

**Tasmanian Counter Terror Review
Team**

Critical Infrastructure Group

RISK MANAGEMENT PROCESS

**DRAFT GUIDANCE MANUAL FOR
INFRASTRUCTURE OPERATORS**

This document has been developed by the Tasmanian CT Review Team based on the work of the Victoria Police, acknowledgement is given for the use of their material.

January 2003

**RISK MANAGEMENT PROCESS
GUIDANCE MANUAL**

TABLE OF CONTENTS

INTRODUCTION..... 3

RISK MANAGEMENT DEFINED..... 3

RISK MANAGEMENT PROCESS 3

 STEP 1 – ESTABLISH THE CONTEXT 4

 STEP 2 - IDENTIFY RISKS 4

Table 1 Control Effectiveness..... 6

Table 2 Control Effectiveness Rating Table 6

 STEP 3 – ANALYSE RISKS 6

Table 3 Measures of Likelihood 7

Table 4 Measures of Consequence 7

 STEP 4 – EVALUATE RISKS 7

Table 5 Risk Evaluation Matrix..... 7

 STEP 5 - DETERMINE AND IMPLEMENT TREATMENT ACTION 8

 STEP 6 - MONITOR ACTION 8

 STEP 7 - COMMUNICATE AND CONSULT 9

FURTHER GUIDANCE 9

KEY TERMS..... 10

APPENDIX 1: RISK REGISTER TEMPLATES..... 11

 TABLE 1 GENERAL RISK IDENTIFICATION MATRIX 11

 TABLE 2 RISK REGISTER 12

 TABLE 3 RISK TREATMENT PLAN 12

Introduction

This manual is intended as a practical, step-by-step guide to assist readers gain an appreciation of risk management principles and assist in the preparation of risk management strategies for their areas of responsibility in Critical Infrastructure Protection. The process described in this manual accords with the Australian Standard for Risk Management (*AS/NZS4360:1999 Risk management*). The techniques defined in this document are designed specifically for internal risk management approaches, particularly those involving infrastructure. Specific comments on the process as it applies to counter-terrorism are provided in text boxes.

Risk Management Defined

Risk Management is a systematic action-oriented process of identifying, analysing, assessing, prioritising, treating and monitoring “risk events” that may prohibit an organisation from achieving its objectives and may adversely impact on the economic, effective or efficient delivery of its operations. These risks may have financial implications such as those associated with injuries to staff and other parties, damage and theft of equipment, or matters that expose an organisation to litigation. Financial risks are often insured, but there are also other less tangible risks that impact on the organisation's reputation such as the inability to effectively deliver services to clients. It is difficult to insure against these intangible risks and as a result other treatment strategies are needed.

The fundamental aim of a risk management approach is the early identification of potential problems to provide sufficient lead-time to avoid crisis situations. The consistent application of the Risk Management process across an organisation will provide assurance that all significant risks to the organisation are being addressed and that surprises are minimised. Through applying a systematic and critical examination technique, vulnerability may be identified and addressed.

Risk Management Process

This Risk Management Process is described as a series of 7 steps through which risks are identified and addressed, as described below:

- Step 1 Establish the context**, Set scene, determine functions/objectives, set evaluation criteria;
- Step 2 Identify risks**, identify/describe risks relating to the functions/objectives, identify vulnerability and interaction, identify the factors that cause these risks, including existing controls or strategies to address risks;
- Step 3 Analyse Risks**: Assess the probability and likely consequences of the risk after taking into consideration the effectiveness of current controls. This will ascertain the residual level of risk exposure;
- Step 4 Evaluate Risks**: Compare listed risks against criteria, set priorities, determine whether to avoid, treat or accept;
- Step 5 Treat risks**: determine options and implement action to treat the residual risk;
- Step 6 Monitor and review**: continually monitor the achievement of actions; and
- Step 7 Communicate and Consult**. Ensure feedback loops and key group input.

This risk management process is demonstrated in Figure 1.

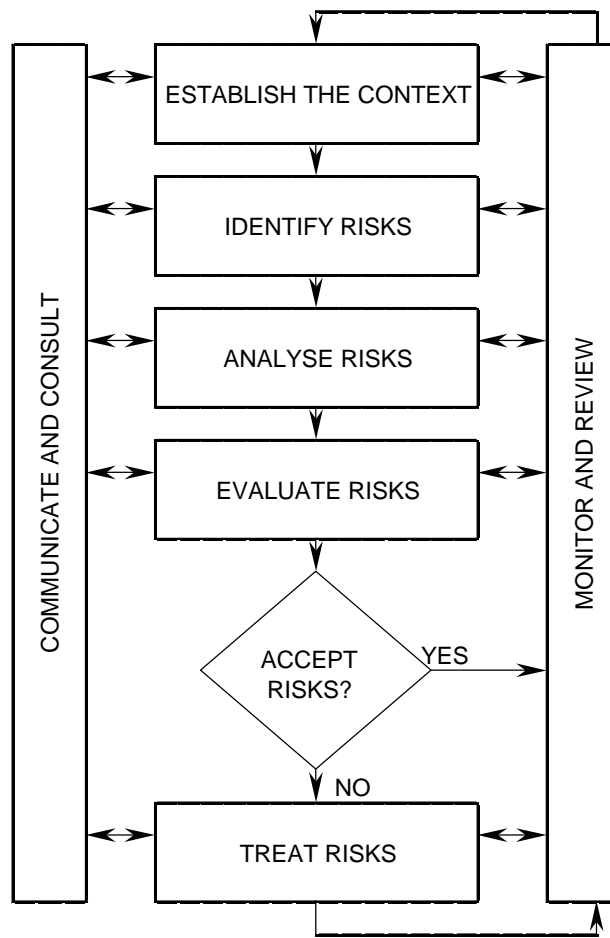


Figure 1 Risk Management Process

Appendix 1 provides an example of a risk register that reflects this process.

Step 1 – Establish the Context

Identify key objectives or functions

To establish the context, identify the function to be performed or the objective to be achieved. Ensure it is as concise and clear as possible otherwise the risk assessment will be difficult and inexact. Consider the stated functions and objectives of the organisation as found in strategic or business plans, organisational reports and other documents.

For critical infrastructure (CI), objectives will likely include the continued delivery of your primary customer service e.g. generation and transmission of electricity, as well as those defined about the retention of your staff, facilities, profits, reputation and assets.

Set evaluation criteria

Criteria need to be identified for your organisation that will be used as part of the evaluation. These include the thresholds for acceptable risk (if possible) as well as your descriptors for measures of consequence.

Step 2 - Identify risks

Determine sources of risk

Identify any inherent sources of risk related to the achievement of the stated function or objectives. Start by considering the following question:

“What internal and external issues or “sources of risk” can I identify that may adversely impact on the economic, effective and efficient operations of this organisation?”

Undertaking a SWOT analysis (Strengths, Weaknesses, Opportunities and Threats) may assist. This involves identifying the strengths and weaknesses of your organisation or facility (an internal focus) and determining the opportunities available and threats you may face (an external focus). This will also spell out the impact of the loss of the facility or service on the community, the extent of damage, alternative sources of supply, time to repair and costs of repairs.

It is important to be thorough so that the process also identifies the less obvious risks (i.e. if you fail to identify a risk, you cannot manage it.) This may require consultation with management and staff, clients, and other key internal and external stakeholders.

It is equally important to identify any related risks, as they will most likely affect the impact and probability of the risks involved. Risk relationships will also influence your choice of control i.e. whether you have the ability to influence or control

“Sources of Risk” for Terrorism could include: denial of service, hacking, hostage taking, explosion, bomb, chemical contamination, biological agent release, radiological release, sabotage, vandalism, fire, loss of key staff, assassination, lifeline disruption, fire, etc. Table 1 in Appendix 1 gives an example identification matrix.

Identify causal factors

Identify what factors would cause the risk, e.g. inevitable event, absence of certain controls etc. It may be useful to document those causal factors that the organisation has control over and those which are outside the control of the organisation.

In exploring factors, the interdependencies between infrastructure elements need to be identified e.g. power is required for water purification or pumping. Causal factors may include inadequate security, limited continuity plans, limited redundancy, etc.

Identify existing controls

Identify the existing controls for each causal factor or source of risk i.e.. *what do we already do to control the risk and/or causal factors?*

The purpose of a control is to provide reasonable assurances regarding the achievement of objectives in terms of effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable legislation.

Assess the adequacy of the existing controls

There will be a need to make judgements on whether or not existing controls are adequate. It may be useful to reflect on past experience and examine instances where there has been exposure to loss and why this has occurred. Alternatively, a simulation of the risk scenario may prove a useful exercise to test the effectiveness of current controls e.g. emergency fire drill.

The Control Practices Matrix shown below in Table 1 provides a simple way of objectively determining the adequacy of your existing controls.

Table 1

Control Effectiveness

	Does the control address the risk effectively?	Is the control officially documented and communicated?	Is the control in operation and applied consistently?
Yes	1	1	1
Partly	3	2	2
No	6	3	3
Add scores	<input type="text"/>	+ <input type="text"/>	+ <input type="text"/> = <input type="text"/>

Total Score

By locating the total score from Table 1 in the rating table (Table 2), a quick assessment of the effectiveness (not necessarily efficiency or economy) of controls may be ascertained.

Table 2

Control Effectiveness Rating Table

Score	Rating	Description
7 – 12	Poor	At best, control addresses risk, but is not documented or in operation; at worst control does not address risk and is neither documented nor in operation.
5 – 6	Fair	Control addresses risk, at least partly, but documentation and/or operation of control could be improved.
4	Good	Control addresses risk, but documentation and/or operation of control could be improved.
3	Excellent	Control addresses risk, is officially documented and in operation and applied consistently.

Ideally “Excellent” or “Good” ratings should be sought for all controls. Risks that are well controlled will have a lower consequence or likelihood depending on the control.

Step 3 – Analyse Risks

Assess the Likelihood and Consequences for each risk

The Likelihood (probability) and Consequences (impact) of a risk are used to identify the significance of the "Residual Risk", which is the level of exposure the risk represents after taking account of the strength of the controls considered above.

There are no definitive ratings or classifications for quantifying probability/likelihood, consequence or significance. Organisations can develop or adopt ratings or classifications that best suit their particular business. In setting the context (step 1) most organisations would consider various thresholds of loss where risk becomes unacceptable in terms of corporate loss. The following approach is based on the Australian Standard AS/NZS 4360:1999.

Determine Likelihood of the risk

Firstly rate the likelihood of the risk occurring in terms of "Rare" to "Almost Certain" (Table 3).

Table 3**Measures of Likelihood**

Level	Descriptor	Description
A	Almost Certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

The measurement of likelihood should be reassessed by CI operators each time a new national (4 Level) security notification is provided, i.e. from low to medium. This is the best underlying evidence operators have of event occurrence that can be fed into changed treatment strategies.

Determine Consequences Of The Risk

Next, rate what you believe the consequences to the listed objective or function would be should the event relating to the risk occur. Rate these from "Insignificant" to "Catastrophic" (Table 4). The description for each level can be tailored for your organisation as part of establishing the context (step one).

Table 4**Measures of Consequence**

Level	Descriptor	Example detail description
1	Insignificant	No injuries, "low" financial loss, no outage
2	Minor	First aid treatment, on site release immediately contained, medium financial loss, local press interest, normal outage
3	Moderate	Medical treatment required, on-site release contained with outside assistance, "high" financial loss, wide area outage
4	Major	Extensive injuries, loss of production capability, off-site release with some effects, major \$ loss, national press, prolonged outage in wide area
5	Catastrophic	Death, toxic release off-site with detrimental effect, huge financial loss, prolonged international press, loss of credibility, extensive state wide loss of service for prolonged period

Step 4 – Evaluate Risks**Determine Risk Priority**

The significance of the risk can then be determined by locating the risk on the matrix of risk levels (Table 5) and assigning an appropriate level of risk significance, ranking or priority.

Table 5**Risk Evaluation Matrix**

	Consequences				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic

Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Moderate	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

The primary output of this step is a prioritised list of the risks to the listed objective(s). This list makes a comparison across sources of risk possible and takes into account existing efforts or controls. It is expected that you would prioritise those risks that are ranked as extreme or high before those that are moderate or low.

Step 5 - Determine and Implement Treatment Action

The appropriate course of action to address each risk will require managers to make decisions on the treatments that they need apply to reduce the identified priority of the residual risk. There are a number of options available including:

- **Avoid** the risk when it is considered too great a threat to the performance of a function or objective. This may involve modifying the function or objective i.e. no longer operating a vulnerable line of business. This approach must be considered though is rarely taken.
- **Accept** the risk because risk level is low and existing controls are sufficient.
- Institute treatment **controls** or enhance existing controls to minimise as far as possible the probability and consequences of the risk when avoidance is not possible.
- **Transfer** the risk by either insuring against it or outsourcing the function. Ongoing monitoring must occur to ensure the course of action remains appropriate.
- Establish **mitigation strategies** to be implemented as part of reducing expected losses should identified risks occur.

Control treatments may include preventative methods such as building awareness, enhancing communication, engineering controls, enhancing robustness of assets, monitoring, security, surveillance, planning and exercising, building redundancy, design, improving response, employee checks, consolidating sites etc.

Mitigation treatments hinge on reducing vulnerability of elements at risk and include a range of resilience building techniques as well as those of response and recovery. Given the likely broad impact of infrastructure loss, treatment may also be directed to building resilience amongst users rather than focusing solely on enhancing the robustness of facilities.

Once appropriate actions to address risks have been determined, there should be an individual assigned responsibility for implementing the action and monitoring effectiveness in mitigating the residual risk.

Step 6 - Monitor action

Once the actions to address the residual risk are implemented, it is necessary to evaluate whether the actions were introduced as planned and whether the actions have been effective in reducing the level of risk. An essential part of this process is to continually identify any remaining

deficiencies and, where necessary, take corrective action and/or initiate mitigation strategies as problems arise.

This continual process of review is necessary to ensure controls have been properly implemented, remain appropriate, are operating efficiently, effectively and economically and are being met

Monitoring of external changes such as the four level National Security Notification Model is essential as part of managing Critical Infrastructure risk. Specific industry advisories may also have a bearing on your application of risk management.

Step 7 - Communicate and Consult

The risk management process is best applied in an iterative manner with continual communication and consultation throughout the various steps and actions. The effect of control actions will be to reduce the impacts considered previously, demanding the rethinking of approaches and re adjustment of priorities.

The Tasmanian CT Team is able to provide some input to the risk management approaches taken by CI operators. This includes the sharing of standard approaches and notification models as provided nationally.

Further Guidance

Further guidance on the subject of Risk Management can be sought from the following sources:

- Standards Australia has developed the Australian Standard AS/NZS 4360:1999 *Risk management* and other related guidance documents associated with this subject.
- CPA Australia Public Sector Centre of Excellence has published a series of reports that cover Risk Management in the Australian Public Sector.
- Tas SES produce an emergency risk management process for application with communities dealing with threats associated with natural and other hazards. This is useful in considering a community-based approach to the management of emergency risk.
- Emergency Management Australia publishes a range of documents outlining an emergency risk management process including specific draft guidelines for critical infrastructure.
- NSW is currently producing a series of guides for CI which should be available in early 2003.

Key Terms

<i>Control</i>	A procedure or activity designed to reduce the probability of the risk occurring and minimise its impact.
<i>Function</i>	A formally assigned responsibility.
<i>Impact</i>	Extent to which a risk is likely to adversely affect the performance of a function or the achievement of an objective.
<i>Inherent risk</i>	The total impact of a risk before treatment measures to eliminate or minimise adverse effects are taken into consideration.
<i>Objective</i>	A goal, defining what is to be achieved (ensure it is concise and clear as possible otherwise risk assessment will be difficult and inexact).
<i>Outcome</i>	Impact or effect on the community as a result of producing outputs.
<i>Output</i>	Products and services delivered by Infrastructure operators to external customers.
<i>Probability</i>	Likelihood of the occurrence of a risk.
<i>Residual risk</i>	The remaining level of risk after (existing) risk treatment measures have been taken.
<i>Risk</i>	The chance of something happening that will have an impact upon objectives (measured in terms of impact and probability). A risk is generally considered in context to a Threat, Uncertainty or Opportunity forgone i.e. there is a risk that X will impact negatively on Y.

Appendix 1: Risk Register Templates

The following are templates for a risk assessment process. Example notations (in italics) have been provided of a potential application.

Table 1 General Risk Identification Matrix

This matrix provides a checklist of your objectives and your identified sources of risk to establish an interaction. Where interaction is recorded then further evaluation can occur using Tables 2 and 3. (examples in italics)

	Elements at risk (<i>example objectives</i>)									
Sources of Risk (<i>examples</i>)	<i>Staff safety</i>	<i>Facility security</i>	<i>IT network</i>	<i>Data</i>	<i>System Network</i>	<i>Service delivery</i>	<i>Corporate reputation</i>	<i>Profit</i>	<i>Site "A"</i>	<i>Customer records</i>
<i>External bomb</i>	✓	✓	✓		✓	✓			✓	
<i>Cyber attack</i>			✓	✓	✓	✓	✓			✓
<i>Supplier collapse</i>	✓					✓	✓	✓	✓	
<i>Internal Sabotage</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>Contamination</i>	✓								✓	
<i>External sabotage</i>	✓	✓	✓		✓	✓		✓	✓	
<i>Loss of services</i>	✓		✓			✓			✓	

Table 2 Risk Register

This register lists the identified along with an assessment.

Risks (There is a risk of)	Control effectiveness	Consequence	Likelihood	Risk level	Priority	
<i>Cyber attack on</i>	<i>Service Delivery</i>	<i>Good</i>	<i>Moderate</i>	<i>Unlikely</i>	<i>Moderate</i>	<i>3</i>
	<i>Data</i>	<i>Excellent</i>	<i>Major</i>	<i>Unlikely</i>	<i>High</i>	<i>2</i>
	<i>Customer records</i>	<i>Excellent</i>	<i>Moderate</i>	<i>Unlikely</i>	<i>Moderate</i>	<i>3</i>

Table 3 Risk Treatment Plan

The Treatment Plan outlines the range of strategies chosen to manage the risk, along with by whom and when it shall be done.

Risk	Priority	Risk Treatment	Responsibility	Timeframe	Monitoring
<i>Cyber attack on data</i>	<i>2</i>	<i>Avoid – not viable, need data</i>	<i>N/a</i>	<i>N/a</i>	<i>N/a</i>
		<i>Transfer – use outsourced provider with tight contractual demands</i>	<i>Director corp services</i>	<i>Feb 2003</i>	<i>Report to committee</i>
		<i>Accept – No, risk is too high</i>	<i>N/a</i>	<i>N/a</i>	<i>N/a</i>
		<i>Control – improve data firewalls, enhance virus protection, train staff, update password protocols, assess website vulnerability, limit external links, join AusCERT</i>	<i>IT manager, HR manager, section heads</i>	<i>Feb March</i>	<i>IT security report HR policy manual Membership accepted</i>
		<i>Mitigate - improve off site storage, divide data into smaller groups,</i>	<i>IT manager</i>	<i>April</i>	<i>IT MGR report</i>