

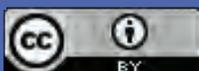
CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY



Victorian Government document endorsed by Minister or Premier.

Authorised by the Victorian Government
1 Treasury Place, Melbourne, 3002

© State of Victoria 2015



You are free to re-use this work under a [Creative Commons Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/), provided you credit the State of Victoria (Emergency Management Victoria) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any images, photographs or branding, including Government logos.
ISBN 978-0-9943637-1-8

Published July 2015

If you would like to receive this publication in an accessible format please email media@emv.vic.gov.au
This document is also available in Word and PDF format at emv.vic.gov.au

TABLE OF CONTENTS

MINISTERIAL FOREWORD	04
EXECUTIVE SUMMARY	06
ADOPTING AN ALL-HAZARDS RESILIENCE FRAMEWORK	08
ARRANGEMENTS FOR VICTORIAN CRITICAL INFRASTRUCTURE	12
VICTORIAN CRITICAL INFRASTRUCTURE MODEL	20
RESILIENCE IMPROVEMENT CYCLE	23
GOVERNMENT-INDUSTRY PARTNERSHIP	28
REGULATIONS & GUIDELINES	31
REFERENCES	31



MINISTERIAL FOREWORD

As Victorian Minister for Emergency Services I am pleased to introduce the Critical Infrastructure Resilience Strategy, which forms part of new arrangements in the management of Victoria’s critical infrastructure. These new arrangements are founded on a strong partnership between government and the industry sectors, working together to build resilience and limit disruption to the supply of essential services to the Victorian community. Resilience recognises that while it is impossible to prevent the occurrence of natural disasters, it is possible to mitigate risks and consequences through effective planning.

This Strategy sets out the vision, principles and strategic priorities for the future direction in building resilience of Victoria’s critical infrastructure. Importantly, the Strategy gives effect to recent legislative changes to the Emergency Management Act 2013 which came in on 1 July 2015. The legislation provides the foundation in the important task of building resilience which will result in reduced disruptions to essential services.

The Strategy outlines the Victorian Critical Infrastructure Model. The key features of the model includes legislation supporting a risk-based approach, a new definition for Victoria’s critical infrastructure moving towards an ‘all hazards’ resilience model which includes a focus on terrorism, partnership between government and industry to build resilience and transparent and consistent method for assessing the ‘criticality’ of infrastructure. The Strategy outlines roles and responsibilities, in order that collectively we can work to building resilience.

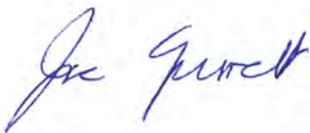


BUILDING THE RESILIENCE OF THE STATE'S INFRASTRUCTURE IS THE RESPONSIBILITY OF GOVERNMENT, PUBLIC AND PRIVATE SECTOR STAKEHOLDERS WORKING IN PARTNERSHIP. THIS DEMONSTRATES OUR COMMITMENT IN WORKING TOGETHER TO BUILD A STRONG AND RESILIENT COMMUNITY AND TO POSITION VICTORIA TO MEET THE FUTURE CHALLENGES AHEAD.

The Strategy reflects best practice internationally and is the culmination of extensive engagement and consultation across government departments, agencies and critical infrastructure owners and operators. Victorian critical infrastructure is all infrastructure, including assets, systems and networks necessary to maintain Victoria's social and economic wellbeing. Critical infrastructure resilience is important for the health, safety and prosperity of the Victorian community.

Building the resilience of the State's infrastructure is the responsibility of government, public and private sector stakeholders working in partnership. This demonstrates our commitment in working together to build a strong and resilient community and to position Victoria to meet the future challenges ahead.

I commend the emergency management sector and critical infrastructure owners and operators for their ongoing energy and recognition of how important this is.



JANE GARRETT MP

Minister for Emergency Services



EXECUTIVE SUMMARY

The health, safety and prosperity of the Victorian community are reliant on certain infrastructure. The complex, interconnected and often interdependent nature of this critical infrastructure increases the risk of a disaster-causing systemic failure.

While primary responsibility for critical infrastructure resilience rests with infrastructure owners and/or operators, the community expects that government will take appropriate measures to ensure that owners and/or operators are managing their risks and that vital service delivery is not interrupted.

The best protection is achieved by improving the resilience of critical infrastructure to all potential hazards, whether natural or human induced. Resilience includes resistance, reliability, redundancy, response and recovery.

This Critical Infrastructure Resilience Strategy (Strategy) builds upon the emergency management reform directions for critical infrastructure outlined in the December 2012 Roadmap for Victorian Critical Infrastructure Resilience. It replaces the Critical Infrastructure Resilience Interim Strategy (December 2013), which introduced the themes and reforms that are now confirmed by this Strategy and Part 7A of the Emergency Management Act 2013 (the Act).

This Strategy reiterates priorities and sets out management arrangements for critical infrastructure resilience. It was developed in consultation with government and industry stakeholders.

The arrangements contain two broad approaches to improving critical infrastructure resilience:

- a Victorian Critical Infrastructure Model under which the criticality of infrastructure is assessed and interventions prioritised, implemented and communicated; and
- legislation and regulations governing resilience arrangements for vital critical infrastructure.



THE BEST PROTECTION IS ACHIEVED BY IMPROVING THE RESILIENCE OF CRITICAL INFRASTRUCTURE TO ALL POTENTIAL HAZARDS, WHETHER NATURAL OR HUMAN INDUCED. RESILIENCE INCLUDES RESISTANCE, RELIABILITY, REDUNDANCY, RESPONSE AND RECOVERY.

A risk-based and transparent methodology, the Victorian Criticality Assessment Tool (viccat), is used to assess the criticality of infrastructure in a consistent manner. Industry is invited to complete a self-assessment with subsequent review, discussion and input from portfolio departments. The relevant department provides a recommendation on the appropriate categorisation of the critical infrastructure to the portfolio minister, who then recommends the designation of critical infrastructure assessed as 'vital' to the Governor in Council.

Part 7A of the Act adopts a transparent, risk-based approach to resilience, applied consistently, but flexibly, across sectors. Owners and operators of critical infrastructure designated as 'vital' are required to comply with mandatory obligations under the legislation, based on a cycle of planning, exercising and validation. A robust performance measurement and assurance framework support achievement of legislative goals while minimising regulatory burden. Owners and/or operators of non-'vital' critical infrastructure are encouraged to develop best practice emergency risk management strategies and practices based on the obligations for 'vital' critical infrastructure.

Regulations prescribe minimum standards for requirements under the legislation. Further guidance is provided in topic-specific guidelines, which are issued by the Minister for Emergency Services.

Governance arrangements for critical infrastructure resilience fit within the broader emergency management committee system in the Victorian Government. Clear roles and responsibilities, whether mandatory or voluntary, are identified for all parties.

The status of, and plans for, critical infrastructure resilience are developed by, and reported through, sector-specific networks. These will be based on collaborative relationships and shared responsibility between government and owners and/or operators of critical infrastructure.



ADOPTING AN ALL-HAZARDS RESILIENCE FRAMEWORK

Since the 2001 terrorist attacks in the United States of America, protecting critical infrastructure from a terrorist attack has been a high priority for Australian governments. However, the changing and complex risk environment requires consideration of other hazards that can also seriously affect critical infrastructure.

Victorians are aware of the hazards that can destroy homes and disrupt businesses. The range of disruptions and crises has become broader and, due to increasing interconnectedness and interdependencies of infrastructure, the consequences wider. Internationally, governments have responded to the new risk environment by moving towards an all-hazards resilience approach to critical infrastructure policy and practice. This approach focuses on managing uncertainty in the emergency risk environment by building resilience to a number of hazards.

At the heart of the all-hazards resilience approach is a recognition that "...comprehensive protection of all critical infrastructure ... against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs"¹. Instead of focusing on the type and likelihood of specific threats, an all-hazards resilience approach focuses on the likely consequences of a failure of a specific asset, network or other infrastructure component and seeks to mitigate them. Although some residual risk will always be present, risk management strategies can help build capacity for communities to become more resilient to disasters, disruptions and crises.

An all-hazards approach to resilience encompasses the idea that planning for one kind of hazard or disaster event can also increase the resilience of a community in the face of a different kind of event. Indeed, different hazard events can have similar consequences on infrastructure². For example, both floods and bushfires can lead to a loss of power.

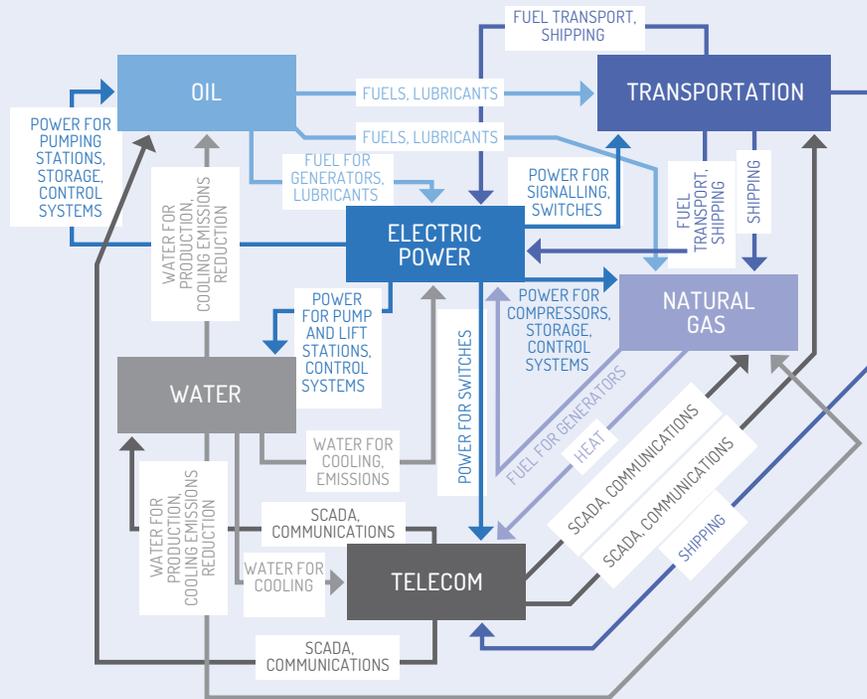
The all-hazards approach to resilience also recognises that our critical infrastructure is highly interdependent in complex ways, both physically and through a host of information and communications technologies (see **Figure 1** and **Box 1** (see below)). Governments and infrastructure owners and/or operators can make better policies and decisions when they identify and analyse these interdependencies, as reflected in the *Victorian Government's Victorian Emergency Management Reform White Paper*³.

¹ Crisis and Risk Network, Focal Report 1: *Critical Infrastructure Protection*, Centre for Security Studies, Zurich, October 2008, p. 3.

² Cabinet Office (United Kingdom), *Keeping the Country Running: Natural Hazards and Infrastructure*, Crown, London, October 2011.

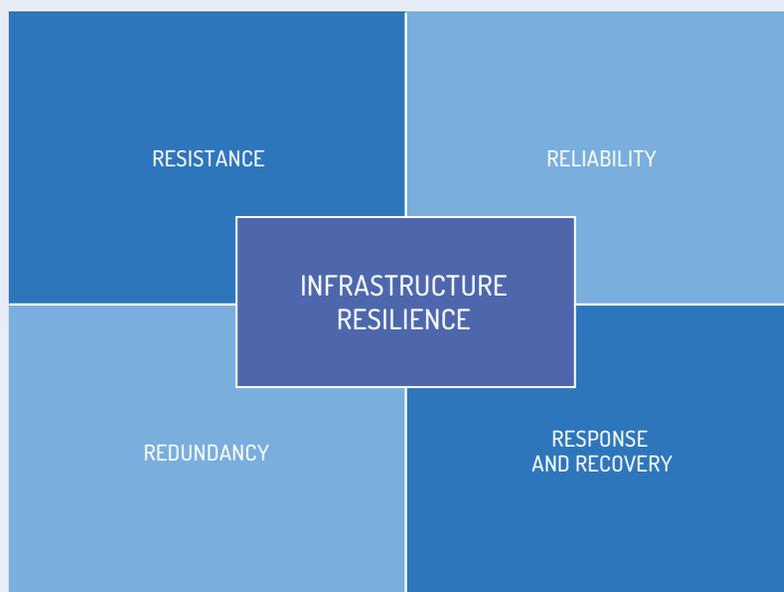
³ Victorian Government, *Victorian Emergency Management Reform White Paper*, Victorian Government, Melbourne, December 2012.

FIGURE 1: EXAMPLES OF INFRASTRUCTURE INTERDEPENDENCIES⁴



The United Kingdom Government provides a useful conceptual framework for thinking about critical infrastructure resilience that spans the emergency management continuum. It identifies four principal strategic components as shown in **Figure 2**. In summary, it shows that “...resilience of infrastructure is provided through ... good design of the network and systems to ensure it has the necessary resistance, reliability and redundancy ... , and ... by establishing good organisational resilience to provide the ability, capacity and capability to respond and recover from disruptive events. The latter is gained through business operations and appropriate support for business continuity management”⁵.

FIGURE 2: THE COMPONENTS OF INFRASTRUCTURE RESILIENCE⁶



⁴S. Rinaldi et al., *Identifying, Understanding and Analysing Critical Infrastructure Interdependencies*, IEE Control Systems Magazine, December 2001, p. 15.

⁵Cabinet Office (United Kingdom), op cit., p. 16.

⁶Cabinet Office (UK), *Keeping the Country Running: Natural Hazards and Infrastructure*, Crown, London, October 2011.



WHILE NOTING THE CONTINUING IMPORTANCE OF MANAGING EMERGENCY RISKS FROM TERRORISM, VICTORIA'S ARRANGEMENTS FOR VICTORIAN CRITICAL INFRASTRUCTURE ARE CONCERNED WITH ALL EMERGENCY RISKS. SECTION 3 OF THE ACT DEFINES AN EMERGENCY AS FOLLOWS:

“Emergency means an emergency due to the actual or imminent occurrence of an event which in any way endangers or threatens to endanger the safety or health of any person in Victoria or which destroys or damages, or threatens to destroy or damage, any property in Victoria or endangers or threatens to endanger the environment or an element of the environment in Victoria including, without limiting the generality of the foregoing—

- (a) an earthquake, flood, wind-storm or other natural event; and
- (b) a fire; and
- (c) an explosion; and
- (d) a road accident or any other accident; and
- (e) a plague or an epidemic or contamination; and
- (f) a warlike act or act of terrorism, whether directed at Victoria or a part of Victoria or at any other State or Territory of the Commonwealth; and
- (g) a hi-jack, siege or riot; and
- (h) a disruption to an essential service.”



BOX 1: CYBER DEPENDENCY

The pervasive reliance on secure cyber-based control technology means that virtually all infrastructure has a cyber dependency. Cyber attack is a global risk that is evolving rapidly as new technologies and systems emerge. The potential economic, social, environmental, political and national security costs of a cyber breach or attack are significant.

Cyber attacks can result in a range of consequences given the widespread application of computer systems and networks within our society, including attacks on:

- individuals or organisations (private sector or government), resulting in service disruption, loss of confidential information and/or economic losses;
- communication service provider systems, resulting in widespread disruption of services;
- banks or financial institutions, resulting in service disruption and/or economic losses; and
- Supervisory Control and Data Acquisition (SCADA) systems for essential services, resulting in service disruption, infrastructure damage and/or loss of life.

Cyber attacks should be one of the emergency risks for which Victorian critical infrastructure owners and/or operators prepare.

A major planned cyber attack in Victoria could involve one or more of three possible tactics:

- a broad-based virus attack on key systems supporting critical e-commerce or service delivery;
- a targeted attack on critical infrastructure, e.g. SCADA systems supporting the delivery of services essential to the community; and/or
- a major distributed denial of a service attack.

Both private and public sector organisations in Victoria have been subject to attacks on systems and networks. Cyber attacks, often referred to as 'hacking', can be carried out from anywhere in the world, which makes them difficult to investigate and prosecute.

In 2014, in response to this emerging issue, the Commonwealth Government established the Australian Cyber Security Centre (ACSC)⁷, which brings together key Commonwealth cyber security capabilities from the Department of Defence, Attorney-General's Department, Australian Security Intelligence Organisation, Australian Federal Police and the Australian Crime Commission. In addition to other functions, the ACSC provides information, advice and support on cyber threats and vulnerabilities to the owners and/or operators of Australia's critical infrastructure and other systems of national interest.

⁷ <http://www.asd.gov.au/infosec/acsc.htm>, current at 1 May 2015.



ARRANGEMENTS FOR VICTORIAN CRITICAL INFRASTRUCTURE

Victorian critical infrastructure delivers services that are essential to maintain the social and/or economic well-being of the State. Continuously improving the resilience of critical infrastructure to better ensure the continuity of essential services requires effective partnerships between government and the owners and/or operators of infrastructure.

This Strategy and Part 7A of the Act support the management of emergency risks to Victoria's critical infrastructure from natural and human-induced emergencies. The Act mandates requirements and coordination structures that create a strong culture of risk management and collaboration to plan for, respond to and recover from emergency events.

The Strategy provides guidance and a strategic framework within which the Victorian Government and key public and private sector stakeholders can work together to enhance Victoria's critical infrastructure resilience. The vision, principles and strategic priorities for Victorian critical infrastructure resilience are outlined in **Figure 3**.

FIGURE 3: VISION, PRINCIPLES AND STRATEGIC PRIORITIES FOR VICTORIAN CRITICAL INFRASTRUCTURE RESILIENCE

VISION	Arrangements for Victorian critical infrastructure resilience, founded on a strong partnership between government and industry sectors, that limit disruption to the supply of essential services to the Victorian community			
PRINCIPLES	Community Critical infrastructure resilience arrangements aimed at maximising the service continuity to the Victorian community	Partnerships Governance arrangements that reflect the collaborative relationship and shared responsibility between government and industry	Skills and knowledge An all-hazards resilience approach that focuses on identifying, assessing, managing and mitigating risks	Assurance A performance measurement and assurance framework that recognises the primary responsibility for resilience of critical infrastructure lies with the owners and/or operators of critical infrastructure
STRATEGIC PRIORITIES	An all-hazards resilience model (which includes a focus on terrorism) A consistent and transparent method of assessing the value and criticality of infrastructure Strong partnerships between government and industry Clearer roles and responsibilities for all actors Consistent but flexible approach for risk management across sectors Transparent risk-based approach to resilience in legislation A robust performance measurement and assurance framework			

Part 7A of the Act mandates risk management strategies for the Victorian infrastructure that are most vital for delivering essential services to the community. The Victorian Critical Infrastructure Model (described in the next section) outlines the process for determining Victorian critical infrastructure. The owners and/or operators of the most critical infrastructure are required to undertake a range of activities that comprise a Resilience Improvement Cycle (the Cycle). Owners and/or operators of other critical infrastructure facilities and sectors are encouraged to undertake similar actions voluntarily.

CRITICAL INFRASTRUCTURE SECTORS

Victoria has adopted a sectoral approach to improve critical infrastructure resilience. There are presently eight critical infrastructure sectors with corresponding lead portfolio departments within the Victorian Government (**Figure 4**).

FIGURE 4: SECTOR RESILIENCE NETWORKS

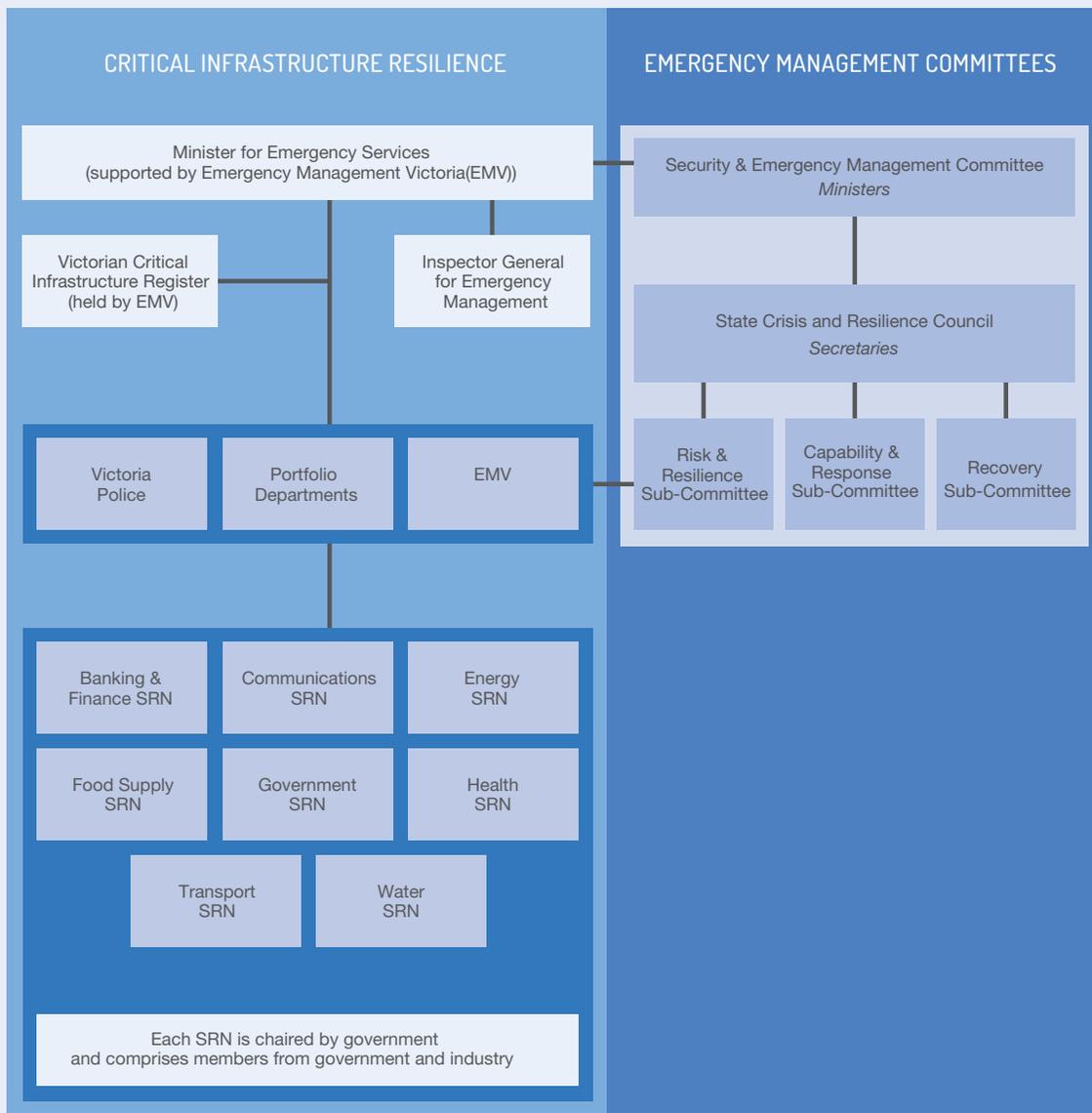
SECTOR RESILIENCE NETWORKS	
SECTOR	RESPONSIBLE DEPARTMENT
Banking and Finance	Department of Treasury and Finance
Communications	Department of Economic Development, Jobs, Transport and Resources
Energy	Department of Economic Development, Jobs, Transport and Resources
Food Supply	Department of Economic Development, Jobs, Transport and Resources
Government	Department of Premier and Cabinet
Health	Department of Health and Human Services
Transport	Department of Economic Development, Jobs, Transport and Resources
Water	Department of Environment, Land, Water and Planning

A Sector Resilience Network (SRN), chaired by the relevant portfolio department, for each critical infrastructure sector brings together portfolio departments with owners and/or operators of critical infrastructure to consider the management of risk and improve the resilience of the sector’s essential goods and service to the community. The role of the SRNs is outlined in the section titled Government-Industry Partnership (see next page).

GOVERNANCE ARRANGEMENTS FOR CRITICAL INFRASTRUCTURE

The SRN structure interacts with the broader emergency management committee structure through the Risk and Resilience Sub-Committee of the State Crisis and Resilience Council (SCRC) (Figure 5). The Risk and Resilience Sub-Committee oversees and provides guidance on matters relating to critical infrastructure resilience – including major developments in each sector – and reports to the SCRC. These arrangements ensure government’s senior executives oversee the work of the SRNs.

FIGURE 5: CRITICAL INFRASTRUCTURE RESILIENCE GOVERNANCE ARRANGEMENTS





VICTORIAN GOVERNMENT SENIOR COMMITTEES, DEPARTMENTS AND AGENCIES

Several Victorian Government entities have key roles and responsibilities, underpinned by legislation, that support critical infrastructure resilience. The Minister for Emergency Services is the minister responsible for critical infrastructure resilience. More information on Victoria's general emergency management arrangements can be found in the *Emergency Management Manual Victoria*⁸.

SECURITY AND EMERGENCY MANAGEMENT COMMITTEE (SEMC)

The SEMC is the Victorian Government's decision-making body for a major incident (including a terrorist incident) requiring whole of government coordination. The SEMC is chaired by the Premier of Victoria and includes ministers with security and emergency management responsibilities. The SEMC also considers whole of government policies and arrangements that advance Victoria's security and emergency prevention and response and recovery capabilities. It is not the role of SEMC to manage the deployment of emergency services.

⁸ Emergency Management Victoria, *Emergency Management Manual Victoria (manual)*, State of Victoria, 2013. <http://www.emv.vic.gov.au/policies/emmv/>, current at 1 May 2015.



STATE CRISIS AND RESILIENCE COUNCIL (SCRC)

The SCRC is the peak crisis and emergency management advisory body to the Victorian Government, providing advice in relation to:

- whole of government policy and strategy for emergency management in Victoria; and
- the implementation of that policy and strategy.

The SCRC is chaired by the Secretary of the Department of Premier and Cabinet, with membership comprising all departmental secretaries, the Chief Commissioner of Police and the Chief Executive Officer of the Municipal Association of Victoria. The Emergency Management Commissioner, the Chief Executive of Emergency Management Victoria (EMV) and the Inspector General for Emergency Management (as an observer) also sit on the SCRC.

In the event of a complex or large-scale emergency, the SCRC's role is to:

- ensure that the broad social, economic, built and natural environmental consequences are addressed at a whole of government level;
- identify and access government resources as required;
- oversee communication strategies; and
- support the SEMC in its response to the emergency.

The SCRC will not be involved in operational or tactical control of the response to major emergencies.



THE RISK AND RESILIENCE SUB-COMMITTEE

The Risk and Resilience Sub-Committee is the peak advisory body to the SCRC on emergency management matters relating to risk and resilience, and shares responsibility for ensuring the delivery of the SCRC Strategic Action Plan with other sub-committees established by the SCRC.

Specifically the Risk and Resilience Sub-Committee will:

- support the SCRC by providing:
 - high-level strategic advice on risk and resilience emergency management reform priorities;
 - oversight of implementation of risk and resilience policy and strategy across the emergency management spectrum;
 - delivery of the Strategic Action Plan as it relates to risk and resilience;
 - the timely provision of emergency planning advice as it relates to risk and resilience and associated activities; and
 - oversight of implementation of risk and resilience associated activities;
- support the government's reform agenda for crisis and emergency management;
- oversee the implementation of the state risk and mitigation arrangements;
- develop and oversee implementation of the risk and resilience work plan for sign off by the SCRC on a yearly basis;
- advise the SCRC on whole of government crisis and emergency management strategy and emerging or complex crisis and emergency management issues relating to risk and resilience; and
- assist the SCRC in the evaluation of projects and tasks.

The Risk and Resilience Sub-Committee will focus on strategy and policy and will not be involved in operational or tactical control of the response to crises or major emergencies.



EMERGENCY MANAGEMENT VICTORIA

EMV is the overarching body for emergency management in Victoria. It has the lead role in maintaining and coordinating whole of government strategy and policy for critical infrastructure resilience to ensure a consistent approach across government.

EMV has specific responsibility to:

- develop and support effective communication, monitoring and reporting networks to provide assurance on the effective implementation of the Strategy;
- hold and distribute the Victorian Critical Infrastructure Register (the Register) (see section titled Victorian Critical Infrastructure Model below);
- disseminate intelligence and information on non-terrorism risks and hazards from relevant sources;
- provide advice to the Minister for Emergency Services on critical infrastructure resilience policy and strategy;
- liaise with the Commonwealth Government on national critical infrastructure resilience arrangements;
- develop the All Sectors Resilience Plans based upon the Sector Resilience Plans (SRPs) produced by individual portfolio departments; and
- inform the SEMC, the SCRC and the Risk and Resilience Sub-Committee on critical infrastructure resilience matters.

EMV promotes information sharing and coordination across sectors and amongst the sector portfolio departments by convening the SRN Coordination Group (SRN-CG). The chairs of each SRN participate in the SRN-CG, where initiatives and experiences are shared and cross-sector dependencies explored.

The EMV also supports the Emergency Management Commissioner in the fulfilment of their functions under legislation and relevant state emergency management plans.



PORTFOLIO DEPARTMENTS

The portfolio departments responsible for each critical infrastructure sector provide the primary interface between government and critical infrastructure owners and/or operators. These departments lead the planning for their sector through annual development and review of SRPs in partnership with industry (see section titled Government-Industry Partnership below). Portfolio departments chair SRNs, consulting with critical infrastructure owners and/or operators through these networks. Portfolio departments work with owners and/or operators of 'vital' critical infrastructure to implement the Cycle through a consistent but flexible approach across sectors. They also engage with their relevant Commonwealth partners on sector-specific critical infrastructure resilience matters.

VICTORIA POLICE

Victoria Police is the control agency for terrorism and other human-induced deliberate threats to critical infrastructure. Where appropriate, it provides protective security advice to industry owners and/or operators on the Register (see section titled Victorian Critical Infrastructure Model below). It provides threat and risk intelligence and information on terrorist risk to relevant owners and/or operators and portfolio departments. Victoria Police may communicate directly with owners and/or operators where there is an imminent and specific terrorism or other human-induced threat to critical infrastructure. Portfolio departments may invite Victoria Police to appropriate exercises; and for those exercises where it is the control agency, it will provide advice as required during the development of the exercises. It participates in the governance arrangements for critical infrastructure and government-industry partnership mechanisms.

INSPECTOR GENERAL FOR EMERGENCY MANAGEMENT (IGEM)

The role of the IGEM is to provide assurance to the government and the community in respect of emergency management arrangements in Victoria and foster continuous improvement of emergency management in Victoria. The IGEM maintains a monitoring and assurance framework for emergency management (inclusive of critical infrastructure resilience). This framework includes outcome measures against which the capacity, capability and performance of the emergency management sector are to be assessed. In this way, the IGEM advises government on the efficacy of Victoria's arrangements for critical infrastructure resilience.



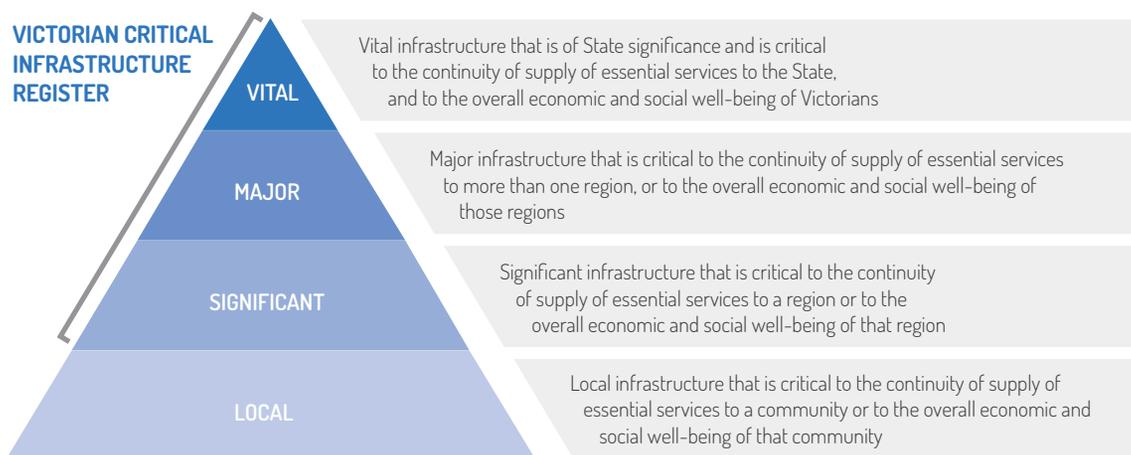
Photos by Roberto Seba

VICTORIAN CRITICAL INFRASTRUCTURE MODEL

Governments around the world use assessment tools to identify those assets most critical to the functioning of their societies, and thus to tailor management approaches to different levels of emergency risk.

Victoria's Critical Infrastructure Model comprises four levels ('vital', 'major', 'significant' and 'local') with the first three forming the Register, (see **Figure 6** below).

VICTORIAN CRITICAL INFRASTRUCTURE MODEL



THE REQUIREMENTS FOR VICTORIAN CRITICAL INFRASTRUCTURE INCLUDED ON THE REGISTER DIFFER DEPENDING ON THEIR CRITICALITY RATING.



A 'local' rating is included in the Model because some infrastructure is critical to the social or economic well-being of an individual community, but not a whole region or larger area. The government recognises that there are benefits for communities in engaging with their local councils and local infrastructure owners and/or operators to talk about strategies for linking private and public goals and interests for enhancing the resilience of important local infrastructure. However, the Register does not include local infrastructure.

The Register is accessible to all who have a need to know, to increase understanding of industry interdependencies.

REQUIREMENTS FOR EACH CRITICALITY RATING

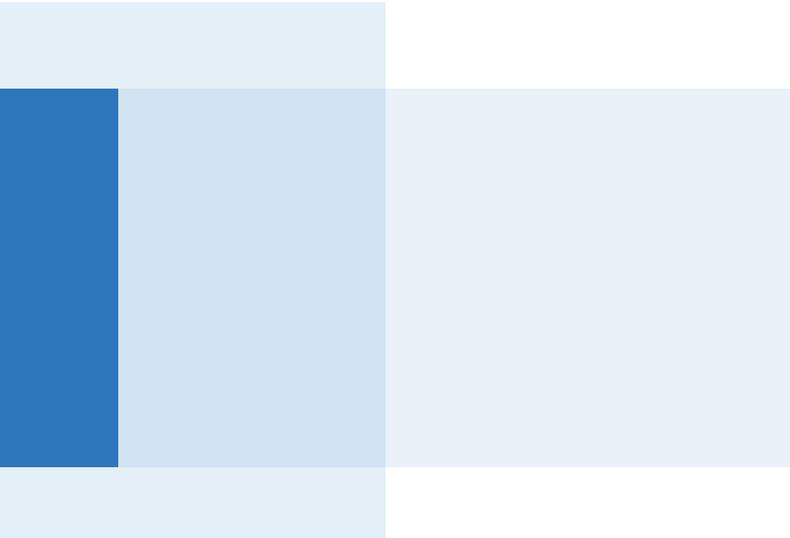
The requirements for Victorian critical infrastructure included on the Register differ depending on their criticality rating.

Mandatory measures under the legislation apply to infrastructure classified as 'vital' (see section on the Resilience Improvement Cycle below for details).

For infrastructure rated as 'major' and 'significant', industry are encouraged to voluntarily develop best practice standards based on the requirements for 'vital' critical infrastructure.

All critical infrastructure owners and/or operators included on the Register are strongly encouraged to participate in the engagement activities outlined under the section titled Government-Industry Partnership below.

Councils are encouraged to consider owners and/or operators of 'local' critical infrastructure (not on the Register) in their municipal emergency management planning processes.



ASSESSING THE 'CRITICALITY' OF VICTORIAN CRITICAL INFRASTRUCTURE

'Criticality' is usually defined as a measure of the consequences associated with the loss or degradation of the infrastructure or the service it provides. "The more the loss of the infrastructure threatens the survival or viability of its owners, of those located nearby, or of others who depend on it (including the nation as a whole), the more critical it becomes"⁹. In particular, an assessment of criticality must be based on the scope and gravity of the potential damage to the community.

'Vital' infrastructure is subject to legislative requirements, therefore it is imperative that the method for assessing the value and 'criticality' of infrastructure be robust, transparent and able to be applied consistently across all sectors. The portfolio departments therefore use a custom-made assessment methodology, viccat, to assess the criticality of Victorian critical infrastructure for their sector.

viccat considers all hazards and a range of emergency risks consistent with AS/NZS ISO31000 Risk Management – Principles and Guidelines and HB 167:2006 Security Risk Management. It involves narrative inputs as well as metrics aligned to the National Emergency Risk Assessment Guidelines¹⁰. It also involves consideration of the vulnerabilities upstream and downstream dependencies, as well as the resilience of critical infrastructure.

The assessment process itself provides for operator input and supports dialogue between government and industry about an individual criticality rating. The relevant minister is responsible for determining the criticality ratings for critical infrastructure in their sector. On advice of the relevant minister, the Governor in Council will designate 'vital' infrastructure under the Act.

The owner and/or operator of the critical infrastructure assessed will be advised of their rating and responsibilities under the arrangements. A focus will be maintained on the most important assets/services.

⁹ Moteff, John, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, CRS Report for Congress, 4 February 2005, p. 5.

¹⁰ <http://www.em.gov.au/Publications/Program%20publications/Pages/NationalEmergencyRiskAssessmentGuidelines.aspx>, current as of 1 May 2015.



RESILIENCE IMPROVEMENT CYCLE

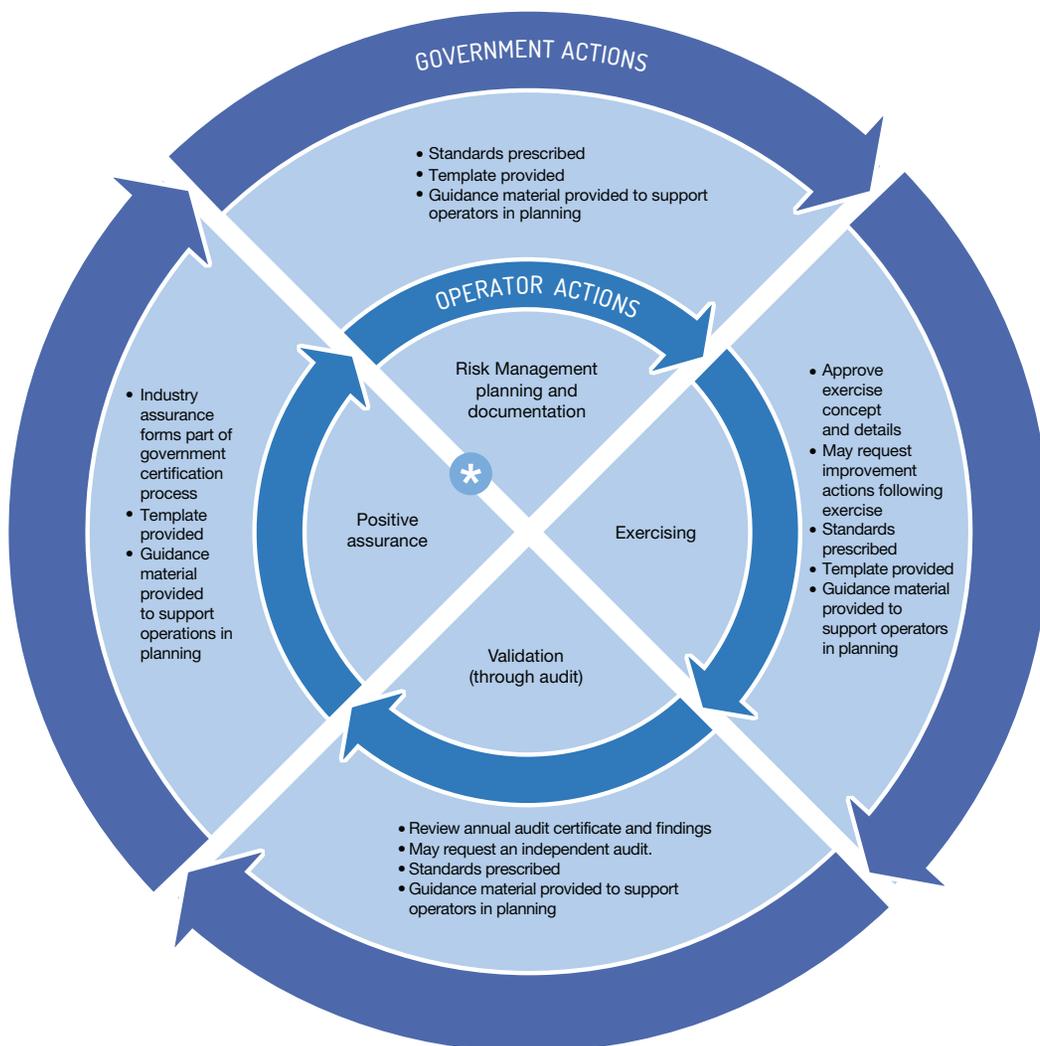
‘Vital’ critical infrastructure participate in a collaborative Cycle to help industry and government articulate the emergency risks to the supply of essential services to the Victorian community, and to develop risk management strategies to mitigate and manage those risks.

The Cycle includes a risk management framework, operating in four key stages. This prompts learning from exercises and emergencies, with a structured approach to developing innovative and adaptive solutions, not just improvements to existing ones.

The Cycle is the framework for engagement between government and industry, and for monitoring the sector’s emergency risk environment. Government may engage with industry in addition to the Cycle, seek improvement actions, or waive or alter aspects of the Cycle, as appropriate. Customisation of the measures by sector and for particular owners and/or operators is also possible. Industry and government roles at each stage are described in **Figure 8** and **Box 2** below.



FIGURE 8: RESILIENCE IMPROVEMENT CYCLE



* Year 1 - Minister and Industry nominate Accountable Officers

There are mandatory elements under each stage of the Cycle for 'vital' critical infrastructure owners and/or operators. Other infrastructure owners and/or operators are encouraged to adopt these measures to assist in planning for any emergency.



THERE ARE MANDATORY ELEMENTS UNDER EACH STAGE OF THE CYCLE FOR 'VITAL' CRITICAL INFRASTRUCTURE OWNERS AND/OR OPERATORS. OTHER INFRASTRUCTURE OWNERS AND/OR OPERATORS ARE ENCOURAGED TO ADOPT THESE MEASURES TO ASSIST IN PLANNING FOR ANY EMERGENCY.

To increase the flexibility of the arrangements and reduce regulatory burden, the government may provide options for industry to demonstrate the fulfilment of requirements under any stage of the Cycle. For instance, with the agreement of the portfolio department, where other standards or legislation have comparable emergency risk management obligations, the industry owner and/or operator may be deemed as meeting the Victorian requirements.

Owners and/or operators of 'vital' critical infrastructure must implement an emergency risk management planning process in accordance with the prescribed standards under the *Emergency Management (Critical Infrastructure Resilience) Regulations 2015* (the Regulations). The risk management planning process must consider all envisaged emergency risks, including security/terrorism risks, for 'vital' critical infrastructure located in Victoria.

Owners and/or operators of 'vital' critical infrastructure are not required to provide their emergency risk management plans to government, unless requested. Instead they must develop, and annually submit to government, a Statement of Assurance which should outline the processes and plans in place to manage the risks identified by the owner and/or operator's Accountable Officer (see below). The Statement of Assurance is not intended to provide a detailed outline of actual risk management plans, but rather a description of the identified risks and actions in place to treat these risks.

Owners and/or operators of 'vital' critical infrastructure must develop, conduct and evaluate an exercise program to test the operation of their emergency risk management processes and their capability to respond to, and recover from, an event in an all-hazards environment. Following an exercise, the owner and/or operator must conduct an audit of their emergency risk management processes.

The owner and/or operator's Accountable Officer is required to submit an audit certificate and findings to the government, which provides assurance that the emergency risk management processes are robust.

The flexibility built into the Cycle means that assurance mechanisms are essential to achieve appropriate oversight and monitoring of actions by both government and industry. In addition to validation through audits, owners and/or operators of 'vital' infrastructure also provide positive assurances to portfolio departments annually.

Accountable Officers have responsibilities for ensuring that their organisations undertake, test and validate appropriate emergency risk management planning. They are nominated by their organisation and appointed under legislation.

Portfolio departments also have responsibilities in the Cycle. This includes annual certification by departmental secretaries to the relevant minister to provide assurance that their departments are assisting and monitoring the performance of 'vital' critical infrastructure.



BOX 2: ROLES IN THE RESILIENCE IMPROVEMENT CYCLE

STAGE 1: RISK MANAGEMENT PLANNING AND DOCUMENTATION

INDUSTRY ROLE

- Operator implements an emergency risk management planning process, in accordance with the Regulations and Ministerial Guidelines for Critical Infrastructure Resilience (the Guidelines), that considers all envisaged emergency risk hazards, including security/terrorism risks.
- A Statement of Assurance outlining the processes and plans to manage the risks identified is submitted to the relevant minister (or nominated delegate) by the company's Accountable Officer. The Statement of Assurance also includes identification of dependencies and the scope of the company's program to test, validate, monitor and positively assure the robustness of the risk management arrangements.
- Following the first year, operators also incorporate their positive assurance statement (Stage 4) into the Statement of Assurance.

GOVERNMENT ROLE

- Regulations and Guidelines exist for the emergency risk management planning process, including a template for the Statement of Assurance. The template can be customised to suit the requirements of individual sectors.
- Regulations prescribe standards to be exercised, with further instructions provided in the Guidelines.
- Government to consolidate all industry Statements of Assurance for input into SRPs in consultation with industry members.

STAGE 2: EXERCISING

INDUSTRY ROLE

- In accordance with Regulations, the operator develops, conducts and evaluates an exercise program to test its capability to respond to and recover from an event in an all-hazards environment. Guidelines are provided by government for the exercise management process.

GOVERNMENT ROLE

- Government approves exercise aims, objectives and details (style, timing and location).
- A delegate of the relevant minister observes the exercise.
- Government prepares a summary of high-level themes from the exercise outcomes for the sector.
- Government may request improvement actions following the exercise.



STAGE 3: VALIDATION (THROUGH AUDIT)

INDUSTRY ROLE

- The Accountable Officer of the company submits an audit certificate and findings to government, which provides assurance that the emergency risk management processes are robust and that strategic outcomes are being achieved. Guidelines exist for audit processes.

GOVERNMENT ROLE

- Government reviews certificate and findings.
- Government may request specific content to be included in the audit plan or that an independent audit be conducted.

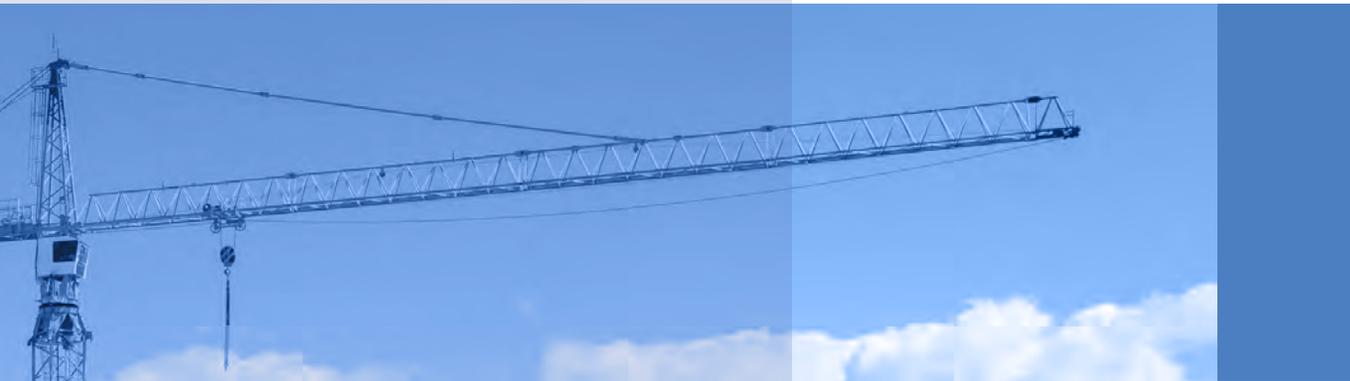
STAGE 4: POSITIVE ASSURANCE

INDUSTRY ROLE

- The Accountable Officer of the company certifies the Statement of Assurance that all actions identified at the start of the Cycle have been undertaken, including the outcomes of the testing and validation processes.

GOVERNMENT ROLE

- Government reviews the Statement of Assurance and seeks supporting evidence as required.
- Secretaries of relevant portfolio departments certify to the SCRC and their portfolio minister that their departments have undertaken nominated actions to support sectoral resilience including development of a SRP.



GOVERNMENT-INDUSTRY PARTNERSHIP

Strong partnerships between government and industry underpin Victoria's ability to effectively address the challenges to, and provide new opportunities for, critical infrastructure resilience.

The majority of Victoria's critical infrastructure assets are owned and/or operated by private entities that have strong incentives for risk management. Government works in partnership with these entities to increase the resilience of critical infrastructure for the wider Victorian community.

The Strategy's key mechanisms for developing these partnerships are SRNs and SRPs. Participation in these is mandatory for owners and/or operators of 'vital' infrastructure, and encouraged for others.

SECTOR RESILIENCE NETWORKS

PURPOSE

The purpose of SRNs is to improve the resilience of each sector's critical infrastructure assets and operations through joint planning, information sharing and reporting to government.

To achieve this, SRNs:

- provide a regular forum to foster and develop collaboration between government and industry;
- enable industry to advise the government on the risks, as well as the security, emergency management, business continuity and resilience arrangements, for the sector;
- allow for the identification of shared resilience issues affecting security and emergency management, and opportunities for improvement across the sector;
- provide opportunities for industry to participate in joint planning exercises and practice preparedness capability (including reviewing outcomes or lessons from such exercises), in addition to cross-sectoral and multi-industry exercises;
- encourage the sharing of information, experience and good practice;
- assist government departments to produce each sector's annual SRP; and
- assist in the identification of, and appropriate planning in relation to, interdependencies.

STRUCTURE

There are eight sector-based SRNs representing each critical infrastructure sector. These SRNs reflect the evolution of the Security and Continuity Networks (SCN) structure introduced in 2007.

In addition to the regular forums provided by the sector-based SRNs, an All Sectors Resilience Network Forum, comprising members from all eight SRNs, is regularly convened. This forum will highlight interdependencies between sectors and increase understanding of cross-sectoral vulnerabilities.

ROLES AND RESPONSIBILITIES

Each SRN is chaired by the portfolio department and includes representatives from industry, EMV and Victoria Police. Other government departments and agencies are invited as appropriate.

Strong industry participation is essential for the successful functioning of SRNs. Industry members include a representative from each 'vital' critical infrastructure owner and/or operator, in line with their legislated Statement of Assurance commitments. Owners and/or operators of 'major' and 'significant' critical infrastructure are also encouraged to participate in SRNs.

SRN GOVERNANCE

The governance arrangements of SRNs reflect the Strategy's strong emphasis on performance monitoring and assurance.

The SCRC, through its Risk and Resilience Sub-Committee, will oversee the operation and activities of the SRNs, ensuring accountability at the most senior levels of government. The central mechanism for the SRNs reporting to the SCRC is the annual SRP. The development process of the SRP is led by portfolio departments, in consultation with industry through the SRNs.

SECTOR RESILIENCE PLANS (SRPS)

PURPOSE

The purpose of the SRPs is to provide the Victorian Government with the status of, and continuous improvement arrangements for, each critical infrastructure sector's overall resilience. In doing so, SRPs fulfil engagement, planning, monitoring and assurance functions.

STRUCTURE

SRPs include four key sections:

1. Overview of the sector;
2. Key emergency risks and dependencies of the sector;
3. Resilience improvement initiatives; and
4. Departmental attestation.

Through industry collaboration, they provide an overview of the sector's critical assets and operations. The SRPs develop a profile of risks facing the sector, including an evaluation of the risks identified. Responding to this identification and evaluation of sector risks, the SRPs identify resilience improvement initiatives to address significant emergency risks posed to the sector. The implementation of these initiatives is monitored by government.

ROLES AND RESPONSIBILITIES

Portfolio departments lead the development and drafting of annual SRPs in collaboration with industry, through their SRN.

Secretaries of portfolio departments attest to the accuracy of the SRP to the SCRC as part of the Cycle. Secretaries also attest that the SRP provides for the status of emergency risks faced by the sector as advised by industry, as well as having appropriate measures to address those emergency risks, where required. Secretaries are not required to attest to any action or improvements that have been, or will be, undertaken by industry.

Industry support portfolio departments in the development of the SRPs through the SRNs. The role of industry includes sharing information on emergency risks faced by owners and/or operators of critical infrastructure to identify resilience improvement opportunities, partnering with portfolio departments in developing appropriate resilience improvement initiatives to strengthen the mitigation of emergency risks, and undertaking these activities in line with the SRPs.

Completed SRPs are submitted to the Risk and Resilience Sub-Committee. The Risk and Resilience Sub-Committee reviews the SRPs, which then go on to inform the development of an All Sectors Resilience Report (ASRR).

Portfolio departments are also responsible for briefing relevant ministers on the completed SRPs and monitoring the implementation of resilience improvement activities undertaken by industry.

ALL SECTORS RESILIENCE REPORT

Produced annually by the EMV through the Risk and Resilience Sub-Committee, the ASRR summarises the resilience of Victoria's critical infrastructure sectors. The ASRR includes an overview of the key emergency risks facing Victoria's critical infrastructure and the resilience improvement measures being adopted by the Victorian Government and industry in response to those risks. Interdependencies between sectors are also identified in the ASRR.

Upon completion, the ASRR is used to brief the SCRC and the Minister for Emergency Services on the resilience of Victoria's critical infrastructure and to assist the SCRC to determine if any further actions by portfolio departments are required.

To promote public accountability and transparency of both government and industry's critical infrastructure resilience, the Minister for Emergency Services authorises the annual public release of the ASRR.

Photos by: Roberto Seba



REGULATIONS AND GUIDELINES

The Regulations prescribe a minimum set of standards for emergency risk management planning, exercise management and audit processes. The limiting of the Regulations to standard-setting facilitates flexibility of practice by industry and government.

Guidelines on the following topics provide further detail to assist in meeting the requirements of legislation:

- criticality assessment methodology;
- emergency risk management planning;
- exercise management;
- audit processes; and
- template and requirements for SRPs.

Guidelines on additional topics may be published from time to time by government.

REFERENCES

An electronic copy of this Strategy is available on the EMV website at www.emv.vic.gov.au.

Emergency Management Act 2013

Emergency Management (Critical Infrastructure Resilience) Regulations 2015

Emergency Management Manual Victoria

Ministerial Guidelines

Victorian Emergency Management Reform White Paper

Roadmap for Victorian Critical Infrastructure Resilience (December 2012)

Critical Infrastructure Resilience Interim Strategy (December 2013)

