energy
Marsh Pty Ltd
Melbourne Water Corporation
NSW Dept. of Public Works and Services
NSW Police
NSW Critical Infrastructure Review Group
NT Power Water
Office of Energy QLD
Powerlink QLD
Res Eng (Australia) Pty Ltd
SA Dept. of Administrative Services
SA Water
Santos Ltd
Sydney Catchment Authority
Sydney Water
TAS State Emergency Service
Telstra
United Energy Ltd
VIC Office of Gas Safety
VIC Workcover Authority
Water Corporation WA
Water Services Australia
Western Power Corporation
Yarra Valley Water VIC

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 the emergency risk manager to qualitatively assess their degree-of-readiness for catastrophic 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, an event that extends an organisation beyond routine processes.

Environment

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

ERM - Emergency Risk Management

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

Enabling Resource

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

Essential Service

An indispensable supply or activity. The various Australian jurisdictions have various 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 it does not become an emergency.

Recovery

Measures supporting individuals, communities and organisations in the reconstruction or restoration of critical infrastructure, emotional, economic and physical well being.

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 after sustaining loss. 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 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 risks, communities and the environment.

Risk acceptance

An informed decision to accept a particular residual risk.

Risk analysis

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

Risk avoidance

An informed decision to 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

A selective 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 treatment

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

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 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. *e.g.*, 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 environment to consequences of events.

Contents

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 appropriately qualified and experienced emergency risk managers are the audience and that these managers have an extensive 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 during risk assessment of critical infrastructure as having **catastrophic** consequences. Catastrophic consequences depend on context, what is catastrophic 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 very different way to normal, there is a need for non routine activity.

Catastrophic 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;
- 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.

What happened in October 1970 that took 35 lives?

In September 1975, 13 people died in an accident. Would you be ready?

January 1977, 83 dead - 213 injured. How would you manage?

Dec 1989, 13 dead - approx 160 injured. Could you deliver your critical infrastructure services or facilities?

1.2 Benefits

ERM is of considerable value to stakeholders and communities. Planning establishes dialogue, personal networks and relationships between a wide-range of individuals and organisations. Proving and testing of plans further develops these relationships and creates trust and confidence.

Participation is the first step towards developing partnerships and their supporting relationships. 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.

Communication and consultation, combined with monitoring and review, provide the frameworks for improving stakeholders and communities abilities to deal with uncertainty and latent risk. These management actions are also critical to successful corporate governance and identifying and meeting the needs of communities reliant upon critical infrastructure.

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 context is often not able to be properly determined until a variety of sources of risk and draft risk treatments have been fully explored. The context may also change rapidly, based on changes in information or circumstance.

Fifty (50) assurance indicators[7] are provided to allow the emergency risk manager to qualitatively assess their degree-of-readiness for catastrophic 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.

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.

Can you answer yes to these questions?:

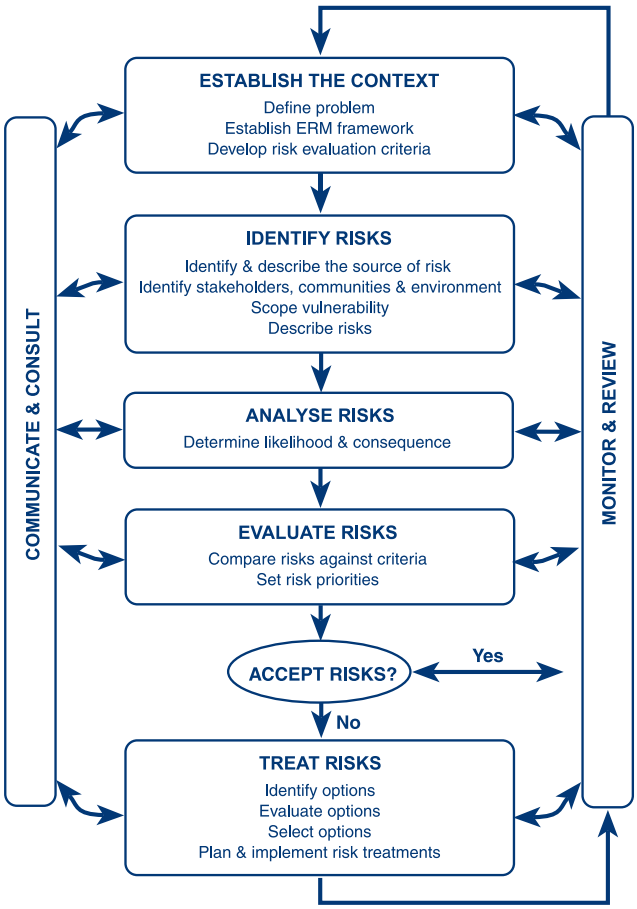
- Does your ERM address the risk posed by external factors?
- Do you have working relationships with government & emergency services?
- Do you have mutual support arrangements with others in your sector?
- Would your sector's emergency response be effective?

Have you established agreed protocols for recovery of your critical infrastructure services or facilities?

2.0 ERM Overview

2.1 The ERM Process Elements

The main elements of the emergency risk management process are:



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.

2.2 ERM Terms

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

Establish the context.

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

Review the levels of acceptable risk using tools such as consultative groups, and develop risk evaluation criteria. Where legislation, operating licences or similar instruments define the level of risk, review and modify these if required with respect to 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 risk associated with the problem by determining the likelihood and consequence of the identified risks.

Evaluate risks.

Compare risks against risk evaluation criteria, prioritise the risks and decide on risk acceptability.

Treat risks.

Identify and evaluate the treatments. Respond to the level of risk by deciding which source of risk, stakeholders, communities or environment can be addressed, either by increasing resilience or robustness, to reduce risk. Model changes to obtain the new level of risk. Select treatments, plan and implement.

Communication and consultation.

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 catastrophic events communication and consultation is considered extremely important. Communication and consultation develop resilience amongst stakeholders and communities and will be invaluable in terms of regaining control of critical infrastructure during catastrophic events.

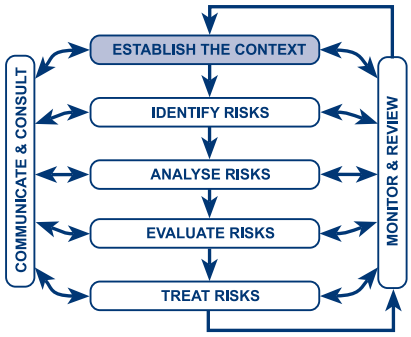
Monitor and review.

Systems that monitor and review risk, and its management, must be established and maintained. Latent and residual risk are ever-present. ERM must be on-going to ensure that change and uncertainty can be accommodated.

Documentation.

Appropriate documentation should be maintained at all stages to retain knowledge and satisfy audit requirements.

3.0 Establish the Context



3.1 Engagement

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 a technical or political process - it is also a social process.

There may be great diversity of opinion on the actual risks and their various sources, given different perceptions, knowledge and experience.

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 a catastrophic event. The inability to deliver the service or facility may be considered to be a loss-of-control. It may come in many forms including loss of operational control, loss of access, inability to maintain quality, loss of assets or loss of jurisdictional authority. Regaining the ability to deliver the service or facility becomes the primary concern of the critical infrastructure operator.

Loss-of-control may be partially compensated by the degree-of-resilience of the various stakeholders and communities. The degree-of-resilience will be greatly dependent on the effectiveness of prior engagement, particularly if alternative delivery systems are deployed with which they have had little or no experience.

Regaining control may include recovery of the infrastructure, or it may include deploying alternatives, or a combination of both, to ensure that the critical infrastructure service or facility is provided.

Two primary groups may be identified for establishing the context: those involved with addressing the resilience of the stakeholders and communities; and those involved with regaining the ability to deliver the service or facility. Those that contribute most to improving resilience and regaining control should be afforded priority. The following is suggested:

To address …	**Suggested priority 1**	**Suggested priority 2**
Stakeholders and communities resilience.	local communities and media business and industry safety providers local authorities/government agencies residential property owners direct and indirect customers local representatives hospitals/medical practitioners welfare	regional communities cyber communities aid providers non-government organisations investment property owners welfare and Church groups shareholders
Regaining control. Restoring the ability to deliver the critical infrastructure service or facility	energy (electricity, gas, etc.) water & sewage telecommunications transport emergency services personnel unions decision makers key suppliers	regulators insurers legal advisors auditors peak industry bodies professional advisors internal experts intelligence organisations

3.2 Evaluation Criteria

In relation to critical infrastructure, evaluation criteria and levels of acceptable risk may be prescribed through legislation, operating licence or other statutory instrument.

Tools such as consultative groups can be used to help develop risk evaluation criteria and levels of acceptable risk if they are not prescribed. Such groups 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 operates.

When developing risk treatments for catastrophic events it is important to consider the potential for severe adverse effects on the physical, social, economic or environmental 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. In particular for critical infrastructure, specific evaluation criteria may need to be developed that correspond to specific sources of risk or anticipated risk treatments. For example, in the case where a risk treatment called 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

3.3 Assurance Indicators and Typical Evidence

- Organisational policies for ERM have been proclaimed.

  Typical Evidence: Policy documentation endorsed by the CEO/Board. 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.

- An appropriate project management structure to develop ERM, and a process for continual improvement of 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.

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

  Typical Evidence: Stakeholders and communities registers/databases containing contact details, meeting schedules etc. Minutes of meetings and associated action sheets/files. Documentation outlining rationale for engagement.

- 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. are in place and operational, reaching all levels in the organisation. The existence of appropriate committees, media strategies, stakeholders and communities groups, supporting structures, etc.

- Stakeholders and communities expectation and perceptions have been recognised.

  Typical Evidence: Records of public meetings, surveys etc. are available. Documentation indicating that demographic or other data has been considered. Review of legislation, operating licences, statutory instruments etc.

- Knowledge of what is unacceptable to stakeholders and communities.

  Typical Evidence: Documentation indicating 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. Documentation that a confirmation process would be established during an event.

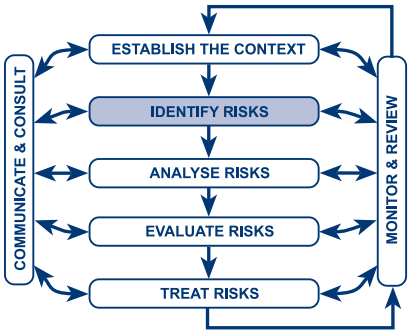
- Risk evaluation criteria are available.

  Typical Evidence: Documentation indicating that technical, economic, legal, social, humanitarian or other criteria as determined by the organisation with regard to stakeholders and communities input have been developed.

- 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 and project management minutes etc.

4.0 Identify risks



4.1 Sources of Risk

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 and interaction of the sources of risk, the stakeholders and communities, and the environment.

A source of risk presents the potential for loss or harm to the stakeholders, communities and/or environment. Sources of risk may come from natural, technological, biological or civil/political origins. The following list of sources of risk[8] may be useful to the ERM process for critical infrastructure.

Primary	May also consider …
aeronautical	carcinogens/mutagens/pathogens
biological	desertification
chemical	drought
civil disturbance/riot	economic recession/depression
electronic/cyber attack	electromagnetic radiation
explosion/incendiary/fire (residential, industrial, bush, etc.)	epidemic (human, animal, plant)
hazardous materials	erosion (soil, coastal)
human acts (terrorism/vandalism/wilful damage/retribution/sabotage)	fog
industrial accident (chemical, mine, plant, smelter etc.)	frost/extreme cold management/ organisational failure
infrastructure failure (power, water, telco, gas, etc.)	plague (animal, human, insect, plant)
market failure	resource shortage/depletion
manipulation (deliberate or forced misuse of controls)	salinisation
pollution (chemical, oil, waste, etc.)	sea level rise
radiological/nuclear	space debris
seismic (earthquake, tsunami, volcano)	subsidence
slope failure (landslide, rock fall, mudflow)	supply chain failure
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 a catastrophic event, it is certain that a combination of a number and types of stakeholders, communities and environments will be impacted.

The ERM process for critical infrastructure should therefore identify and describe sources of risk in terms of spatial (geographic) distribution, temporal distribution (speed of onset, duration, etc.), intensity, and manageability.

The stakeholders and communities may be geographic groupings, shared experience groupings, sector based groupings, or function based groupings. Individuals may belong to several groupings.

The process of identifying and describing stakeholders and communities examines information including population size, spatial distribution, remoteness, prior experience or perception, degree of exposure, capacity, access to resources, and susceptibility or resilience.

Without detailed knowledge about the stakeholders, communities and environment, it is impossible to determine the elements at risk and to describe their vulnerability, and thus develop appropriate risk treatments. The following characteristics may be used as prompts:

Some stakeholders, communities & environmental characteristics

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

The environment is a set of conditions or influences that surround or interact with the stakeholders and communities and the sources of risk. Elements of environment may include the physical environment or the social environment. These have complex intra/ interactions.

The process of identifying and describing the environment examines information including the degree of mitigation or protection afforded to the stakeholders and communities as well as their susceptibility or resilience.

4.2 Scope Vulnerability

When determining vulnerability by establishing the capability of stakeholders, communities and the environment to anticipate, cope with, and recover from emergencies, it is important to consider the level of volatility and the potential rates of change that may exist.

Studies of vulnerability involve both quantitative and qualitative methods. A variety of models exist[9] to identify or describe the cumulative impact of risks and the causal relationship between them. Whatever the focus, (data, financial, information, resource, system, network, meeting, supply, etc.) risk will be present.

Understanding vulnerability means understanding the relationships of these risks and how they could combine to trigger or escalate an event. To gain a thorough understanding of the interactions between risks it may be necessary to identify and implement appropriate indicators or performance measures.

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	Robust, protected	Frail, exposed
Employment	Little 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

4.3 Describe Risks

Sources of risk identification concerns discovering what risks may impact stakeholders and communities through the inability of the critical infrastructure to deliver services and facilities.

It is not always straightforward as people may have different perceptions on what constitutes significant sources of risk. It is therefore important to engage the stakeholders and communities and consider:

- the impact of the loss of critical infrastructure services or facilities on stakeholders and communities;
- the possible extent of damage;
- alternative means of providing critical infrastructure services or facilities;
- the existence of risk management systems;
- the amount of time repairs would take; and,
- the cost of repairs.

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 National governments;
- mapping stakeholders, communities and environmental characteristics; and,
- using groups (internal and external) to identify possible sources of risk.

Four primary characteristics are considered in relation to catastrophic events:

1. spatial distribution (the area that a source of risk may impact);
2. temporal distribution (warning time, duration, time of day/week/year);
3. intensity (how big, fast, powerful); and,
4. 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 means 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.

A systematic approach to describing risk, such as a risk matrix, may be used. The following hypothetical examples explore two scenarios, the first an electrical storm and the second a flood event.

In the first example, an electrical storm causes a transmission outage due to lightning discharge. The response to such an event would be routine, however at around the same time generation control is lost. The combination of these impact stability of the network. Ultimately a system restart is required which is not routine.

In the second example, a forecast and manageable flood event occurs. The response to such an event would be routine, however at around the same time a sewage escape occurs due to an unrelated failure. This triggers a range of health concerns. Before the flood peaks the telecommunications are lost and an evacuation is commenced. The situation is not routine.

Example of mapping source and element at risk

Source of risk	Element at risk – example stakeholders and communities (repeat for environment and other defined elements at risk)				
Electrical storm *Intensity/Impact*	Cyber	Precinct	District	Regional	State
Sub-station damage	✓	✓	×	×	×
+ transmission outage	✓	✓	✓	×	×
+ lost generation control	✓	✓	✓	✓	✓
+ lost frequency control	✓	✓	✓	✓	✓
= system restart	✓	✓	✓	✓	✓
Flooding *Intensity/Impact*	Cyber	Precinct	District	Regional	State
Pump-station damage	×	✓	×	×	×
+ sewage escape	✓	✓	✓	×	×
+ health incident	×	✓	✓	✓	×
+ telco outage	✓	✓	✓	✓	×
= evacuation	×	✓	✓	✓	✓
etc.					

SCENARIO ANALYSIS

What is the cause? What is the likely effect?

Scenario analysis can be used to determine cause-effect relationships for complex situations. Risk scenarios can describe source 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.

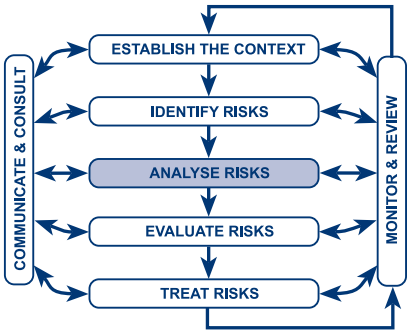
For example, failure to develop risk scenarios and address the individual elements of risk may be seen in the Piper Alpha oil and gas platform fire. In this case, failures in risk treatment occurred with:

- design that did not consider all risks (poor risk analysis);
- ignoring the negative results of a risk audit;
- failure of the 'permit to work' system;
- lack of briefing of incoming duty manager by outgoing duty manager;
- lack of training in fire and evacuation procedures;
- poor emergency process shut-down procedures; and,
- poor inter-platform communication protocols.

4.4 Assurance Indicators and Typical Evidence

- The sources of risk have been identified and described.
  Typical Evidence: Documentation or databases such as source of risk or risk registers.
- The communities have been identified and described.
  Typical Evidence: Documentation, supporting surveys, demographic information etc.
- The environments have been identified and described.
  Typical Evidence: Documentation of environmental factors, impact statements etc.
- The vulnerability of the identified communities has been scoped.
  Typical Evidence: Documentation indicating appropriate research and analysis of vulnerability in terms of the ability to cope with and recover from a catastrophic 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 a catastrophic event.
- Explanation of how the sources of risk have been analysed/classified.
  Typical Evidence: Documentation indicating review of sources of risk to critical infrastructure including qualitative description and the rational behind declaring a risk.
- Risk statements have been generated.
  Typical Evidence: Risk matrices or similar analysis tools such as databases etc.
- Risk evaluation criteria have been revisited.
  Typical Evidence: Minutes of meetings, action sheets, project documentation etc.
- The stakeholders and communities have been involved in the identification of risks.
  Typical Evidence: The presence of, and documentation for, consultative groups, public meetings, correspondence etc
- Monitoring and review processes have been established to capture future sources of risk.
  Typical Evidence: Quality/project management systems, project meetings, feedback protocols etc.

5.0 Analyse Risk



5.1 General

The purpose of analysing risks is to provide information to assist in the evaluation and treatment of risks. With respect to catastrophic events for critical infrastructure significant analysis is required in relation to:

- infrastructure interdependencies within and external to the organisation;
- physical resources availability, prioritisation and substitutability; and,
- enabling resource availability, prioritisation and substitutability.

Analysis will require considered and experienced judgments 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.

5.2 Determine Likelihood and Consequence

Predicted likelihood and expected consequences relate to the sources of risk associated with catastrophic events, however our experience of catastrophic events is usually limited. To overcome this, experienced emergency risk managers need to source a variety of information and apply a variety of techniques. To avoid biases 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; and
- peer reviews and audit.

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. Sources of risk can be described to enable the evaluation of the likely merit of risk treatments explored by the scenario.

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.

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 the determination of effective treatments.

5.3 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, substitutable equipment, supplies, chemicals, spare parts etc.

- Supporting resources have been identified and described.

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

- The level of risk has been assigned to the risk statements.

  Typical Evidence: Review of the risk statements.

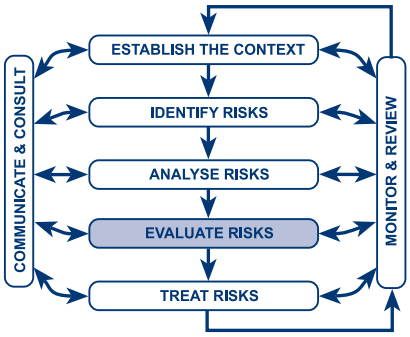
- The views of stakeholders and communities have been included in the analysis and the results discussed with them.

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

DERWENT RIVER TAS. January 1975

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

6.0 Evaluate Risks



6.1 General

The purpose of evaluating risks is to make judgements about their relative seriousness. These judgements will guide the emergency risk manager in terms of prioritisation.

Given limited resources, it is necessary to determine which risks will be treated.

The primary output of a risk evaluation is therefore a prioritised list of risks for further action. The prioritisation tools must be logical, documented and based on likelihood and consequence.

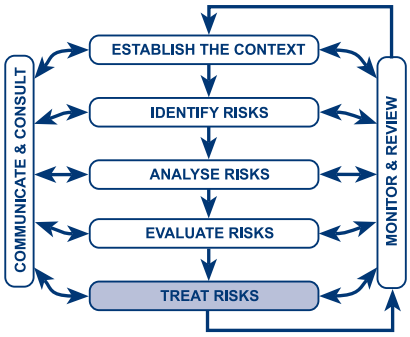
Importantly, the level of confidence in the evaluation should be discussed. The level of confidence will depend on the quality of analysis. For example, the information used and the type of evaluation (desk-top or full investigation) will greatly impact the overall quality of the evaluation and prioritisation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

Stakeholders and communities should be educated about the implications of prioritisation and the level of confidence associated with them.

6.2 Assurance Indicators and Typical Evidence

- Likelihood and consequence have been used to undertake the evaluation.
  Typical Evidence: Documentation of the process.
- 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.
- 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 developed with stakeholders and communities, or sourced from legislation or operating licence conditions. A review process exists.
  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 risk acceptability. Legislation/operating licences etc.
- Risk statements with assigned consequences, reflecting vulnerability, likelihood, risk levels, confidence limits, and priorities are in place with a monitoring and review process established to ensure they remain current.
  Typical Evidence: Risk statements contained in a risk registry with assigned responsibilities, treatments, mitigation strategies etc.

7.0 Treat Risks



7.1 Risk Treatment Criteria

The purpose of treating risks is to reduce the likelihood or consequences of an event.

For critical infrastructure there may be few practical engineering or structural risk treatments available for catastrophic events once the infrastructure has been commissioned.

Many of the structural risk treatments should be addressed as part of the infrastructure's initial risk assessment during the design, planning and commissioning phases.

As much of Australia's infrastructure is mature, and significantly geographically dispersed, risk treatments are likely to focus on operational and managerial solutions.

To implement all possible risk treatments is not cost-effective or even possible. 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 risks to others are not inadvertently increased. A number of assessment criteria for risk treatments are suggested below.

7.2 Choosing the Risk Treatments

There are a number of ways of thinking about risk treatments. These include:

- prevention, preparedness, response and recovery (PPRR);
- the 'hierarchy of control'[10]; and,
- standard treatments such as avoidance, reduction, sharing and acceptance.[11]

For critical infrastructure, the PPRR approach may be used. Other ways of thinking about risk treatment are encouraged. For example, it may be possible to categorise risk treatments into those that address the 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.

Each risk treatment should be considered in terms of the priorities established during the evaluation. Those treatments rated as the most appropriate with the highest priority should be implemented.

Risk treatment plans should document how the chosen treatments will be implemented. They should identify agreed responsibilities, schedules, the expected outcome of treatments, budgeting, performance measures, and the monitoring and review process.

Some criteria for assessing risk treatments[12]

Criteria	Questions
Administrative efficiency	Is it easily administered or will its application be neglected because of difficulty of administration 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 there likely to be adverse reactions to this option?
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 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 the option lead to further risk-reducing actions by others?
Political acceptability	Is it likely to be endorsed by the relevant governments?
Residual and Latent Risks	What are the residual and latent risks and how can they be managed?
Risk creation	Will this option itself introduce new risks?
Risk reduction potential	What proportion of the losses will this option prevent?
Timing	Will the beneficial effects of this option be quickly realised?

7.3 Suggested Risk Treatments

A range of risk treatments may be available. These may address resilience or robustness and include:

Example risk treatments	To address …	
	resilience	robustness
Awareness and vigilance	Primary	Secondary
Communication and consultation	Primary	Secondary
Engineering options	Secondary	Primary
Monitoring and review	Primary	Secondary
Resource management	Primary	Secondary
Security and surveillance	Secondary	Primary

These may then be further categorised as illustrated in the table below.

	Prevention Mitigation	Preparedness	Response	Recovery
Awareness and vigilance	General staff training include ERM issues. Management controls.	Specific ERM training. Leadership training.	Develop relationships.	Debriefing and review.
Communication and consultation	Community and stakeholder awareness raising and briefing. Media liaison.	Engage stakeholders and communities in risk assessments, drills and scenario testing. Brief media and prepare media plans around possible scenarios.	Communicate effectively with stakeholders, communities and media. Implement media strategy, such as providing media access to command centre.	Debrief stakeholders and communities. Extract lessons learned. Report on incident to stakeholders and communities.
Engineering options	Design features to minimise risk. Review design standards.	Modification or addition of infrastructure to reduce risk.	Emergency repairs and coping mechanisms, including substitute services.	Restoring infrastructure and, where necessary, redesigning.
Monitoring and review	Review ERM process and risk treatments.	Monitor and review state of preparedness.	Monitor and review progress of emergency response.	Monitor and review progress of recovery and organisational performance.
Resource management	Assign necessary resources to deal with ERM	Drills and scenario exercises involving stakeholders, communities, staff, contractors and consultants.	Implement emergency command structure. Deployment of resources and implementation of plans.	Mobilisation of resources. Supplementary crews for relief.
Security and surveillance	Physical security, surveillance and monitoring system. Identification of staff, contractors etc.	Testing security and surveillance systems. Drills and tests.	Deployment of supporting surveillance and physical security.	Performance review of security and surveillance systems.

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 proper 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 may be employed that confirms that the chemical ordered is that which is received and used in the subsequent treatment process.

When dealing with catastrophic 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 catastrophic 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 catastrophic 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 on-route storage, telecommunication providers can shed or re-route congestion. A variety of plans may be developed outlining the ways that infrastructure can be configured to reduce the likelihood and consequences of catastrophic 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 outlining the ways that organisation can begin to provide their critical infrastructure service or facility in the event of significant or critical asset loss. This may involve other actions aside from repairs to the existing infrastructure. *e.g.* It may include the provision of community watering points if water reticulation infrastructure is not available. It may include the provision of wireless communications if PSTN networks are unavailable etc.

A variety of plans may be developed outlining 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 the sharing of 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.

Resource management:

During catastrophic events others may have control of the organisation's resources. This may be the case with the invoking of a Responsible Officer or other assignment of authority 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 catastrophic flooding along State borders.

Mechanisms for deploying expertise should be considered. It should be remembered that in catastrophic 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, bush fire volunteers, *etc.*, it is likely that in a catastrophic event these resources may be utilised by others and be unavailable.

Security and surveillance:

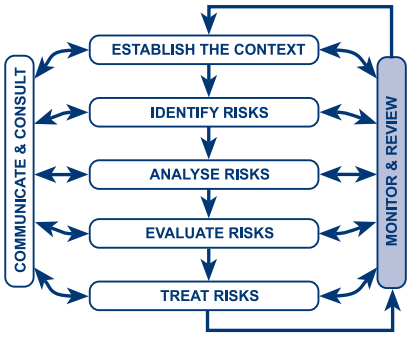
Much of Australia's critical infrastructure is geographically dispersed, often remote and exposed. Physical security and surveillance, with associated response, may be a possible risk treatment to a variety of sources of risk.

Examples include remote monitoring, security patrols, as well as ingress and access controls.

7.4 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 treatments implementation schedules developed and endorsed by CEO/Board.
  Typical Evidence: Project schedules, Gantt charts etc., documentation indicating executive endorsement.
- 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.
- 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 and provided details of the risk treatment plans.
  Typical Evidence: Documentation of meetings, consultative groups, etc.
- Risk treatments have been subjected to a proving or testing process.
  Typical Evidence: Evidence that scenarios or other appropriate proving and testing activities have been undertaken.

8.0 Monitor and Review



8.1 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;
- stakeholders;
- communities;
- environment; and
- events.

Importantly, risks and the effectiveness of the risk treatments need to be monitored to ensure changing circumstances do not alter priorities. Ongoing review, such as environmental scanning[13], may be used. Any event involving the same or similar elements or issues should be evaluated to determine whether there are lessons to be learned.

Documentation should be managed as part of a document control system and include assumptions, methods, data sources, and results. Documentation should provide[14]:

- 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.

8.2 Assurance Indicators and Typical Evidence

- Environmental scanning takes place on a regular basis.

  Typical Evidence: Access to media outlets, journals, conferences etc. have been developed and used. Evidence that review processes have been initiated.

- 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).

  Typical Evidence: Evidence that management reviews, incremental improvement techniques etc. have been used.

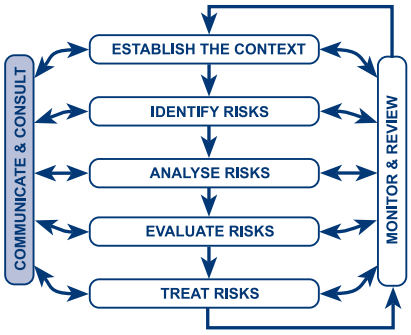
- Regular progress and status reports are provided to the organisation's executive.

  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.

9.0 Communication and Consultation



9.1 General

Communication and consultation are an important consideration at each step of the ERM process. It is important to develop a communication strategy that will engage stakeholders and communities at the earliest stage.

Effective communication and consultation is important 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.

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

Stakeholders and communities are likely to make judgments on the acceptability of a risk based on their beliefs, perceptions and ability to implement mitigation strategies. Critical infrastructure operators must therefore recognise that communication messages can become inconsistent. 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.

Since stakeholders and communities can have a significant impact on the decisions made, it is important that their perceptions of risk, as well as their perceptions of benefits, be identified and documented and the underlying reasons for them understood and addressed. For critical infrastructure operators confusion can arise when levels of risk are prescribed by operating licences but they 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);
- mode (radio, television, journals, person-to-person, consultative committee *etc.*);
- accessibility (language, readability, vision impaired, *etc.)*;
- sensitivities; (political correctness, empathy, social, *etc.*); and,
- boundaries (legal, political, social, technical, *etc.*).

COMMUNICATION

The expertise of the emergency risk manager is revealed through their ability to communicate. If the emergency risk manager is not able to communicate, problems will arise. Some of the common communication traps include:

- The application of inappropriate techniques 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.

The nature and timing of a catastrophic event will dictate many elements of a communication strategy. The following elements are suggested:

Pre event	Post event
Engage stakeholders and communities (incl. Community representatives, politicians, etc.)	Review stakeholders and communities views. Brief stakeholders and communities.
Provide basic emergency hints.	Monitor spokesperson's performance – beware of unintended messages.
Qualify guarantees in the case of emergencies.	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 ASAP, 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 stakeholders and communities 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
Develop regulator/jurisdiction protocols.	Implement regulator/jurisdiction protocols.

9.2 Assurance Indicators and Typical Evidence

- Communication and consultation strategy exists.

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

- Stakeholders and communities have been engaged in the development of the communication and consultation strategy.

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

- Stakeholders and communities views are monitored and where necessary changes addressed.

  Typical Evidence: Surveys, questionnaires, meetings etc.

- Media spokespeople have been identified and trained.

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

- Stakeholders and communities liaison officers have been identified and trained.

  Typical Evidence: Training records, responsibility charts etc.

APPENDIX A – Assurance Summary

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

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

It is recognised that organisations involved with critical infrastructure vary considerably in terms of size, structure, resources and sources of risk. The handbook suggests a range of evidence that is generic but 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.

Context

- Organisational policies for ERM have been proclaimed.
- An ERM framework has been established.
- An ERM Committee has been identified and established.
- An appropriate project management structure to develop ERM, and a process for continual improvement of the process, is established.
- Stakeholders and communities have been identified, prioritised and engaged.
- Communication and consultation protocols have been developed and implemented with the participation of stakeholders and communities.
- Stakeholders and communities expectation and perceptions have been recognised.
- Knowledge of what is unacceptable to stakeholders and communities.
- Risk evaluation criteria are available.
- Risk evaluation criteria have been reviewed throughout the ERM process.

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 has been scoped.
- The vulnerability of the identified environments has been scoped.

- Explanation of how the sources of risk have been analysed/classified.
- Risk statements have been generated.
- Risk evaluation criteria have been revisited.
- The 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.
- Supporting resources have been identified and described.
- The level of risk has been assigned to the risk statements.
- The views of stakeholders and communities have been included in the analysis and the results discussed with them.

Evaluate Risks

- Likelihood and consequence have been used to undertake the evaluation.
- Prioritisation tools, such as ranking systems, have been developed and endorsed by the CEO/Board of the organisation.
- Risks have been subjected to the prioritisation tools and the results documented.
- Risk acceptability criteria have been developed with stakeholders and communities, or sourced from legislation or operating licence conditions. A review process exists.
- Risk statements with assigned consequences, reflecting 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 treatments implementation schedules developed and endorsed by CEO/Board.
- Risk treatment plans have been developed.
- 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 and provided details of the risk treatment plans.
- Risk treatments have been subjected to a proving or testing process.

Monitoring and Review

- Environmental scanning takes place on a regular basis.
- The ERM project is subject to routine audit.
- A system is established to assimilate knowledge and experience from other emergency events (internal and external).
- Regular progress and status reports are provided to the organisation's executive.
- A documentation control system is established and operating.

Communication and Consultation

- Communication and consultation strategy exists.
- Stakeholders and communities have been engaged in the development of the communication and consultation strategy.
- Stakeholders and communities views are monitored and where necessary changes addressed.
- Media spokespeople have been identified and trained.
- Stakeholders and communities liaison officers have been identified and trained.

End Notes and References

[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*

[3] Anne-Marie Akle, Bruce Angus, Alexander Bailey, George Bawtree, Graham Begg, Ken Brown, Rodney Cade, Arthur Conomos, Chris Davis, Gordon Dojcinovic, Bevis Dutton, Mike Ebdon, Mark Fitzhardinge, Peter Fowler, Peter Garland, Carl Gibson, Jim Gifford, David Harris, Peal Heaton, Aneurin Hughes, Trevor Jenner, Paul Killeen, John Langford, Mark Lanham, Michael Lawry, Gavin Love, Clive Manley, Erik Maranik, Robert McIntyre, Damian McKenzie McHarg, David Morton, Darren Newton, Paul O'Connor, Des Pane, David Parsons, Siraj Perera, John Reid, Les Semple, Glenn Sheedy, Rod Stewart, Mike Tarrant, Aart ter Kuile, Joe Tomasi, Scott Vines, Peter Whelan, Ronald Whitelaw, Rod Wilkes, Christopher Yam, Constantine Zakis.

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

[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.*

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

[8] Adapted from *Emergency Risk Management Applications Guide*, Emergency Management Australia (2000).

[9] For example, the Delphi technique. Standards Australia (1999) *HB 143:1999 Guidelines for managing risk in the Australian and New Zealand public sector.*

[10] Standards Australia (1997) AS/NZS 4804:1997 *Occupational health and safety management systems-General guidelines on principles, systems and supporting techniques,* Homebush, Australia.

[11] See Standards Australia (1999) AS/NZS 4360:1999 *Risk Management.*

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

[13] *Emergency Risk Management Applications Guide*, Emergency Management Australia (2000), p.23.

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