

Ministerial Guidelines for
Critical Infrastructure Resilience

Ministerial Guideline

Preface

Introduction

The arrangements for Victorian critical infrastructure resilience aim to provide clear guidance and a strategic framework within which the Victorian Government and key public and private sector stakeholders can work together to enhance Victoria’s arrangements for critical infrastructure resilience.

These Ministerial Guidelines for Critical Infrastructure Resilience (Ministerial Guidelines), issued in accordance with section 74W of the *Emergency Management Act 2013 (the Act)*, are designed to assist stakeholders to implement requirements under the arrangements. They are empowered under the Act, and are statutory in nature.

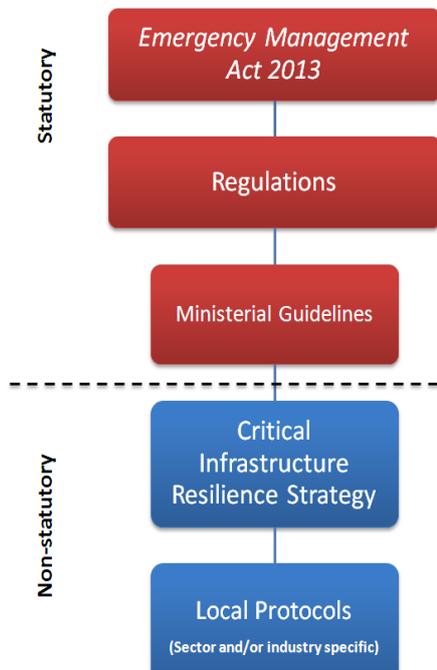


Figure 1

Figure 1 illustrates the hierarchy of documents involved in the critical infrastructure resilience arrangements.

Relevant Departments may also issue their own local protocols or guidance to meet sector-specific needs.

Objectives of the Ministerial Guidelines

These Ministerial Guidelines provide guidance for Relevant Departments and industry members to meet requirements under the Act, the *Emergency Management (Critical Infrastructure Resilience) Regulations 2015 (the Regulations)*, and the *Critical Infrastructure Resilience Strategy (Strategy)*. While the Regulations set out minimum standards for the legislated requirements of risk management plans, exercises and audits, these Ministerial Guidelines provide more explicit guidance to

assist in undertaking these and other activities specified in the Strategy.

Relevant Departments and owners and/or operators of critical infrastructure should work together using the approach set out by these Ministerial Guidelines, to achieve the best results under the Act for the Victorian community.

Commencement

These Ministerial Guidelines commence operation of the day they are approved, as indicated in the Appendix to each Guideline.

Ministerial Guidelines for Critical Infrastructure Resilience

It is intended that these Ministerial Guidelines and templates contained within will be reviewed periodically. Emergency Management Victoria will lead the review process.

Any revisions of the Ministerial Guidelines will be endorsed by the State Crisis and Resilience Council and the Minister responsible for the Act.

Key Definitions

Act refers to the *Emergency Management Act 2013*.

Critical dependency refers to assets, systems or infrastructure which, if disrupted, would significantly inhibit the ability of a Sector to deliver its essential services to the community.

Critical infrastructure has the same meaning as provided in section 74B of the Act.

Criticality assessment methodology has the same meaning as provided in section 74B of the Act.

Exercise means an exercise required by section 74Q of the Act.

Emergency has the same meaning as provided in section 3 of the Act.

Emergency Risk Management Plan has the same meaning as provided in section 74P of the Act.

Guidelines refers to guidelines issued under section 74W of the Act.

Industry Accountable Officer has the same meaning as provided in section 74I of the Act.

Key sector risk is a risk which, if realised, could disrupt the supply of the Sector's critical services to the community.

Owners and/or operators refer to any entity which owns and/or operates critical infrastructure and is listed, or is likely to be listed on the Victorian Critical Infrastructure Register.

Region has the same meaning as defined in Part 8 Appendix 8 of the Emergency Management Manual Victoria.

Regulations refers to the *Emergency Management (Critical Infrastructure Resilience) Regulations 2015*

Relevant department has the same meaning as provided in section 74B of the Act.

Relevant minister has the same meaning as provided in section 74B of the Act.

Resilience Improvement Cycle has the same meaning as provided in section 74M of the Act.

Responsible entity has the same meaning as provided in section 74H of the Act.

Statement of Assurance has the same meaning as provided in section 74B of the Act.

Strategy refers to the *Critical Infrastructure Resilience Strategy* (Victorian Government, 2015)

Vital Critical Infrastructure has the same meaning as provided in section 74B of the Act.

Security Classification

Material provided by owners and/or operators of critical infrastructure to Government will be treated as PROTECTED and will only be accessible to those with a demonstrable need to access the material.

Further information on the measures for handling PROTECTED material can be found in the Commonwealth's *Protective Security Policy Framework Information Security Management Guidelines* at www.protectivesecurity.gov.au.

The Hon James Merlino MP

Minister for Emergency Services

23 August 2016

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services
23 August 2016	Inclusion of definition for 'region'

Ministerial Guideline

Criticality Assessment Methodology

Introduction

The relevant minister, or his/her delegate, must assess or reassess major, significant and/or vital critical infrastructure having regard to the criticality assessment methodology. The relevant minister must then advise the Minister for Emergency Services of the outcome of this assessment or reassessment.

Objective of the Ministerial Guideline for the Criticality Assessment Methodology

The Ministerial Guidelines for the Criticality Assessment Methodology provides advice on the appropriate methodology for relevant Ministers to use to assess critical infrastructure under sections 74D and 74E of the *Emergency Management Act 2013*.

Key Principles of the Criticality Assessment Methodology

For the purposes of the definition of criticality assessment methodology, the prescribed methodology is the Victorian Criticality Assessment Tool (viccat).

viccat is Microsoft Sharepoint high-security, online reporting tool. It can be accessed at <https://www.viccat.vic.gov.au>. Relevant departments and critical infrastructure identified by relevant departments will be provided with a log-in and password by Emergency Management Victoria. Initial training on the tool will be provided to owners and operators of critical infrastructure by the relevant department.

While relevant ministers have primary responsibility for assessing the criticality of the infrastructure within their portfolio, as per section 74D of the *Emergency Management Act 2013*, the final recommendation considers input from a self-assessment process from owners and operators of critical infrastructure, and an assessment from the relevant department. Operators may elect not to conduct a self-assessment, in which case, the recommendation to the Minister will be based upon the assessment of the department alone.

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services

Ministerial Guideline

Emergency Risk Management Planning

Introduction

Risk Management Plans (RMPs) for emergency risks are to be prepared and maintained by responsible entities, being owners and/or operators of Vital Critical Infrastructure. RMPs must include:

- the identification and assessment of the emergency risks faced;
- the existing and planned actions or activities to manage each of the emergency risks; and
- the arrangements, processes and procedures that implement these actions or activities.

It is recognised that RMPs for emergency risk may be integrated within enterprise risk management plans or form a part of other risk management plans prepared to satisfy other legislative requirements.

To provide assurance that the RMPs meet the requirements of the *Emergency Management Act 2013* (the Act), the annual Statement of Assurance which is to be submitted by the Industry Accountable Officer in accordance with section 74N of the Act is to contain a signed attestation.

A template has been developed to assist responsible entities in preparing the annual Statement of Assurance. The annual Statement of Assurance to be submitted by Industry Accountable Officers must be broadly consistent with this template.

Objectives of the Ministerial Guideline for Emergency Risk Management Planning

The *Ministerial Guideline for Risk Management Planning* provides appropriate guidance to assist responsible entities to effectively manage emergency risk, and to prepare the annual Statement of Assurance. The structure of the Ministerial Guidelines has been summarised below:

- Key definitions and principles relevant to the development of RMPs and the preparation of the annual Statement of Assurance are provided on **page 2** below.
- A sample template for the annual Statement of Assurance for use by responsible entities is at **Schedule 1**.
- The template for the annual attestation by the Industry Accountable Officer is at **Schedule 2**.

Key Principles for Emergency Risk Management Planning

The *Emergency Management (Critical Infrastructure Resilience) Regulations 2015* prescribe the international standard *ISO31000:2009 Risk Management – Principles and Guidelines* as the basis for emergency risk management planning by responsible entities.

The following principles are provided to guide responsible entities in the development of their RMPs:

Ministerial Guidelines for Critical Infrastructure Resilience

1. The development and implementation of the RMP must give due consideration to the following guidance publications:
 - *HB436:2013 Risk Management Guidelines – Companion to AS/NZS ISO31000:2009;*
 - *HB89:2013 Risk Management – Guidelines on Risk Assessment Techniques;*
 - *ISO31010: Risk Management – Risk Assessment Techniques;*
 - *HB158:2010 Delivering Assurance based on ISO31000:2009;*
 - *National Emergency Risk Assessment Guidelines;*
 - *HB 167:2006 Security Risk Management.*
2. RMPs must consider the impact on responsible entities and the response to an emergency risk event experienced by a service on which the responsible entity is dependent. RMPs should also consider the responsible entities collaboration with other Vital and Major Critical Infrastructure which depend on its services in the development and implementation of the RMP.
3. RMPs must contain the emergency response procedures to be implemented in response to the occurrence of an emergency risk event.

Emergency response procedures must be aligned to and be consistent with the *State Emergency Response Plan* and its sub-plans, and the *Emergency Management Manual Victoria*.

Emergency response plans are also to be broadly consistent with the international standard *ISO22320: Societal Security – Emergency Management – Requirements for Incident Response*.
4. RMPs must contain the procedures for recovery of the Vital Critical Infrastructure from an emergency risk event, and for its continued safe operation. Recovery and continuity procedures should be broadly consistent with *AS5050:2010 Business Continuity – Managing Disruption-related Risk*.
5. RMPs must provide details of the approach to assurance - assurance and risk management being complementary processes.
6. The annual Statement of Assurance prepared in accordance with section 74N of the Act should be broadly consistent with the template provided at **Schedule 1** of these Ministerial Guidelines.
7. The annual Attestation by the Industry Accountable Officer shall be completed using the template provided at **Schedule 2** of these Ministerial Guidelines.

Reporting

Responsible entities are required to submit a Statement of Assurance annually to the relevant department. The timing of the submission is to be in accordance with section 74N(1) of the Act, and is dependent on the date of receipt of an Order under section 74E of the Act.

SCHEDULE 1

Statement of Assurance Template

[SECTOR]

Statement of Assurance

For the Year Commencing [YEAR]

Attestation by the Industry Accountable Officer

For the Year Ending – [YEAR]

A Statement of Assurance in accordance with section 74N of the *Emergency Management Act 2013*.

STATEMENT OF ASSURANCE

Vital Critical Infrastructure:
Responsible Entity:
Address
Industry Accountable Officer:
Contact Details
Year Commencing: <input type="text" value="Month / Year"/>

EMERGENCY RISK CONTEXT

Risk Analysis Criteria

Please provide details of the likelihood / Impact matrix with supporting scale descriptors

Summary of Risk Assessment

Please provide summary details of:

- the emergency risks identified;
- the assessed likelihood, consequence and level of risk for each identified emergency risk;
- current and proposed risk management actions or activities to manage the identified emergency risks;

- the status and assessed effectiveness of the risk management actions or activities;
- upstream and downstream interdependencies.

EMERGENCY RISK MANAGEMENT PLAN

The Risk Management Plan for the management of the identified emergency risks is comprised of the following manuals and documents:

Please provide summary details of each manual and document, including:

- title;
- version number;
- version date;
- approval authority;
- date of next scheduled review.

COMPLETION OF ACTION PLAN

Please provide a statement of completion of the action plan contained in the prior year's Statement of Assurance. Where actions are incomplete or circumstances have changed, please provide an explanation and intended resolution as appropriate.

ACTION PLAN:

Please provide details of the planned actions or activities to be undertaken in the coming year. The action plan should include:

- planned improvements to risk treatments arising from:
 - emergency risk assessment;
 - exercise outcomes;
 - audit findings;
 - operational experience;
- training approach and activities;
- exercise schedule and style;
- engagement, collaboration and participation with:
 - interdependent infrastructure owners / operators;
 - the Sector Resilience Network;
 - emergency service organisations;
 - Government;
- assurance activities:
 - audit program;
 - monitoring, review, improvement;
 - reporting;
- indicative implementation schedule.

SCHEDULE 2
Attestation Template

Attestation by the Industry Accountable Officer

I, _____ of _____, being the
Industry Accountable Officer for the responsible entity of _____,
the owner/operator of vital critical infrastructure known as _____,
do hereby attest that :

For the period from _____ to _____,

1. The information provided in the accompanying Statement of Assurance accurately reflects the status of the management of emergency risk, planned actions and activities, and the assurance program for emergency risk management.
2. [Name of responsible entity] has complied with the requirements of Part 7A of the *Emergency Management Act 2013* other than any exceptions noted in the attached Schedule.
3. [Name of responsible entity] will undertake the emergency risk management actions and activities proposed in the accompanying Statement of Assurance in the resilience improvement cycle from _____ to _____.
4. The emergency risk management actions and activities proposed for the previous resilience improvement cycle Statement of Assurance dated _____ have been undertaken other than any exceptions noted in the attached Schedule.

..... Date:

[Name]

Industry Accountable Officer

[Name of responsible entity]

Ministerial Guidelines for Critical Infrastructure Resilience

[Address of responsible entity]

Schedule

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services

Ministerial Guideline Exercises

Introduction

Responsible Entities, being owners and/or operators of Vital Critical Infrastructure must develop, conduct and evaluate an exercise to test their planning, preparedness, prevention, response or recovery capability in respect of an emergency.

Objectives of the Ministerial Guideline for Exercises

The *Ministerial Guidelines for Exercises* provides advice on exercise management to assist operators designated as 'Vital' under Part 7A of the *Emergency Management Act 2013* (the Act). These Guidelines cover suggested methodology and the approach to the preparation, conduct and evaluation of exercises in accordance with requirements under sections 74Q (Exercise by responsible entity) and 74R (relevant minister to review exercise), of the Act and standards prescribed under Part 7A.

The *Australian Emergency Management Handbook 3 – Managing Exercises* is the standard for exercise management which must be complied with by 'Vital' operators.

These standards are available for download at <https://ema.infoservices.com.au/items/HB3-2ND>

Key Principles for Exercises

The *Emergency Management (Critical Infrastructure Resilience) Regulations 2015* prescribes the *Australian Emergency Management Handbook Series – Handbook 3 (Managing Exercises)* as the basis for the development, conduct and evaluation of exercises by responsible entities.

Responsible entities should also give due consideration to *Australian Emergency Management Handbook Series – Handbook 8 (Lessons Management)*.

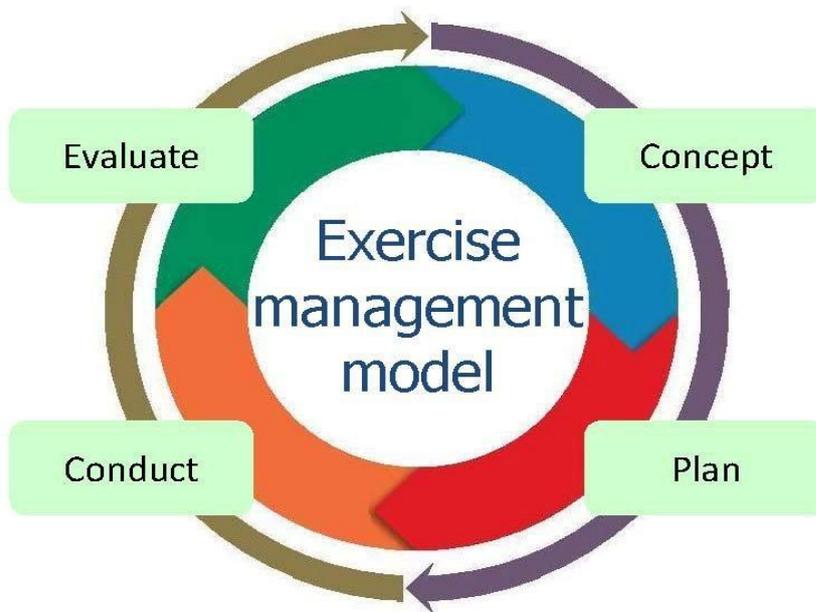
The following principles are provided to guide responsible entities in the development, conduct and evaluation of their exercises:

- The focus of Part 7A exercises is an emergency risk within an 'all-hazards' context;
- Exercise designers should:
 - consider the processes or capabilities within their plans that need to be tested or practised,;
 - develop measurable objectives that will provide observable activities that can be used to measure performance and then design a scenario focussed on those capabilities.

- Exercise scenarios should be identified that will cause the activities to occur to test the measurable objective.
- Exercises should be needs-based considering organisational requirements and the risk context in which the organisation is operating;
- An exercising program should be incorporated into the organisation's continuous improvement cycle; and
- Exercises should consider the relationships with state and regional emergency management arrangements, as appropriate.

Exercise management model

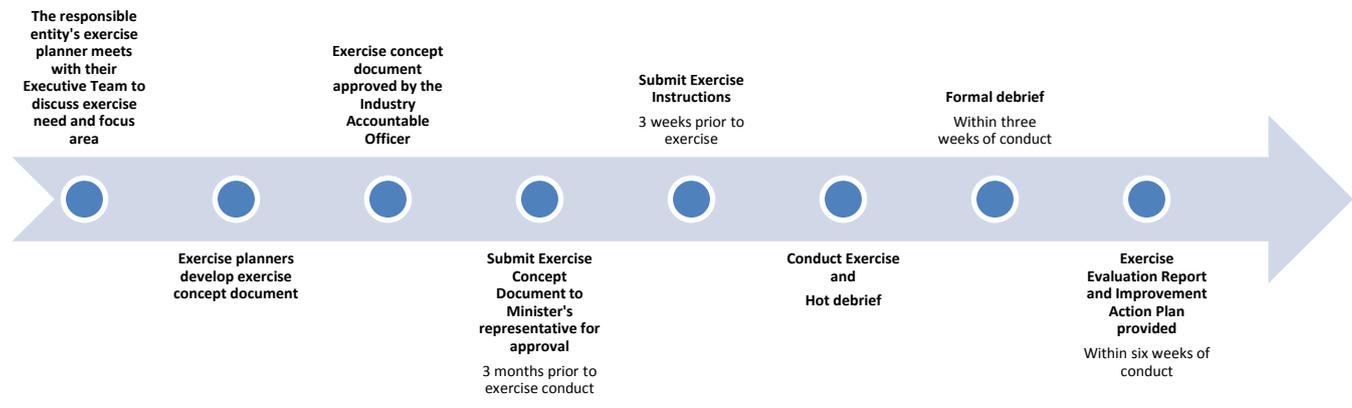
An exercise is a controlled, objective driven activity used for testing, practising and/or evaluating processes or capabilities. The exercise management model provides a structured approach to the exercising cycle and highlights the phases required to design, plan, conduct and evaluate an effective exercise.



Source: Australian Emergency Management Handbook 3 – Managing exercises

Key timeframes in the exercise cycle

The minister's representative will monitor all aspects of the exercise cycle.



Responsible entities may seek amendment to the timeframes outlined in this schedule through consultation with the minister's representative.

Exercise Concept

Exercise Concept Document

The exercise concept document is used to obtain the authority to conduct the exercise. The concept document should be approved by the Exercise Director, in this case the Industry Accountable Officer (as defined under section 74I of the Act). The concept should then be submitted to the relevant minister (department), for review and approval before detailed exercise planning commences, ideally 3 months prior to the proposed exercise conduct date.

The Exercise concept document should include detail about:

- The need for the Exercise;
- Exercise Overview;
- Exercise Aim;
- Exercise Objectives and performance measures;
- Exercise Scope;
- Exercise Outline (including style);
- Governance;
- Evaluation;
- Timeline.

Exercise Design

The aim and objectives of the exercise will help determine the most appropriate style of exercise.

The *Managing Exercises Handbook* describes three exercise styles, being:

- Discussion exercises;
- Functional exercises;
- Field exercises.

Within each of these styles there are different methodologies that can be used (detailed descriptions of the different styles can be found in Handbook 3). It can be an effective strategy to run a graduated exercise program where a discussion exercise is conducted in conjunction with any functional or field exercise.

While the majority of exercises will be functional this does not preclude organisations from considering other styles based on their exercise need. The proposed style should be described in the concept document and be agreed to by the minister's representative.

Exercise Planning

An exercise planning team must include at least one person from each organisation (or section in a single agency exercise) to ensure there is sufficient subject matter expertise to design a realistic exercise that adequately activates all the processes necessary to genuinely exercise plans and procedures.

Responsible entities should ensure adequate information security and confidentiality protocols are in place surrounding exercise material to ensure realism and to obtain maximum value from the conduct of the exercise.

A set of exercise instructions should be developed for those in Exercise Control. These instructions should be provided to the minister's representative two weeks prior to the conduct of the exercise and should include:

- Exercise control appointments;
- An exercise contact list;
- General Idea;
- A master schedule of events (MSE).

An evaluation plan should also be documented and may be included as an annexure. The Evaluation plan should be provided to the Minister's representative three weeks prior to the conduct of the exercise.

Responsible entities should consider involving relevant stakeholders or agencies, such as interdependent entities, to take part in the exercise.

Exercise Conduct

Designated entities should ensure that any stakeholders that may be affected by the conduct of the exercise are properly notified. Strategies should be in place to manage any real incidents that may occur during the exercise, including events that may precipitate the early termination of the exercise.

A hot debrief is to be conducted at the conclusion of the exercise to capture the initial reflections of the participants and identify any critical issues. A formal (cold) debrief should be conducted within three weeks of the exercise conduct. The minister's representative is to attend and participate in the formal debrief.

Exercise Evaluation

Exercise Evaluation process

At the concept development stage the evaluation process should start with the development of evaluation questions. These questions will shape the development of the objectives and guide the design of the exercise.

Any exercise evaluation should include:

- Performance against objectives;
- Exercise management.

There are four stages in the exercise evaluation process:

- Plan and coordinate the evaluation;
- Observe the exercise and collect data;
- Analyse the data;
- Develop the exercise report.

Evaluation conduct

Generally, evaluators should not intrude in the conduct of the exercise. The only exception to this is in the event of a safety issue where evaluators must intervene immediately.

Evaluators should record their observations in terms of what worked well and why, and what did not work well and why.

Exercise feedback

The relevant department will provide the operator with feedback focussed on both the performance against objectives as well as the process of designing and managing the exercise as a requirement under section 74R (b) of the Act. These observations will be fed in to the evaluation process.

If the observer of the exercise considers that the exercise did not provide adequate assurance of preparedness then the operator may be required to conduct another exercise, conduct training or other remedial activities as required under Section 74R (c)

Analysis of data

Initial analysis and summarising of data should identify the causes of any observed issues as it is the causes (rather than the observable symptoms) that need to be addressed in order to effect continuous improvement.

Once root cause analysis has been undertaken other analysis techniques can be applied.

Exercise Evaluation report

An exercise evaluation report should be produced that describes what happened in the exercise, details observations of good performance and areas of improvement. It is most important to detail the observations – possible treatment options for areas of concern may also be included.

The exercise report should be provided to the minister’s representative within six weeks of the conduct of the exercise.

Improvement Action Plan

Any Improvement Action Plan should capture elements of performance that need to be sustained as well as improved.

The Improvement Action Plan should have a timeline for implementation and allocate responsibility for each item. Systems should be in place to ensure that the progress of items captured in the Improvement Action Plan are progressed.

In the event that the relevant minister (department) considers that there are significant issues with the exercise conduct or outcome, the relevant minister may request in writing that specified improvement actions be completed and/or a second exercise be conducted, as per section 74R (c).

The Improvement Action Plan should form part of the Annual Assurance Statement in accordance with section 74N(3).

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services

Ministerial Guideline

Audits

Introduction

Responsible entities must conduct an audit of their emergency risk management processes after the completion of an exercise.

Objectives of the Ministerial Guideline for Audits

The Ministerial Guideline for Audits provides appropriate guidance on audits to assist responsible entities under Part 7A of the *Emergency Management Act 2013* (Act).

These Ministerial Guidelines suggest approaches to achieving assurance by conducting an audit of the responsible entity's risk management processes after the completion of an exercise. This is required under section 74S of the Act.

Key Principles of Audits

The *Emergency Management (Critical Infrastructure Resilience) Regulations 2015* prescribes the international standard handbook *HB 158- 2010 Delivering assurance based on ISO 31000: Risk Management - Principles and guidelines* as the basis for the planning and conduct of audits by responsible entities.

The following principles guide responsible entities in the planning and conduct of their audits:

- the main focus of the audit should be to evaluate efficiency, effectiveness of the risk management processes;
- audits should form a key part of the responsible entity's assurance program;
- audits should be aligned with the responsible entity's existing processes to avoid duplication;
- audits should be conducted as an independent activity.

Audit Scope

The audit should evaluate the efficiency, effectiveness and appropriateness of the responsible entity's management of risks to its capability in relation to planning, preparedness, prevention, response and recovery of provision of critical services.

The responsible entity should determine the audit scope in consultation with the relevant minister.

In determining the audit scope, the responsible entity should consider:

Ministerial Guidelines for Critical Infrastructure Resilience

- clearly defining the extent timing and nature of the audit;
- the risk assessment process;
- the risk to the capability of the responsible entity to plan, prepare, prevent, respond and recover from emergency events.

Appointment of an Auditor

The audit is to be undertaken by an audit team with adequate knowledge of the subject matter and audit techniques who were not involved in the emergency risk management process or the development or conduct of an exercise.

Audit Methodology

The planning stage of the audit should consider:

- understanding the responsible entity and its key stakeholders;
- the responsible entity's operating environment and its internal control systems;
- assessing the risk of misstatement;
- the design of audit procedures commensurate with the assessed level of risk;
- sources of evidence.

Typically the audit should include:

- an analysis of documented procedures;
- interviews /consultation with relevant staff and key stakeholders;
- involving appropriate staff to assess the effectiveness of training;
- an analysis of information systems to assess effectiveness;
- an analysis of quality controls;
- an identification of changes in systems and documented procedure;
- an evaluation and documentation of deficiencies.

Audit Report

The audit findings should be documented in a report which includes:

- a description of the audit objective, audit scope and methodology;
- audit questions , sources of data and limitations of data;
- the systems, processes and procedures examined;
- recommendations for improvements based on findings where relevant.

Auditors are encouraged to report audit outcomes using a grading system.

The responsible entity has the right of reply to any of the audit findings and should prepare a response to the audit report as appropriate.

Audit Certificate

Following the audit, the relevant Industry Accountable Officer, should submit to the relevant minister an audit certificate confirming that the audit has been completed, as soon as practicable. The certificate should include the outcome of the audit and whether any required actions have been identified and any responsible entity management response.

The identified actions and the expected timing for implementations should be included in the annual Statement of Assurance submitted to the relevant department.

Second audit

The Act provides that the relevant minister can request a second audit if the relevant minister is not satisfied that the audit has met the intent of the Act.

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services

Ministerial Guideline

Sector Resilience Plans

Introduction

Sector Resilience Plans (SRPs) are produced annually by government departments in collaboration with industry through Sector Resilience Networks (SRNs). SRPs are based on information supplied by the sector and provide Government with:

- a picture of each sector's overall resilience;
- key emergency risks faced by the sector;
- the potential consequences of those risks; and
- resilience improvement initiatives to be undertaken by the Sector Resilience Network in the following 12 months.

SRPs will also perform an assurance function. Government departments are accountable for their responsibilities under the Strategy and their role in promoting the resilience of their sector through the SRP's Departmental Attestation.

Objectives of the Ministerial Guideline for Sector Resilience Plans

The *Ministerial Guideline for Sector Resilience Plans* provides guidance to assist government departments to complete SRPs. The structure of the Ministerial Guideline is summarised below:

- Key engagement principles relevant to the completion of SRPs are provided on **page 1**.
- A sample Sector Resilience Plan template to guide government department in the development of their SRPs is at **Schedule 1**.

Key engagement principles in developing the Sector Resilience Plan

The following principles are provided to guide government departments in the development of their SRPs:

1. SRPs should represent a collaboration between the government departments and industry stakeholders through the Sector Resilience Networks.
2. The Ministerial Guideline for Risk Management Planning issued under the *Emergency Management Act 2013* requires 'vital' critical infrastructure owners and operators to participate in the development of the SRPs.
3. Government departments should work with industry to develop the content of the SRPs. However, departments will remain the final arbitrator of the content of the SRPs in the interest of improvement of sector-wide resilience. Some matters, such as specific terrorism risks and mitigations, may be considered by departments or sectors to be too sensitive to include within the SRPs. The Secretary of the department for the sector may determine that the sensitivity of any matters warrant that they should be referenced only at a high level or, where there is exceptional justification, not be included in the SRP. Where possible

the issues should be summarised prudently with guidance provided on related resilience improvement initiatives or other actions that are planned.

Reporting

SRPs are completed annually by government departments. Emergency Management Victoria (EMV) will determine appropriate timelines in consultation with government departments, however an indicative reporting cycle is at **Table 1** below to assist in planning.

Table 1: SRP Reporting Cycle				
Date	1 July previous year	1 July	August - September	October – December*
SECTOR RESILIENCE PLANS	<i>Commencement</i> Government departments begin drafting SRPs.	<i>Submission</i> Finalised SRPs provided to EMV.	<i>Approval Process</i> Finalised SRPs provided to Risk and Resilience Sub-Committee, followed by SCRC for endorsement.	
ALL SECTORS RESILIENCE REPORT			<i>Drafting</i> EMV drafts All-Sectors Resilience Report.	<i>Approval and Release</i> All-Sectors Resilience Report publicly released following the endorsement of SCRC and the Minister for Emergency Services.
* Indicative dates dependent on annual meeting schedules of SCRC and the Risk and Resilience Sub-Committee.				

SCHEDULE 1

Sample Sector Resilience Plan Template

Sector Resilience Plan

[SECTOR]

[YEAR] - [YEAR]

A Sector Resilience Plan in accordance with the Victorian Government's *Critical Infrastructure Resilience Strategy*.

OVERVIEW OF THE [INSERT SECTOR] SECTOR

1. Defining the Sector

Please provide a description of the ‘sector’, including the key goods and/ or services provided by the sector to government, industry and the Victorian community.

! Note that the description provided may influence the risks identified under the KEY EMERGENCY RISKS FACING THE SECTOR section.

2. Scope of Sector Resilience Plan (SRP)

Please provide a brief description of the scope of the SRP, including the owners and/ or operators who contributed to the SRP’s development through the SRN.

Where the focus is on a particular risk and/ or resilience theme, this should be noted.

3. Key Industries and Stakeholders

Please provide a brief overview of the key industries and stakeholders that underpin the sector.

4. Key Assets and Infrastructure

5. Please provide an overview of key assets or infrastructure within the sector.

6. Emergency events that have challenged the sector (within the previous 12 months)

Please provide a summary of any emergency events which had the potential to, or did challenge, the resilience of the sector’s infrastructure, operations or deliverables (where relevant and appropriate, noting that some owners and/or operators may have security or reputational concerns about being identified).

7. Summary of actions taken arising from previous SRP

Please provide a brief progress summary of each Resilience Improvement Initiative listed in the sector’s most recent SRP.

Progress should be assessed against the desired outcomes and timelines identified for each Initiative.

KEY EMERGENCY RISKS AND DEPENDENCIES OF THE SECTOR

Emergency Risk Environment of Sector

Please provide a brief, high-level narrative of the emergency risk environment of the sector, including the nature of risks facing, or expected to be faced, by the sector.

The narrative may draw on:

- information provided by risk assessments available to the department;
- threat assessments; long-range weather forecasts;
- supply and/ or demand issues; and
- other relevant material available to the department or provided by the sector's owners and/ or operators.

Any significant changes in the emergency risk environment from previous years should also be included, along with an explanation of the change.

The Secretary of the department for the sector may determine that the sensitivity of any matters warrant that they should be referenced only at a high level or, where there is exceptional justification, not be included in the SRP. Where possible the issues should be summarised prudently with guidance provided on related resilience improvement initiatives or other actions that are planned.

Key Emergency Risks and Critical Dependencies of the Sector

[KEY EMERGENCY RISK OR CRITICAL DEPENDENCY]

Please identify key emergency risks and critical dependencies facing the sector in this section. Departments are encouraged to consider the following sources :

- recurring risks or themes across the sector identified by RIC and RMP processes;
- the relevance of risks identified in the latest iteration of the State Emergency Risk Assessment Report to the sector;
- any reports, threat assessments, analyses or risk identification products undertaken by, or provided to, the department in the preceding 12 months (where relevant), and
- Victoria Police in regard to any criminal threat.

Description

Please provide a brief qualitative description of the key emergency risk or critical dependency, including the possible or likely consequences of the risk. *as appropriate*,

Current Controls and Preparedness

Please provide a brief qualitative description of the current controls in place and general preparedness of the sector to deal with, and respond to, the key emergency risk or critical dependency identified.

The entities responsible for each control identified should be listed.

Sector Exposure to Risk or Critical Dependency

Please provide a brief qualitative description of the sector’s overall exposure to the key emergency risk or critical dependency, noting the residual exposure of the sector’s critical services to the key emergency risk or critical dependency.

[Repeat headings for additional risks as necessary]

The relevant headings to be repeated for each *key emergency risk* and *critical dependency* are:

- ! • [KEY EMERGENCY RISK OR CRITICAL DEPENDENCY] (Heading)
- Description
- Current Controls and Preparedness
- Sector Exposure to Risk or Critical Dependency

Resilience Improvement Initiatives

Theme of Resilience Improvement Initiatives [Optional]

Government departments may opt to identify a theme to underpin the sector’s Resilience Improvement Initiatives for this SRP cycle.

Themes may be based around a specific emergency risk or risks, categories of risk controls, such as improved risk analysis, mitigation planning and information sharing; staff training; improved practices, technology, infrastructure or maintenance; or government-industry engagement.

This is optional and should be deleted if not used.

[Initiative]

Please provide a Resilience Improvement Initiative that the government department will pursue to drive improvements of the sector’s resilience over the SRP cycle in this section.

Initiatives identified should relate to:

- the enhancing of the sector’s overall resilience to respond to, adapt and build upon unexpected circumstances or events; and/ or
- the sector’s risk exposure from key sector risks and/ or critical dependencies identified under the KEY EMERGENCY RISKS FACING THE SECTOR section.

! Improving the sector’s resilience to risks identified in the SRP is an ongoing process. Progressing initiatives that lead to incremental improvements in resilience over a number of SRP cycles is appropriate.

Emergency Risk being addressed (where applicable)

Where an Initiative is responding to a key sector risk or critical dependency, the key sector risk or critical dependency, this should be identified.

Delete this heading if not required.

Description of Resilience Improvement Initiative

Please provide a summary description of the Resilience Improvement Initiative. The description should provide:

- the objective of the initiative and desired outcomes;
- a description of the Initiative;
- the steps or processes required to complete the Initiative with estimated completion dates; and
- any problems that may be foreseen.

Key Roles and Responsibilities

Government departments should articulate their role in completing the Initiative.

The Departmental Attestation requires Secretaries of government departments to attest that their Department will undertake the resilience improvement initiatives identified in the Sector Resilience Plan.

! The fulfilment of roles and responsibilities outlined in this section by government departments will be used to measure departmental accountabilities.

Key stakeholders including other government departments and agencies (including regulators); the sector’s owners and/ or operators; and any additional stakeholders – where relevant – should be identified.

Relevant roles or responsibilities of key stakeholders for undertaking the Resilience Improvement Initiatives should also be identified.

Where specific improvements in sector resilience rely, in part, on the actions of industry, the SRP should articulate this reliance.

Government departments should closely collaborate with key stakeholders to complete resilience improvement initiatives.

! Government departments will not be accountable under the Departmental Attestation for any actions taken or failed to be taken by other stakeholders.

[REPEAT headings as necessary for additional Resilience Improvement Initiatives]

The relevant headings to be repeated for each Initiative are:

- [INITIATIVE]
- ! • Emergency Risk being addressed (where applicable)
- Description of Resilience Improvement Initiative
- Key Roles and Responsibilities

DEPARTMENTAL ATTESTATION

NAME OF DEPARTMENT

[SECTOR]

Departments must complete the relevant fields of the attestation, including obtaining the Secretary’s signature.

Secretaries are not expected nor asked to attest to the intentions or actions of the sector’s industry.

Once finalised, the SRP must be lodged with Emergency Management Victoria by the completion of the SRP annual cycle.

Government department Responsibilities

1. The [INSERT DEPARTMENT] has fulfilled legislative requirements and responsibilities under Part 7A of the *Emergency Management Act 2013*.
2. The [INSERT DEPARTMENT] has conducted the [INSERT SECTOR]’s Sector Resilience Network with industry and government representatives in accordance with the Critical Infrastructure Resilience Strategy.

Sector Resilience Plan

3. The [INSERT SECTOR]’s Sector Resilience Plan for [YEAR] – [YEAR]:
 - a. has been completed in consultation with the [INSERT SECTOR] Sector Resilience Network;
 - b. provides a summary of the key emergency risks facing the [INSERT SECTOR] sector, as advised by industry; and
 - c. outlines resilience initiatives that will be undertaken through the Sector Resilience Network

NAME OF SECRETARY

Date:

DEPARTMENT

Appendix

This Ministerial Guideline commences operation on the day it is approved. The table below records updates of the Guideline as approved by the Minister for Emergency Services.

Date of Approval	Version
28 May 2015	Original Guideline issued by Minister for Emergency Services
27 March 2017	Updated Table 1: SRP Reporting Cycle