NSW Critical Infrastructure Resilience Strategy Guide

A Focus on Strategy Outcome 2: Organisational Resilience

Resilience NSW
GPO Box 5434
SYDNEY NSW 2001
(02) 9212 9200

Authors: Bill Bryant, Chris Quin (Resilient Projects).

Acknowledgements: The contributions made by all the stakeholders involved in the planning, workshops, and development of the NSW Critical Infrastructure Resilience Strategy 2018 are acknowledged.

Disclaimer

This document has been prepared by the Department of Justice for general information purposes and while every care has been taken in relation to its accuracy, no warranty is given or implied. Further, recipients should obtain their own independent advice before making any decisions that rely on this information (2021).

Table of contents

Introduction: Critical infrastructure resilience

The critical infrastructure (CI) of NSW is exposed to an increasing number of threats, hazards, shocks and stresses.[1],[2] Disruptions to critical infrastructure can result in loss of life, negative economic impact and harm to communities, including psychological distress.[3] More frequent natural disasters of greater magnitude[4], and a heightened risk profile in relation to criminal threats including cyber-attack[5],[6] mean NSW's infrastructure and organisations must be more resilient than ever.

The Critical Infrastructure Resilience (CIR) Strategy promotes critical infrastructure that can:

- withstand shock events to continue operating; or
- be returned to service as soon as possible after any disruption; and
- responds to long-term stresses.

A focus on physical infrastructure alone will not achieve this. This strategy has three outcomes:

- Improved **infrastructure resilience**;
- Improved **organisational resilience**; and
- Improved **community resilience**.

To achieve these outcomes, priority is given to:

- **Partnering** for shared responsibility around critical infrastructure resilience;
- **Preparing** for all hazards, not just the ones we can foresee; and
- **Providing** continued service from critical infrastructure with minimal disruption.

Together we can build a safer, more secure and more resilient NSW.

Key terminology

Critical infrastructure (CI) is the assets, systems and networks required to maintain the security, health and safety, and social and economic prosperity of NSW. These are underpinned by the organisations and people that support them.

Infrastructure providers include any organisation that provides NSW critical infrastructure, including privately owned organisations, local government, state government, and government-owned corporations.

Critical infrastructure protection (CIP) minimises vulnerability to criminal or malicious threats via physical, procedural, person-based, and electronic defences. CIP is a key part of CIR. At the national level, CIP focuses on mitigation against the specific threat of terrorism. [7]

In NSW, CIP is delivered jointly by the NSW Department of Justice through the Office for Police and the NSW Police Force, by working closely with other NSW agencies and the owners and operators of CI.[8] This Strategy complements existing CIP arrangements by encouraging CI providers in the all-threats and all-hazards approach to protecting CI.

Critical infrastructure resilience (CIR) is the capacity of CI to withstand disruption, operate effectively in crisis, and deal with and adapt to shocks and stresses. It includes the flexibility to adapt to present and future conditions. At the national level, CIR is the term used to describe an 'all hazards' approach to CI activities across the spectrum of prevention, preparedness, response and recovery.

In NSW, while infrastructure providers retain responsibility for CIR, it is delivered as a partnership between infrastructure owners, infrastructure operators, the NSW community, and local, state and federal government.

Within this strategy, CIR outcomes are divided into three categories, or types of resilience:

Infrastructure resilience (IR) is the resilience planned for, designed, and built into assets, networks and systems.

Organisational resilience (OR) is the resilience of the organisations, personnel and processes supporting infrastructure to supply a service.

Community resilience (CR) focuses on the role the community plays in building and maintaining its own resilience while contributing to critical infrastructure resilience.

Strategy Outcome 2: Improved organisational resilience

Organisational resilience refers to the resilience of the organisations, personnel and processes supporting the infrastructure to supply a service.[9]

The people and organisations that support infrastructure have as much impact on CI resilience as the assets, systems and networks themselves. Without holistic resilience across the people, systems and physical elements, the resilience of NSW CI will not improve. The CIR Strategy encourages organisational resilience for all CI providers so they can improve together and provide a reliable and safe service to NSW.

Organisational resilience is not just for infrastructure providers, it is also for community and business users of critical infrastructure – to ensure they have planned for what to do when interruptions to infrastructure service provision affect their organisation.

The benefits to business of enhanced organisational resilience are not reserved for emergencies. Enhanced organisational resilience improves organisational culture and ability to solve business problems. [9]

The graphic below identifies ways to improve organisational resilience. These are expanded upon within this guide.

Figure 1: Improving organisational resilience[10]

Organisational resilience framework

Organisational resilience refers to an organisation's ability to adapt and evolve as the internal and external environments are evolving, to absorb, deflect, respond to and recover from short term shocks — be they natural disasters or internal business disruptions — and to adapt and shape itself to respond to longer term challenges brought about by changes – for example in technology, politicals/legal/regulatory environments, climate, social, economic and market conditions.

Why organisational resilience matters:

- The viability and sustainability of organisations continues to be tested in a world that is constantly changing.
- Many organisations are realising that traditional corporate strategies are not protecting them from unexpected events.
- Organisations need to be able to absorb an event that necessitates change, to adapt and continue to maintain their competitive edge and profitability.[11]

For CI providers, the community and the economy increasingly rely on highly-available infrastructure – whether that is water, energy, food, communications, healthcare, transport networks, banking & finance, education, or the built environment. The CI must not only be available, accessible and reliable, but the CI providers themselves must be able to continue to deliver, support and maintain that infrastructure – even in the immediate aftermath of a disaster event.

Global experience following significant disaster events demonstrates that the recovery and continued availability of critical infrastructure has a direct impact on how an impacted community recovers and the speed of that recovery. Examples include Hurricanes Katrina and Sandy in the US, cyclones Debbie, Oswald and Yasi in Australia and flooding events in many Asian countries.

Disruptions to the operation of critical infrastructure come not only from natural events (storm, cyclone, earthquake, landslide, tsunami etc.) but can come from other sources, such as supply chain failures (volcanic ash clouds disrupting transportation, fuel shortage, industrial action, supplier closing its operations etc.), technology failures, direct human activity (fraud, theft, malicious damage, terrorism, cyber threats), indirect human activity (accident, lack of/improper maintenance), and staff shortages (industrial action, pandemic, skills shortage due to competitor activity).

Each organisation will need to develop its own definition of resilience based on the organisation's objectives, its structure, stakeholder expectations, operational capabilities and capacity. It is important to recognise that resilience is a **journey of increasing maturity**. Resilience is not a single set of criteria to check off and declare the organisation to be "resilient", but more a state or condition that the organisation aspires to, which can change over time. Resilience is more a reflection of the culture of the organisation and the capability of its people than being an auditable checklist of activities.

Having said that, there are some established disciplines and activities that provide the organisation with a solid foundation to help develop the right culture. These are identified in the organisational resilience framework diagram (Figure 2) that follows the prevention, preparation, response and recovery (PPRR) model that has been widely adopted by Australian state, federal and emergency service agencies. Improved resilience is achieved through effectively harnessing and integrating these disciplines into the organisation's decision-making framework. These foundation disciplines are outlined in subsequent sections and include:

- risk management
- security management (both physical and digital security)
- emergency management (including incident, disaster & crisis management)
- business continuity management
- ICT disaster recovery management
- insurance management.

Figure 2: Organisational resilience framework

In a resilient organisation the processes of these foundational disciplines (identified in the green objects in Figure 2) should be considered in the decision-making process of all the organisation's other disciplines (identified in the light grey objects in Figure 2) and would support the organisation's purpose and objectives. An organisation's resilience capacity is developed through the application of the disciplines and through the commitment to a foundation of good corporate governance and continual improvement in the capability of its people.

Leading organisational resilience

Resilience is not just sound risk management, effective emergency/crisis management or business continuity management. It is an organisational approach that embraces asset and resource protection, performance and strategic leadership, organisational development, and a responsive and adaptive culture.[12] The community benefits of embedding resilience thinking into the planning, design and operation of services from infrastructure create a **double dividend** of avoided costs from disasters, but also co-benefits that arise even in the absence of a disaster.[13] These benefits not only include the reduction in the organisation's costs in future disruption events. It also includes increased utility and service to customers and communities, less revenue loss (resulting from service disruptions), improved business and consumer confidence, positive impact on productivity and economic growth and potentially lower insurance premiums.

Resilience isn't achieved through having plans, processes and documents that sit on a shelf gathering dust. Rather, it is achieved through the commitment of an organisation's leaders to place an emphasis on driving the right culture and capability within that organisation. It is

achieved through the appropriate allocation of time, effort and resource with a clear focus on the resilience objectives for the organisation. It is further achieved by the engagement of all employees through a comprehensive training, education and awareness program.

This can only be effectively achieved when the organisation's leaders are fully engaged, committed and providing direction to their people. Senior management understands the goals and objectives of the company and is ultimately responsible for their achievement. With senior management's support, organisational resilience and the enabling management disciplines of risk, security, emergency, business continuity and insurance will gain added importance and focus. Management sets the tone and direction of the resilience program and can define what is most critical.

Assessing organisational resilience maturity

To assist in progressing along the resilience maturity path it is useful to understand where the organisation is currently, where its leaders wish to get to, and what is needed to be done to cover the gap.

Because organisation resilience is not a technical discipline in its own right, there is no over-arching technical "standard" that can be applied, or have the organisation's performance assessed against, although there is a standard that provides some guidance regarding the principles of organisational resilience – "ISO22316 Organizational resilience – Principles and attributes". The organisation's leaders must determine their own resilience objectives.

The Trusted Information Sharing Network (TISN), through its Resilience Expert Advisory Group (REAG), have developed an organisational resilience model for critical infrastructure organisations that identifies three key attributes of a resilient organisation together with 13 behavioural indicators (figure 3)[14].

Figure 3: Organisational Resilience Model[14]

These behavioural indicators are used to determine how well an organisation demonstrates organisational resilience attributes. To facilitate an assessment of the organition's resilience maturity, TISN has developed a "healthcheck" tool that asks a series of questions to assess an organisation's level of performance across the 13 indicators. This tool then provides suggestions regarding possible actions to improve resilience in specific areas and inhibitors that might be preventing the organisation from developing resilience. This information can be used to develop strategies and initiatives to mature the organisation's resilience capability.[15]

It is noted that there are other resilience assessment tools available online. The British Standards Institution offers an Organisational Resilience Benchmark[16] tool that offers to benchmark an organisation against a database of 1,250 other organisations by assessing 16 indicators across 4 key attributes. However, the TISN tool has been developed for CI organisations operating in the Australian context.

Further reading

Organisational Resilience: A Position Paper for Critical Infrastructure – www.tisn.gov.au/Documents/Organisational+Resilience+PDF.pdf

The Triple Dividend of Resilience: Realising development goals through the multiple benefits of disaster risk management. 2015. Global Facility for Disaster Reduction and Recovery (GFDRR) at the World Bank and Overseas Development Institute (ODI) – www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/10103.pdf

TPP18-07 Organisational Resilience Guidelines: Practitioner Guide for the NSW Public Sector Organisations – www.treasury.nsw.gov.au/sites/default/files/2018-09/TPP18-07%20Organisational%20Resilience%20-%20Practitioner%20guide%20for%20NSW%20Public%20Sector%20Organisations.pdf

CEO Perspectives on Organisational Resilience – www.organisationalresilience.gov.au/Documents/ceo-perspectives-on-organisational-resilience.pdf

Organisational Resilience Good Business Guide 2016 – www.organisationalresilience.gov.au/Documents/Organisational-Resilience-Good-Business-Guide.PDF

Organisational Resilience: The Relationship with Risk Related Corporate Strategies – www.organisationalresilience.gov.au/Documents/organisational-resilience-the-relationship-with-risk-related-corporate-strategies.pdf

Resilient Organisations: Resilience Guides – www.resorgs.org.nz/resources/resilience-booklets/

Organisational Resilience HealthCheck www.organisationalresilience.gov.au/HealthCheck/overview

Foundations of OR: Risk management

Risk Management is a fundamental management discipline that should be embedded right across an organisation to facilitate better decision-making in all other management disciplines and processes. Whilst it is not the only input to decision-making, risk management provides a framework and foundation that considers the organisation's objectives and seeks to identify the opportunities and threats that might exist to enhance or hinder the organisation in achieving those objectives. At its core, risk management provides insight to prioritise the activities and initiatives of the organisation and the allocation of its finite resources.

The ISO31000:2018[17] risk management standard defines risk as "*the effect of uncertainty on objectives*". Risk lies in the uncertainty around how an organisation might successfully achieve its objectives, so managing risk is about seeking to provide as much certainty as is practicable. It is NOT about managing and mitigating every single risk that an organisation might identify as that would take too much time and cost too much money. It IS about identifying the material risks (i.e. those risks which, if realised, would have a material impact on the achievement of an objective) and determining how much of the organisation's resource could, or should, be applied to mitigate those material risks.

It should be recognised that there are different types of risk management:

- **Enterprise risk management** is the term that refers to the overall framework for managing risk within an organisation.
- **Strategic risk management** is the activity that considers the external and aggregated internal risks that would impact and influence the organisation's purpose, strategies and direction.
- **Financial risk management** is activity focussed on the specific financial objectives of the organisation and relies heavily on quantitative analysis of the financial consequences of risk and the likelihood of those consequences occurring.
- **Operational risk management** is activity that considers the opportunities and threats to the achievement of the organisation's operational objectives.
- **Project risk management** is activity used within project and programs to manage the project scope, design, development, delivery and operate & maintain risks.
- **Safety risk management** is activity that typically focuses on hazards to human health and safety but should also consider the safety and security of equipment and assets.
- **Task/activity risk management** is the activity used by individuals and teams to successfully complete specific tasks and operational activities.

Whilst these individually address risks at different levels within an organisation, and within a specific context, the same risk management framework can be used to identify, analyse, treat, review and communicate risk throughout the organisation. By managing risk well, the organisation can reduce the impact of unexpected events and provide more certainty to its employees, stakeholders, shareholders, customers and the community regarding the ongoing operation of CI and delivery of services.

Two useful enterprise risk management frameworks exist to help develop an organisation's risk management framework – the International Organization for Standardization "ISO31000:2018 Risk Management Guidelines" and the COSO "Enterprise Risk Management – Integrating with Strategy and Performance".

ISO31000 is a globally adopted standard that focuses wholly on the components of a comprehensive risk framework. COSO is a US-based framework developed to design, manage and audit an organisation's internal controls, with Enterprise Risk Management a specific activity within that framework. Neither of these will provide a boiler-plate design to be adopted by an organisation. Each organisation should develop its own framework and

processes (based on their chosen guiding standard) that is fit-for-purpose according to the organisation, its objectives, its structure, the industry, the markets it operates in and the infrastructure it owns and/or operates.

Further reading

Sendai Framework for Disaster Risk Reduction 2015–2030 – www.unisdr.org/we/coordinate/sendai-framework

National Emergency Risk Assessment Guidelines. Australian Disaster Resilience Handbook Collection. Handbook 10 – knowledge.aidr.org.au/resources/handbook-10-national-emergency-risk-assessment-guidelines/

NSW Government, Resilience NSW – 2017 State Level Emergency Risk Assessment: Executive Summary – https://www.opengov.nsw.gov.au/publications/19463

Resilience Priority 1: Partner

"*We must **Partner** in shared responsibility for critical infrastructure resilience."*[10]

To be truly resilient an organisation cannot operate in isolation but must partner, both internally and externally, to understand and support their customer and community needs and to draw upon specialist skills and resources in times of need. To quote Ethel Barrymore – "*The best time to make friends is before you need them.*"

Developing networks and support communities and developing an understanding of each other's needs, capabilities, limitations and dependencies in peace time ensures that everyone is prepared and ready to respond when a disruption event occurs.

Community groups, industry bodies, special interest groups (e.g. the Trusted Information Sharing Network sector groups), emergency management organisations, communities of practice (e.g. NSW Organisational Resilience Community of Practice) – these are just some examples of the groups that currently exist and have resilience high on their agenda. These groups provide valuable ways of connecting with skilled and experienced practitioners and developing mutual aid agreements to provide support through provision of people, knowledge/advice, equipment and material supplies when an organisation is responding to, and recovering from a significant disruption event.

OR Activity: Capability improvement

The true level of resilience of an organisation is inextricably linked to the skills, abilities and attitudes of the people within it. It is the people who implement the plans and conduct the activities identified in all of the organisation's processes and, in particular, the OR disciplines. The best fit-for-purpose plans and procedures are of little use if people are unaware of them, unable to implement them or lack the skills or ability to undertake the specific tasks and activities that need to be completed. It makes sense that as much effort (if not more) should be expended in preparing and equipping the organisation's people to prevent, prepare for, respond to and recover from disruption events as is spent on developing the policies, standards, guidelines, plans and procedures that form the OR framework.

There are two elements to capability improvement in an OR context: Capability and personal resilience.

Firstly, the development of the technical skills, knowledge and capability to fulfil the variety of roles and responsibilities identified through the various OR disciplines. These are developed through formal training programs, education and/or on-the-job training. A useful model that can be applied to the challenge of capability improvement is provided in Figure 5. This ties in all elements of the OR framework as the improvement needed can be identified at any point across the framework (or organisation generally), either as a result of risk analysis or following an operational activity or incident. The improvement initiative (in this context being training of employees) needs careful planning and development to ensure not only effective delivery of the training event but that the appropriate change in knowledge, skill and behaviours is achieved. This can be validated by evaluation either following an exercise or real incident and the review determines whether further needs exist.

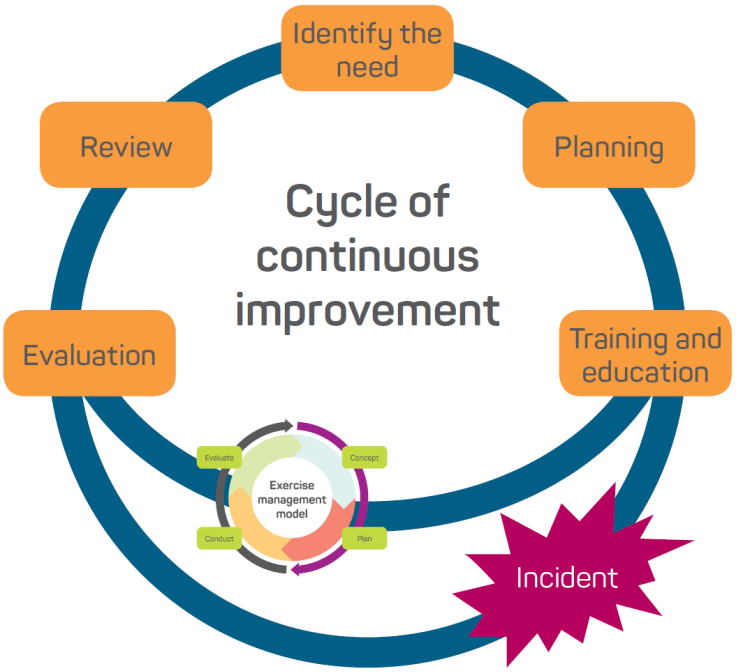

Figure 4: Continuous improvement model[18]

Secondly, there is development of personal resilience. Like organisational resilience, personal resilience is the process of adapting well in the face of adversity, short term shocks (e.g. trauma, tragedy, threats etc.) or significant sources of stress (e.g. unsustainable workloads, change etc.). Resilience is not a trait that people either have or do not have. It involves behaviours, thoughts and actions that are developed through personal experience but can be learned and developed in anyone. Personal resilience is described as "*the capacity of employees, facilitated and supported by the organisation, to utilise resources to positively cope, adapt and thrive in response to changing work circumstances*."[19] This definition proposes that employees are not simply surviving through disruptive events but that they are managing actions towards a positive outcome and learning through the process.

The organisation has a large role to play in developing and facilitating employee resilience. Many studies show that a significant contributor to personal resilience is having caring and supportive relationships, and that operating in an environment that values communication and trust enables employees to learn and experiment. Signs of personal resilience include:

- Having the capacity to make realistic plans and take action to achieve them;
- Individuals having a positive view of themselves and confidence in their strengths and abilities;
- Individuals developing their skills in communication and problem solving;
- Individuals having the capacity to manage strong feelings and impulses.

All of these are factors that individuals can develop in themselves and directly contribute to the overall resilience of an organisation. The organisation should be continually seeking opportunities to assist their people to develop, learn and practice these traits, with the preference being that personal resilience is built in a managed and considered way through training and exercising, rather than as an unplanned consequence of real emergency events. This is particularly important for people who are engaged in the response and recovery elements of the OR framework so they can contribute in a calm, considered state of readiness.

Further reading

Adversity Leadership
www.organisationalresilience.gov.au/Documents/AdversityLeadership.pdf

Staffed or Stuffed: Creating resilience through your people
resorgs.org.nz/wp-content/uploads/2017/07/Resilient_Organisations_Staffed_or_Stuffed_online_version.pdf

Building Adaptive Resilience: High performing today, agile tomorrow, thriving in the future
resorgs.org.nz/wp-content/uploads/2017/07/Resilient_Organisations_Building_Adaptive_Resilience_online_version.pdf

Decision Making During A Crisis: A Practical Guide
www.organisationalresilience.gov.au/Documents/decision-making-during-a-crisis-a-practical-guide.pdf

OR Activity: Exercising and lessons learned management

Building on the theme of Capability Improvement, one of the best ways for providing people with experience of the response and recovery activities without the stress of a real event is through exercising.

The primary purpose of an exercise is to ensure that plans, and the people implementing those plans, work when they are needed. Exercises offer a legitimate and effective means of improving understanding of the response and recovery plans and procedures, and the various roles, responsibilities and inter-dependencies that exist in a coordinated response and recovery effort. Exercises are a useful and effective way of evaluating and validating the content of the plans and the processes and procedures contained within them. They also provide an opportunity to test and evaluate new ideas, procedures or equipment. Exercising should be considered an essential component of the continuous improvement effort in organisational resilience.

Another reason for conducting regular testing and exercising is to ensure any changes within the organisation are reflected in the plans and that the efficiency and effectiveness of the response and recovery effort is maintained.

Changes might be made to organisational structure, roles, technology, business processes or equipment, and the implications of those changes can be understood and communicated to the relevant stakeholders as part of the planning and design of the exercise, with any changes to plan content validated during the exercise. Additionally, they provide the ability to assess inter-organisation links, processes and dependencies: to challenge previous assumptions regarding an external organisation's activities, capabilities and response priorities. By their nature, exercises are a collaborative activity that need to embody the partnering approach to develop trust, understanding, and a higher level of engagement between teams and departments both internal and external to the organisation.

There are different styles of exercise that can be utilised, depending on how mature an organisation's response and recovery plans are, the roles and responsibilities defined in those plans, the experience of the people undertaking those roles and whether the exercise is for a single team, department, whole organisation or multiple organisations.

Depending on the exercise objective, the organiser might choose either a discussion style of exercise or an activity based/simulation style of exercise. Discussion style exercises are generally easier to organise, develop and run as they involve people discussing the exercise scenario and verbally walking through the tasks, activities and actions that would be taken over a period of time. Simulation style exercises require considerably greater effort in developing, coordinating and running as they require real-time activities and thinking to occur with the scenarios sufficiently defined to anticipate the possible decisions and activity outcomes. Simulations can be much more effective in assessing the response and recovery procedures, the capabilities and competencies of team members and the interactions and integration of cross-team functions.

For an exercise to be effective there needs to be some clear objectives for the exercise. Thought needs to be applied regarding the plan(s) to be exercised, what the outcomes might be, what changes might be expected as a result of the exercise, and what disruption risks need to be tested against. In choosing the style of exercise there should be consideration of the participants and their roles, the time and resources available, the complexity of the proposed exercise scenario and needs of the stakeholders.

Given that smaller, less disruptive, yet unplanned, incidents occur quite frequently within organisations, an organisation might also consider using these small real incidents as an opportunity to exercise their plans and consider the scenario if the event had been much larger in scope and severity. Just like sporting teams use training to rehearse their plays and set pieces in order that their movement and actions become instinctive in the heat of the game, exercises give the organisation's response and recovery teams that much needed practice to become a cohesive and effective emergency management team when a larger scale event occurs.

One of the major outcomes of any plan activation, whether as a result of an exercise or real event, is to learn from it and improve both the plan contents and also the knowledge, skills and capability of the team members. It is also an opportunity to reflect on how effective the current arrangements are and identify areas that can be improved upon. As changes occur within organisations, their processes, the technology they employ, the environments they operate in and the skills required of their people the existing plans may become outdated or inappropriate. Exercises seek to tease this information out and this new intelligence should be captured, validated and acted upon.

Formally reviewing operational events and exercises (often referred to as a 'debrief') enables the organisation to better understand its disruption risks and how the organisation is equipped to manage them. This, in turn, should inform decisions regarding the need for process change, training and upskilling of its people, revisions of roles and responsibilities and operational performance requirements.

Effective reviews need a commitment from the organisation to not only invest the time and effort into conducting debriefs and identifying the lessons to be learned, but also to implement changes within the organisation as a result. This should include the ongoing monitoring and evaluation of those changes to ensure they are implemented and provide the required improvement in efficiency and/or effectiveness. The Infrastructure Resilience Process provided in the Infrastructure Resilience Guide provides a continuous improvement model that should be applied when turning the information gathered in the lessons learned process into implemented improvement actions.

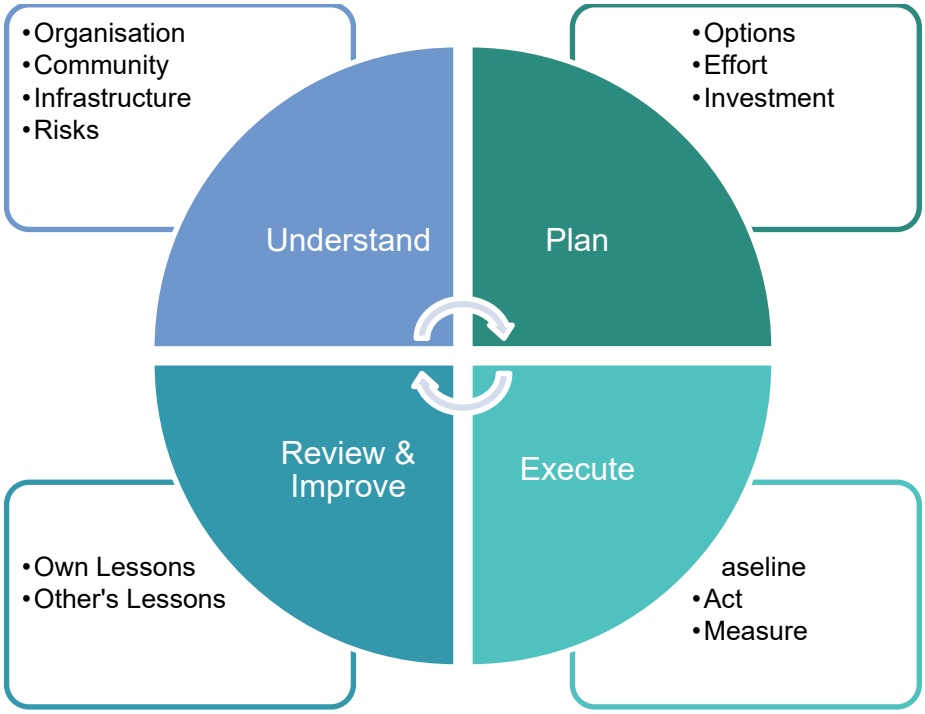

Figure 5: Continuous improvement model[20]

To be effective, the proposed change must consider the desired outcome in the context of the organisation and its capability. Therefore, a thorough **understanding** of the organisation's operating environment, infrastructure, available resources and ability of the organisation to implement the proposed changes must be developed during the lessons management phase. This information will help determine the scope of the change and the approach needed to implement and effect the change.

The change must be **planned** to determine the appropriate option for the change itself but also to identify the organisational change activity that must also be undertaken to ensure the change is effective. For example, changes to equipment, response/recovery processes, role duties or team structures etc. will require procedural changes to be documented, communicated and might even necessitate additional training.

The changes must be **executed** in accordance with the plan with all change activities managed across the organisation in a controlled and coordinated manner. This will ensure that all stakeholders are informed of, and understand, the purpose of the change, the outcome desired from the change and the revised process and procedures to be followed.

Once implemented, the impact of the change should be **reviewed and monitored** to ensure the benefits sought by the change are, indeed, delivered. This would, ideally, be done through additional exercising prior to a real disruption event but, at the very least, should be reviewed

as part of the next lessons learned process following a real event. Frequently, further amendments are implemented to **improve** a change as a result of real-world experience.

Further reading

Managing Exercises. Australian Institute for Disaster Resilience Handbook Collection. Handbook 3 – knowledge.aidr.org.au/resources/handbook-3-managing-exercises/

Lessons Management. Australian Institute for Disaster Resilience Handbook Collection. Handbook 8 – knowledge.aidr.org.au/resources/handbook-8-lessons-management/

Resilience Priority 2: Prepare

"*We must **Prepare** for all threats and all hazards, not just the ones we can foresee.*" [10]

In the context of organisational resilience, effective preparation begins with a comprehensive understanding of the disruption risks faced by the organisation and the impacts that disruption will have on the achievement of the organisation's objectives, its people, customers, communities and stakeholders. The organisation should strive to **prevent** (where possible) the disruption events from occuring and **prepare** for those disruptions that cannot be controlled by the organisation. This requires not only preparing for a repeat of events that have occurred in the past but undertaking horizon scanning of the environments that the organisation operates within, such as political, social and behavioural, legal and regulatory, economic, technological, and environmental, to anticipate and understand changes and the potential for different disruption events that might occur in the future.

OR discipline: Security management

The Australian Government Protective Security Policy Framework defines Protective Security as "a combination of procedural, physical, personnel, and information security measures designed to protect information, functions, resources, employees and clients from security threats."[21] Security Management is a management discipline and a systematic set of risk management activities that ensure safe and reliable operation, and thus reduce the likelihood of the negative impacts from unauthorised access to, control or use of the organisation's resources (which includes its buildings, facilities, assets, equipment, people, money, systems, data and intellectual property). Typically, responsibility for physical security is allocated separately to responsibility for digital security, although there is often interdependency.

Physical security focuses on the prevention of unauthorised access to physical resources by controlling who gains entry using physical barriers (e.g. locked entry points, electronic access control, security guards, high fences etc.). Digital security focuses on the prevention of unauthorised access to, and use of, the organisation's ICT systems and data/intellectual property. The objective of both is to understand and control who should have access, to identify, prevent or delay access attempts made by unauthorised entities and to provide early alert to successful breaches of the security measures. Responses to those breaches might be managed through the emergency management process.

Good security helps to prevent business disruptions by ensuring security, integrity and availability of organisational resources and contributes to the mitigation of the organisation's fraud, financial, safety, legal, operational and reputational risks. A security risk assessment is

crucial. Without an assessment, it is impossible to design good security policies and procedures that will defend your organisation's critical resources.

Identifying threats and vulnerabilities is an important part of the security risk management process. Threats can occur as a result of human or natural factors and can be caused by internal or external events. Figure 4 identifies some common threats to security. This is not meant to be an all-inclusive list but indicates some of the ways in which the organisation can be threatened. Threats can also occur due to other reasons, such as errors in computer code or accidental or unintentional actions of employees.

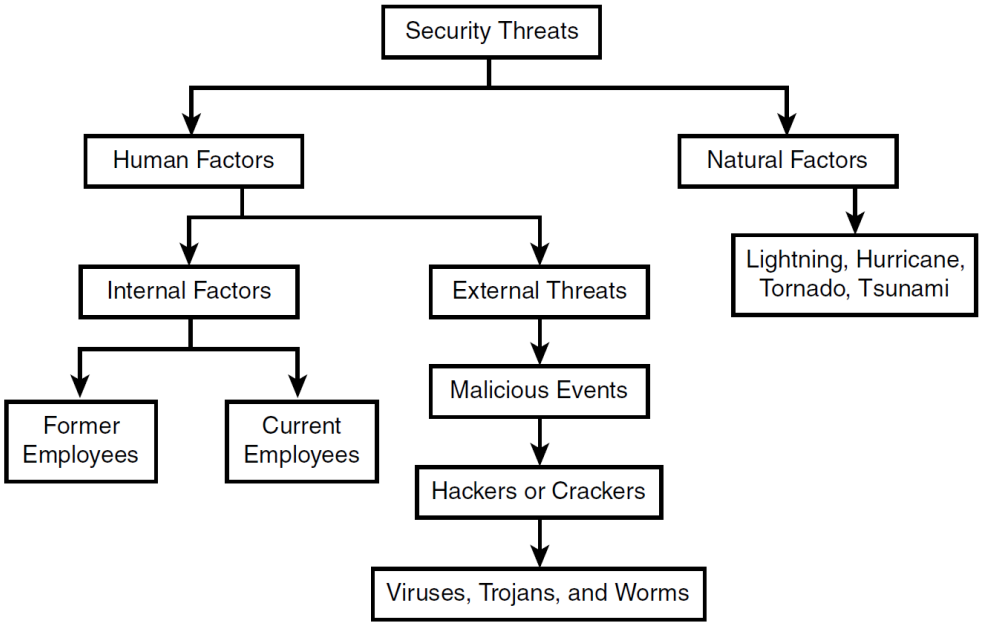

Figure 6: Security threat sources [22]

Good security management ensures that the organisation:

- has established security policies, standards, guidelines and procedures that staff are aware of and implement
- has responsibilities and accountabilities defined, agreed and documented
- has a comprehensive set of identified and assessed security risks with a prioritised set of control measures and actions to cover any unacceptable risk exposures
- identifies and proactively manages its authorised users and controls access levels to specific resources
- has a visitor management process to understand and manage who is accessing their resources
- has a proactive security monitoring, alert, reporting and assurance capability
- conducts identity verification and background checks (where appropriate) on staff, contractors and service providers
- has a security incident response capability that is documented, communicated and exercised, with specific access/penetration testing conducted on prioritised resources;
- engages with external entities (e.g. police & counter-terrorism agency, TISN, industry regulators etc.) to understand the current threat environment
- conducts employee awareness and training to foster a security-conscious workforce.

Further reading

Physical Security Management Guidelines: Security Zones and Risk Mitigation Control Measures – matryxconsulting.com.au/wp-content/uploads/2015/06/Australian-Government-physical-security-management-guidelines-Security-zones-and-risk-mitigation-measures.pdf

The Insider Threat To Business: A Personnel Security Handbook – www.organisationalresilience.gov.au/Documents/the-insider-threat-to-business.pdf

National Guidelines for Protecting Critical Infrastructure from Terrorism – www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

OR discipline: Insurance management

Insurance Management implements a risk mitigation control that seeks to protect the organisation from financial loss and assist with the recovery from a disruption event by:

- providing capital to repair assets/equipment or to rebuild infrastructure; and/or
- replace irreparably damaged, lost or stolen assets and equipment; and/or
- replace lost income or revenue; and/or
- cover third party liabilities.

The essential pre-activity to implementing an effective insurance program is risk assessment. This should identify the insurable risks that the organisation faces and determine the level of risk the organisation can tolerate (based on its risk appetite) in order to establish the appropriate level of insurance cover. Some insurance is compulsory for an organisation (e.g. workers' compensation for employees) or a financial institution may insist on the organisation maintaining certain minimum levels of insurance cover.

The cost of insurance reflects the level of cover sought and the insurer's assessment of the likelihood that the organisation will make a claim, considering the risk factors that would give rise to an insurable loss occurring. It also includes the insurer's business costs. Insurance cost can be reduced by managing the likelihood of a risk event occurring and claims being made. This can be greatly influenced by the organisation's risk management, infrastructure resilience, security management, emergency management, business continuity and insurance management programs and having the insurer engaged in better understanding how these programs reduce their risk exposure.

For example, programs that harden infrastructure assets to natural weather events reduce the likelihood of storms and floods damaging them. Where this can be measured and demonstrated the result could be expected to be a lower insurance premium due to the reduced likelihood of a claim being made. However, there are many factors that might influence the cost of insurance, including:

- inflation;
- changes in government taxes and any state duties or levies;
- the number of claims experienced in that industry or location;
- large-scale claims due to natural weather events such as floods and cyclones;
- investment returns – insurers invest premiums to help ensure they have sufficient capital to pay future claims and poor returns may require a lift in premiums;
- regional or global changes that affect the price and availability of reinsurance;
- the value or quantity of what you are insuring may have changed; and
- the insurer's cost of doing business.

Further reading

Cover Your Assets: A Short Guide on Selecting & Getting the Best from Your Commercial Insurance Policy –
resorgs.org.nz/wp-content/uploads/2017/07/Resilient_Organisations_Cover_Your_Assets_print_version.pdf

Insurance –
www.business.gov.au/Risk-management/Insurance

Understand Insurance –
understandinsurance.com.au/types-of-insurance/business-insurance

Resilience Priority 3: Provide

"We must **Provide** critical infrastructure services with minimal interruptions." [10]

For the disruption risks that cannot be prevented, the organisation must be prepared to **respond** quickly and be able to **recover** any business functions or services that were impacted by the disruption event.

The negative impact on society and to the economy increases rapidly while essential services remain unavailable. The recovery costs also rise, not just the direct costs in labour and materials to restore the infrastructure and services, but the indirect costs in lost production, increased insurance and compensation claims, business failures, forced migration of displaced residents, increased welfare and benefits payments.

Building infrastructure to withstand impact from external shocks and stresses is the goal but, where that is not economically achievable, having an ability to respond and recover from a disruptive impact is essential.

OR discipline: Emergency management

The emergency management discipline provides a responsive capability by coordinating the organisation's people and activities to effectively respond to any unplanned event. Performing a risk assessment will help an organisation determine those events, both internal to the organisation and externally, that would have a disruptive impact on the CI it provides and the communities it serves.

These events can be known by different names – incident, emergency, disaster or crisis. It is useful to develop definitions within the organisation in order that everyone understands the scale of the event and severity of its impact. For example:

- An “Incident” might be described as an unplanned event that can be managed and recovered from using Business-As-Usual resource and processes;
- An “emergency” might be described as an unplanned event that requires an immediate and coordinated response, through a formal emergency management structure, to prevent escalation of its scale or severity and to protect the organisation’s employees, customers and assets;
- A “Disaster”, in the context of CI, typically means a large external event impacting communities and multiple CI providers that endangers the safety and wellbeing of people, causes significant damage to, or loss of, property and/or negatively impacts communities and the local or regional economies;
- A “Crisis” might be defined as a situation (whether a single event or a sequence of compounding events) that threatens the ongoing viability of the organisation requiring the intervention of the most senior executives, board and specialist advisors to manage.

Having a structured and coordinated response capability ensures that the organisation identifies the roles, responsibilities, tasks, activities and stakeholders that need to be considered and engaged when responding to an incident, emergency, disaster or crisis. Having it established prior to a disruption event means that, during an event, people do not have to identify key tasks and activities whilst under pressure but can refer to guidance detailed in an emergency management plan. Plans enable people to understand not only their own role, responsibilities, key tasks and activities but also those of the rest of the participants in the emergency management team. Further, a well-defined plan identifies the communications that must occur between identified stakeholders both within the organisation and external to it.

The Australian Inter-Service Incident Management System (AIIMS) is the Incident Control System used by all fire, emergency service and land management agencies within Australia. It provides a set of core principles and guidance in the development of an organisation’s emergency response capability and incident management team structure. Whilst it has been designed for use by the emergency response agencies in large scale disasters, AIIMS provides a common management system that facilitates the effective and efficient coordination of all activities in the resolution of any incident. It has been adopted as the incident management methodology by many CI providers across Australia is it is highly adaptable and scalable to support the management of small or large, simple or complex incidents.

When an incident occurs (or appears likely to occur), no matter what the size, the organisation’s emergency management team should activate its plans and engage all internal stakeholders to gain situational awareness. This is a principle of “Go Big, Go Early” identified as a learning outcome following large scale natural weather events from around the globe. For large-scale events, delay in responding can have catastrophic impacts on the lives and wellbeing of impacted communities (e.g. the increased impact in lives lost and community disruption of Hurricane Katrina compared to Hurricane Sandy).

For smaller scale events, or evolving events in which the final impacts are yet to be determined, pulling all relevant stakeholders together in the early stages of the event ensures a common level of understanding of the event as it unfolds. It is easier to stand down emergency responders if the scale of the event remains small than it is to stand up responders late into an event. Additionally, for small scale events it can be a good opportunity for team members to rehearse their response in preparation for larger events.

An organisation’s emergency management team should include representation from across the business (e.g. its operations functions, communications & stakeholder engagement, human resource, workplace health & safety, environment, property services, procurement, fleet & logistics, legal, finance, etc.). It is difficult, if not impossible, for one person to understand the impacts of an event on all the organisation’s functions and processes and,

therefore, what its response actions need to be. It makes sense to have those key stakeholders engaged in providing situational awareness and identifying response actions.

Further reading

Australian Inter-service Incident Management System – www.afac.com.au/initiative/aiims

Australian Disaster Resilience Handbook Collection, Handbook 9 – Australian Emergency Management Arrangements – knowledge.aidr.org.au/resources/handbook-australian-emergency-management-arrangements/

Incident Management Handbook (coming soon) - knowledge.aidr.org.au/resources/handbook-14-incident-management-in-australia/

Leading in Disaster Recovery: A Companion Through The Chaos – resorgs.org.nz/wp-content/uploads/2017/09/leading_in_disaster_recovery_.pdf

Chaos To Teamwork: A Leader's Role In Crisis – resorgs.org.nz/wp-content/uploads/2017/09/Resilient_Organisations_Chaos_to_Teamwork_online_version.pdf

OR discipline: Business continuity management

Business Continuity Management (BCM) focuses on responding to, and recovering from, disruption events that impact an organisation internally. Internal disruptions can occur from a multitude of sources. These are events that disrupt the day-to-day business functions and activities of the organisation. The community are increasingly expecting high availability and reliability of the services from CI providers. Tolerance to long periods of unavailability is reducing, and dissatisfaction not only impacts the reputation of the CI provider but is generating increased political intervention.

BCM builds upon the disruptive risks identified through the risk management processes and develops the corrective risk controls to recover from a disruption event. BCM doesn't necessarily consider the source of the disruption event. This is because the other OR disciplines of risk management, security management and insurance management consider these and identify the preventative controls that might be implemented to reduce the likelihood of the disruption occurring in the first place. Rather, due to the almost unlimited sources of disruptions, it takes an "all hazards" approach and focuses on the impact of the disruption once it occurs.

BCM provides the organisation with the structured response to recover operational capabilities and critical business functions following disruptions to (BETH3):

- Buildings and facilities;
- Equipment;
- Technology;
- Human resource; and/or
- Third party providers of goods and services.

The starting point to determine the critical business processes and functions that should have a responsive continuity plan in place is using a Business Impact Assessment. This is a method for identifying the impacts from a disruption to the organisation's core services and considers the BETH3 components vital to the delivery of those processes or functions. It also considers the timeframe within which the disrupted items require restoration to prevent unacceptable impacts to the organisation resulting in an ongoing loss of the function.

The analysis should also consider interdependencies with other functions within the organisation, both upstream and downstream of the function being assessed, and identify the key stakeholders to be engaged following an event, either to be notified of the suspension of the function or to be engaged in the recovery of the impacted service or resource.

The objectives of the business continuity plan are to provide a series of actions, identifying roles and responsibilities, to enable the effective recovery from an internally disruptive event. This is to ensure the accountabilities of management and staff are clearly defined when responding to an event and provides the department, work group or team with the strategies to:

- relocate their people following loss of access to a building or facility;
- engage service providers to repair or replace critical equipment following its failure or total loss;
- temporarily implement workaround processes to maintain or restart the function following loss of information and/or communications technology (ICT);
- manage workloads and engage temporary resource following the loss of key resource (for example as a result of illness, accident or industrial action); and
- manage the temporary or permanent loss of critical third party provided goods or services.

It should be noted that the ICT community have their own version of a business continuity plan, referred to as the ICT Disaster Recovery Plan. Whilst this focuses on identifying ICT system criticality to the business which is used to determine system restoration priorities following widespread failure of ICT systems or infrastructure, the methodology used to develop the plan follows the same overall BCM methodology to assess the business impacts, system dependencies and recovery time objectives for the high dependency systems and infrastructure.

Further reading

The Business Continuity Institute (Video): What is Business Continuity? – www.thebci.org/knowledge/introduction-to-business-continuity.html

The Business Continuity Institute: Good Practice Guidelines 2018 Lite Edition – www.thebci.org/resource/gpg-lite-2018-edition.html

NSW Government, Department of Industry – Get Ready Business – www.industry.nsw.gov.au/__data/assets/pdf_file/0008/167831/Get-ready-disaster-tool-brochure.pdf

Appendix A: Case studies

Case study – Organisational resilience as core business: Hunter Joint Organisation of Councils

The Hunter Joint Organisation is preparing a suite of guideline resources focussed on embedding Disaster Preparedness into the Integrated Planning and Reporting Frameworks (i.e. the core business) of Councils across New South Wales.

These resources will directly assist Councils to identify and understand the risks posed to their organisations and local communities from natural disasters, and to better consider and plan (across the PPRR spectrum) for their role in supporting communities withstand and recover from these events.

The focus of the guidelines includes:

- integrating disaster risk and preparedness into planning and operations using the Local Government Integrated Planning and Reporting Framework
- managing Disaster Waste
- the role of Councils in Communicating Disaster Information
- planning for Recovery
- organisational (Corporate) Resilience.

Partner:

To ensure widespread applicability and utility of the guidelines their development has been a collaborative effort, involving contributions from NSW Government Agencies, Emergency Management Authorities, Community Organisations and Councils across NSW – representing a range of roles and responsibilities including enterprise risk management, emergency management, communications, corporate planning and management, asset and infrastructure management, social planning and community services, land use planning and environmental management.

Prepare:

In assisting the councils to better prepare for the future, a more thorough understanding of their disruption risks and likely threats was required. The foundation for this work lies in over a decade of collaborative climate change research, risk assessment and planning (including a strong focus on disaster resilience) undertaken collaboratively by the Councils of the Hunter and Central Coast Region through the Joint Organisation, including:

- Downscaling global climate models to project the regional scale impacts of climate change, with an emphasis on extreme weather events (e.g. bushfire, extreme heat and coastal impacts);
- Developing local and sub regional climate change adaptation plans (encompassing all the regions councils);
- Social research identifying the risk perceptions and levels of preparedness of vulnerable communities to natural disasters;
- Integrating and analysing spatial information datasets representing natural

hazards, demographics and community infrastructure to identify relative community vulnerability (at a Statistical Area Scale) to natural disasters;

- Developing an objective based decision support framework to support Councils plan for the inherent uncertainty posed by climate change for a range of coastal hazards;
- Region wide planning and communication campaigns to raise council and community awareness, capacity and preparedness for the significant health risks posed by heatwaves;
- Pursuing a more consistent "All Hazards" approach to community awareness and education across Councils, community organisations and agencies across the region.

Provide:

Significant elements of this work have been funded through the NSW and Commonwealth Disaster Resilience Program including the Community Resilience Innovation Program (CRIP) and State Wide Emergency Management Projects (SEMP) funding programs.

The work has consistently reinforced the important, often central role that Councils have in supporting communities to prepare for, withstand and recover from natural disaster events. Combined with the region's history of responding to, and recovering from, severe natural weather events, this previous body of work has been a key driver behind the current disaster resilience work of the Joint Organisation.

When complete, the suite of "Is Your Council Disaster Ready?" Guidelines will not only be disseminated and promoted to all Councils across NSW, but their focus and approach will be integrated within the training resources and programs being developed by Resilience NSW for councils across NSW. This will ensure maximum audience reach and ongoing application of these resources by the target audience for whom they have been developed.

For further information on this initiative please contact the Hunter Joint Organisation Environment Division:

Ph. 4978 4020

E envirodirector@huntercouncils.com.au

W www.hccrems.com.au

The Hunter & Central Coast Regional Environmental Management Strategy

Case study: Exercising for ‘Black Sky’ events – EarthEX III / 19

EARTH EX is a self-facilitated, self-assessed, discussion-based, tabletop exercise, that is run annually.

Made available by the Electric Infrastructure Security Council in partnership with The Resilience Shift, EARTH EX III/19 (the 2019 version) was an online interactive exercise available to all registered participants throughout the world. Designed as a come-as-you-are exercise (no required preparation work), the online environment uses videos, dashboards and mapping to create an immersive environment for testing your organisation’s emergency response.

By simulating a multi-jurisdictional long-duration electricity outage due to large scale extreme weather (flooding followed by severe windstorms), organisations from all industries that support critical infrastructure can use the exercise tools to test their emergency planning, preparedness, response and recovery, with a view to building future resilience to extreme hazards.

The exercise highlights the interconnected nature of modern infrastructure systems with simulated large-scale cascading outages to many critical infrastructure services / lifelines.

The objectives of the exercise are to:

1. Improve community resilience to long-duration power outages and Black Sky events through cross-sector planning, training, and exercises.
2. Provide an opportunity to test and refine policies and procedures for responding to a long-duration power outage.
3. Provide an opportunity to facilitate Critical Lifeline Cross Sector discussions.
4. Provide a widely distributed, interactive, multi-language international exercise using new US Department of Homeland Security (DHS) exercise tools.

The exercise is deliberately large in scale – a black sky event. Resilience measures capable of addressing a ‘black sky’ event can’t wait on lessons learned but must rely on lessons imagined and Earth EX provides lots of tools to imagine these extreme scenarios, that while likely to be rare, would have catastrophic consequences for communities.

Case study – Lessons management: NSW SES Lessons Learned Branch

Lessons management is a growing capability across the emergency management sector. This case study explores how several emergency services organisations have collaborated to grow this capability both internally and across the sector.

At the beginning of 2011, the NSW State Emergency Service (NSW SES) established its Lessons Learned Branch with the aim to help the service learn lessons from both corporate and operational activities that would result in improved organisational performance. This was the first lessons management capability for the State Emergency Services nationally. While not a direct response to a formal enquiry or review of the activities of the operations of the NSW SES, the development of this capability followed reviews in other states and was seen as a proactive approach to improving the services delivered to the communities of NSW.

The South Australian Country Fire Service (CFS) had developed a lessons learned capacity following the Wangary Fires in 2005. The Wangary fire and other fires on that day were the most destructive fires, in terms of loss of life and property, that the CFS had seen since the Ash Wednesday fires in 1983. Given the losses, community grief and the coronial inquest into this event, CFS recognised that a more formal approach into learning from these events was required and that the service owed it to the community to demonstrate improvements as soon as possible. This was the first time that a formal approach had been utilised in CFS for collecting, analysing and theming lessons.

The NSW SES Lessons Learned Branch also established a relationship with the National Security Capability Development Division of the Attorney-General's Department (now Home Affairs). This Division had developed a capability for evaluating strategic exercises and identifying lessons from these, including translating these learnings into improved response plans and exercises. The Attorney-General's Department provided linkages to connect a number of agencies nationally to share their lessons frameworks and their learnings about the implementation.

Initial sharing of observations, lessons identified, suggested treatment options and communication challenges between NSW SES and SA CFS led to the interstate exchange of lessons practitioners after major events. In 2017, NSW SES invited practitioners from a number of states to assist with the collection and analysis of data from the 2016 floods in western NSW. Strong collaboration established the relationships that provided the additional resources to enable the analysis of thousands of observations gathered during large-scale events, identify lessons and provide reports for their respective agencies in a timely manner. The lessons identified from this collaboration now form the basis for continuous improvement within the agencies.

The synergies gained through collaboration between lessons practitioners across the emergency management sector contribute to strengthening the lessons capability in each of the participating agencies and result in greater achievements in this sphere than agencies would have achieved working in isolation.

Original Information sourced via the Australian Journal of Emergency Management April 2018 (volume 33, issue 2), "Case Study: Lessons Management Capability in Emergency Management and Beyond" by Heather Stuart & Mark Thomason and republished with the permission of the Australian Institute for Disaster Resilience.

Australian Institute for Disaster Resilience

Case study – Hunter Water: An adaptive organisation

Hunter Water Corporation (HWC) promotes organisational resilience as a tool to strengthen its people to adapt to change, rather than to just cope with the disruptions that are likely to come.

A resilient organisation can withstand shocks and thrive in a changing environment. By eating into the fear of change, HWC promotes resilience to not only deal with shocks and stresses in relation to natural hazards and a changing climate, but the organisation is also better able to adapt to all types of change, including political, regulatory, technological, and business-based change.

Being a resilient, learning, adaptive organisation assists HWC to:

- Adapt to population growth;
- Avoid redundant infrastructure;
- Invest prudently in the right level of service for consumers;
- Plan in a resilient way, not just de-risk decisions;
- Understand and value difference;
- Provide enhanced consumer choice; and
- Provide targeted services to different consumers (e.g. developers, large services).

The board of HWC is highly engaged with the adaptation strategy, with a keen focus on water resilience and learning together – "being thirsty for learning" - both as an organisation and for the people who power the organisation.

HWC's marketing around Love Water, takes community understanding of the need to adapt to a new level, with water not only seen as a precious resource, but as an integrated service in consumer's lives and the community as partner in the supply and management of water as a whole.

By investing in the adaptive capacity of its people, Hunter Water Corporation is positioning itself well to enhance infrastructure, organisational and community resilience.

Appendix B: Resilience Checklist

The following checklist provides a quick assessment of the organisation's preparedness and resilience. This is not intended to be a comprehensive assessment of the maturity of an organisation's resilience program. However, identified gaps from this checklist can be used to inform the organisation's program of work to mature and enhance the resilience of the organisation and the critical infrastructure it is responsible for.

ACTION	EXISTS?
RISK MANAGEMENT	
Risk Management framework is established and supports the organisation's decision-making, with leadership commitment, policy, standards and procedures, roles and responsibilities defined.	
Disruption risks are identified, recorded, assessed and get reviewed periodically to ensure risk controls are agreed, developed, implemented and their effectiveness monitored.	
Disruption risks consider impacts to assets & infrastructure, organisational capacity & capability, legal & regulatory compliance, supply chain, customers & community (in terms of quantity, quality and cost of supply).	
Mitigating actions to manage the disruption risks are recorded, communicated, have an identified owner, have a delivery timeframe and are reported regularly to the risk owner(s).	
SECURITY MANAGEMENT	
Protective security framework exists and identifies owners of security risks & responsibilities (covering physical security of people, property, assets and infrastructure and digital security of information, technology and systems, including SCADA).	
Security standards for the protection of people, property, assets, information and infrastructure are developed, implemented and used to develop appropriate mitigating controls for security risks.	
Security is actively managed and risks monitored to detect and respond to security breaches or weaknesses.	
Processes for alerting and escalating security breaches to the organisation's incident response function and executive leadership is established and effective.	
Security screening of prospective employees, contractors, consultants and service providers is in place and used to minimise the insider threat to the safety and security of people, property, assets, information and infrastructure.	
Procedures established that identify and proactively manage authorisation and access controls of authorised users to specific resources and are audited for compliance and effectiveness.	
Visitor management process established and implemented to understand and manage who is accessing the organisation's resources.	

ACTION	EXISTS?
Employee awareness and training activities conducted to support and improve the effectiveness of security measures.	
INSURANCE MANAGEMENT	
Insurance program exists to provide financial protection from business disruption events (whether through purchased insurance policy or self-insured financial contingencies).	
Insurers are engaged to better understand the organisation's disruption risks and effectiveness of controls to ensure policy costs are minimised / appropriate to the true risk.	
Insurance program is reviewed periodically to ensure cover is appropriate to the disruption risks and potential losses that exist.	
BUSINESS CONTINUITY MANAGEMENT	
Business Continuity Management framework is established with leadership commitment, policy, standards and procedures, roles and responsibilities defined.	
Business continuity plans have been developed to provide response to disruptions of time-critical business processes and services and are reviewed periodically through a Business Impact Analysis.	
Business continuity plans consider disruptions to buildings, equipment, technology, human resource and third party suppliers/service providers (BETH3).	
Business continuity plans are validated through regular exercising and updated periodically or as the business needs change (following organisational structure changes, business process change, new disruption risks identified etc.).	
ICT Disaster Recovery framework and capability is established, managed and exercised, with roles, responsibilities and prioritised recovery actions documented, reviewed and tested periodically.	
INCIDENT / EMERGENCY / DISASTER / CRISIS MANAGEMENT	
Emergency Management framework is established with leadership commitment, policy, standards and procedures, command and control structures, roles and responsibilities defined.	
Emergency management framework identifies different levels of event (e.g. incident, emergency, disaster, and crisis) and the organisational structure, including roles and responsibilities, to respond effectively to those events.	
Incident / emergency management plans have been developed to provide timely and effective response to disruption events that identify actions (with owners), incident team roles & responsibilities, activation and escalation triggers, reporting and communication requirements.	
Asset / Infrastructure Contingency plans exist for critical assets that provide operational response and recovery capability to quickly restore services and manage recovery, restoration or replacement of the impacted assets.	

ACTION	EXISTS?
Incident / emergency management plans are validated through regular exercising and updated periodically or as the business needs change (following organisational structure changes, business process change, new disruption risks identified etc.).	
LESSONS LEARNED MANAGEMENT	
Formal processes exist in the business continuity, ICT disaster recovery and incident / emergency management to conduct post incident, exercise and training reviews, with roles and responsibilities documented.	
Lessons learned from exercises, real disruption events and training activities are captured, reviewed, analysed and shared with stakeholders to inform improvements in the organisation's business continuity and incident / emergency management planning, as well as training and exercise delivery.	
Lessons management promotes continuous improvement across the organisation and findings are used to develop process improvement actions.	
CAPABILITY IMPROVEMENT PROGRAM	
Key personnel and decision makers are trained in leading incident / emergency management events, including the command & control, communication and decision-making processes.	
Regular reviews of the organisation's training needs are conducted, and the findings are used to inform capability development of key personnel and decision makers.	
Information systems, data management/quality and reporting processes are documented and updated following post incident, exercise and training reviews.	
Succession planning and knowledge transfer is formalised and managed as a business-as-usual activity across the organisation to manage key person risk and increase knowledge skills and operational capability in resilience activities.	
Key personnel engage in external groups, forums and networks to develop knowledge, understanding and best practices in resilience-related activities and disciplines.	
STAKEHOLDER ENGAGEMENT & MANAGEMENT	
Key Stakeholders, Customers and Communities at risk of impact from a disruption event are defined and can be targeted with contextualised information and messaging.	
Roles and responsibilities for producing information/reports and intelligence are agreed and documented across all incident / emergency management teams.	
Information sharing protocols across all levels of the incident / emergency management arrangements are in place and agreed before events, and align with business continuity and emergency management practices, systems and requirements.	
Communications systems are established that support the continuous flow of up-to-date critical information between key stakeholders.	

ACTION	EXISTS?
Key Stakeholders, Customers and Communities at risk of impact from a disruption event receive appropriate, consistent and accurate information through all phases of events.	
Communications systems and processes support the continuity of the organisations processes and services through all phases of disruption events and are resilient to the range of reasonably foreseeable operating environments.	
ASSET MANAGEMENT	
Planning for new infrastructure includes resilience principles that consider resistance in future operating conditions, reliability to meet forecast utilisation, redundancy to provide contingency in operation and recoverability to aid restoration following damage or failure.	
Asset and resource registers are regularly maintained and shared – including asset condition monitoring and maintenance programs, asset criticality and risk assessments.	
Asset criticality definitions and assessment methodology is established and utilised to inform the asset risk assessments.	
Resilience concepts have been integrated and embedded into all aspects of the asset management lifecycle (e.g. planning, design, construction, operations, maintenance and decommissioning).	
Robust processes are in place to conduct post-disaster damage assessments and to report on impacts to critical infrastructure.	

Appendix C: Abbreviations and glossary

Abbreviation	Meaning
AIIMS	Australian Inter-Service Incident Management System
All Hazards	An approach to manage the uncertain nature of emergency risk by building resilience to all or multiple hazards
BCM	Business Continuity Management
BCP	Business Continuity Plan
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection (protection against terrorism specifically)
CIR	Critical Infrastructure Resilience (protection against all hazards)
Dependency	When a critical infrastructure relies on another critical infrastructure, good or service for continued service provision
Disaster	When a hazard or threat intersects with a vulnerability, and the ability of local resources or business as usual to cope is overwhelmed
EMDRR	NSW Emergency Management and Disaster Resilience Review
ERM	Enterprise Risk Management
Hazard	A threat, usually natural, that unintentionally disrupts critical infrastructure service provision
Infrastructure Provider	An organisation responsible for providing an infrastructure service at a state, regional or local level, whether publicly or privately owned
Interdependency	When multiple critical infrastructures rely on each other for continued service provision
Mitigation	Measures taken in advance to reduce the likelihood or consequence of a hazard or threat.
REAG	Resilience Expert Advisory Group (Part of TISN)
Sector	An industry or service group identified within the NSW CIR Strategy
SEMC	State Emergency Management Committee
SCADA	Supervisory Control and Data Acquisition (SCADA) systems are used for remote monitoring and control in the delivery of critical services such as electricity, gas, water, waste and transportation.
SLERA	NSW State Level Emergency Risk Assessment
Threat	A hazard, usually man-made, that deliberately disrupts critical infrastructure service provision
TISN	Trusted Information Sharing Network (information sharing network co-ordinated by Commonwealth Home Affairs Department)
Vulnerability	The conditions determined by physical, social, economic, and environmental factors or processes which increase the susceptibility of an individual, a community, assets, or systems to the impacts of hazards. (Source: NDRRF Glossary)

Appendix D: References

[1] Resilience NSW. 2017. *NSW State Level Emergency Risk Assessment.* Available at: https://www.opengov.nsw.gov.au/publications/19463
[2] 100 Resilient Cities. *What is Urban Resilience?* Available at http://www.100resilientcities.org/resources/
[3] Australian Business Roundtable for Disaster Resilience & Safer Communities. 2016. *The Economic Cost of the Social Impact of Natural Disasters.* Available at http://australianbusinessroundtable.com.au/our-papers/social-costs-report
[4] State of New South Wales through Office of Environment and Heritage. 2016. *About Climate Change in NSW.* Available at http://climatechange.environment.nsw.gov.au/About-climate-change-in-NSW
[5] State of New South Wales through NSW Police Force. *Secure NSW: The Current Security Environment.* Available at https://www.secure.nsw.gov.au/the-current-security-environment/
[6] Commonwealth of Australia. 2017. *Australian Cyber Security Centre 2017 Threat Report.*
[7] Commonwealth of Australia. 2015. *National Guidelines for Protecting Critical Infrastructure from Terrorism.*
[8] State of New South Wales through NSW Police Force. *Secure NSW: Working with NSW Businesses.* Available at http://www.secure.nsw.gov.au/what-we-do/working-with-nsw-businesses/
[9] Adapted from: United Kingdom Cabinet Office. 2011. *Keeping the Community Running: Natural Hazards and Infrastructure.* Available at https://www.gov.uk/government/publications/keeping-the-country-running-naturalhazards-and-infrastructure
[10] Resilience NSW. 2018. *NSW Critical Infrastructure Resilience Strategy*. Available at: https://www.opengov.nsw.gov.au/publications/19460
[11] Commonwealth of Australia. 2016. *Organisational Resilience Web Site.* Available at http://www.organisationalresilience.gov.au/Pages/default.aspx
[12] Commonwealth of Australia through the Trusted Information Sharing Network. 2011. *Organisational Resilience: A Position Paper for Critical Infrastructure.* Available at https://www.tisn.gov.au/Documents/Organisational+Resilience+PDF.pdf
[13] Australian Business Roundtable for Disaster Resilience & Safer Communities. 2017. *Building resilience to natural disasters in our states and territories*. Available at http://australianbusinessroundtable.com.au/assets/documents/ABR_building-resilience-in-our-states-and-territories.pdf
[14] Commonwealth Attorney-General's Department. 2016. *Organisational Resilience Good Business Guide*. Available at https://www.organisationalresilience.gov.au/resources/Documents/Organisational-Resilience-Good-Business-Guide.PDF
[15] Commonwealth Attorney-General's Department. *Organisational Resilience HealthCheck.* Available at https://www.organisationalresilience.gov.au/HealthCheck/Pages/default.aspx
[16] The British Standards Institution. 2018. *Organisational Resilience Benchmark.* Available at https://www.bsigroup.com/en-GB/our-services/Organizational-Resilience/Organizational-Resilience-Benchmark/
[17] Standards Australia. *ISO31000:2018 Risk Management Guidelines*. Available at https://infostore.saiglobal.com/en-au/Standards/ISO-31000-2018-597093_SAIG_ISO_ISO_1367729/
[18] Australian Institute for Disaster Resilience Handbook Collection. Handbook 3: Managing Exercises. Available at https://knowledge.aidr.org.au/resources/handbook-3-managing-exercises/
[19] Naswall, K et al, University of Canterbury (2013) Employee Resilience Scale (EmpRes): Technical Report. Available at: https://ir.canterbury.ac.nz/bitstream/handle/10092/9469/12647836_employee_resilience_scale.pdf
[20] Resilience NSW. 2021. *NSW Critical Infrastructure Resilience Strategy: Infrastructure Resilience Guide.*
[21] Commonwealth Attorney-General's Department. *The Protective Security Policy Framework.* Available at: https://www.protectivesecurity.gov.au/Pages/default.aspx
[22] Gregg, M (2005) *Security Management Practices*. Available at http://catalogue.pearsoned.co.uk/samplechapter/078973446X.pdf