International benchmarking on organisational resilience

1 Enterprise View of all Risks
Catastrophic Risk Management
Emerging Threats
Critical Dependancies
Scenario based Modelling

2 Readiness Strategy
Stakeholder Management
Plans and Procedures
Equipment, Facilities and Tools
Training and Awareness

3 Response Strategy
Exercise Development
Communications
CM Leadership and Critical Thinking
PIRs and Learning Centres

4 Governance Structure
Risk Reporting
Surveys
Benchmarking
Audit

International Benchmarking on Organisation Resilience includes a detailed list of key indicators that are grouped into four main areas of assessment which are: RISK; READINESS; RESPONSE and ASSURANCE.

Resilience is a broad concept and there are many philosophical and ideological views on resilience but for the purposes of benchmarking, Organisational Resilience has been defined as:

"A resilient organisation has the ability to intelligently anticipate and manage change swiftly, has the capacity to learn from challenges and seeks opportunities to enhance its capability to adapt, bounce back faster, smarter and stronger".

Benefits of building a Resilient Organisation

- A resilient organisation that is aware of its resilience strengths will function well under stress and be able to successfully adapt and see the opportunity in whatever situational changes they face
- Resilient organisations are more competitive during business-as-usual as similarities exist between operational excellence and Organisational Resilience

Why measure resilience

Benchmarking indicators can guide an organisation in understanding their strengths and weaknesses so that they know where to invest resources to build their capability.

Ensuring that all key areas have an effective level of capability allows an organisation to rapidly adapt and respond to internal or external change; risks, opportunities, demands, disruptions or threats; and continue operations with limited impact to strategic direction.

Drivers for measuring resilience

- To have leading (as opposed to lagging) indicators of resilience across the organisation
- To have quantifiable evidence of improvements made from prior investments
- To have visibility of the current vulnerabilities and areas that need investment
- To provide KPIs to business units in building and maintaining their resilience
- To be able to prioritise future investments
- To provide assurance to key stakeholders
- To provide visibility of the resilience capability that exits that links to competitive advantage in BAU

An organisation with a mature resilience capability is able to demonstrate the following:

- Integrated and consistent approach to the management of strategic, operational and financial risks
- Capability to respond to known 'catastrophic' risks
- High levels of confidence to respond to emerging threats
- Embedded critical thinking across the organisation
- Alignment of plans that are understood, tested and continually improved
- A robust set of tools that are embedded within the organisation
- A positive change culture that includes the identification of opportunities
- Alignment of resilience capability with key inter-dependencies
- Regular assurance to the board, regulators and other key stakeholders

Assessment criteria

The benchmarking ratings use a 5-tiered assessment against the key indicators which are used to review specific *business units* or *across an entire organisation*.

The aim of the assessment rating is to provide visibility on:

- Areas of risk that need immediate attention
- Assurance on the areas that do not require further work
- Areas of excellence that should be applied more broadly

Assessment criteria

RATING	DESCRIPTION
OUTSTANDING	An area of excellence in process and capability that should be further reviewed for broader application
EFFECTIVE	Processes and procedures meet International and organisational Standards and no improvements have been identified
MINOR WEAKNESS	Processes and procedures are at an acceptable level with isolated minor weakness and could undermine systems and controls or operational efficiency
DEVELOPMENT REQUIRED	Significant weakness likely to compromise the process or procedures. May lead to financial or operational loss, safety or compliance breach, environmental or reputational damage if not resolved
AT RISK	Key Controls absent or not effective, highly likely to compromise systems or internal controls or operational efficiency. May lead to significant operational losses, safety or compliance breach, environmental or reputational damage

The indicators measured and ratings given are supported by evidence detailed in the benchmarking assessment report.

Measuring Organisational Resilience

Organisational Resilience leading indicators are grouped into four key areas of RISK, READINESS, RESPONSE and ASSURANCE and are aligned with the following Standards and Guidelines:

- *ISO 31000:2009 Risk management – Principles and guidelines.*
- *AS/NZS 5050:2010 Business continuity – Managing disruption related risk.*
- BS 65000:2014 Guidance on Organisational Resilience
- *Australasian Inter-Service Incident Management System [AIIMS] and Prevention, Preparedness, Response and Recovery [PPRR] principles.*
- Australian Federal Governments Resilience Strategy and Guidelines for organisation responsible for Critical Infrastructure.

1. RISK	2. READINESS	3. RESPONSE	4. ASSURANCE
Protect the organisation through identification and mitigation of critical risks	Minimise impact to people and business through preparation and planning	Optimise performance of teams for BAU and crisis events	Continuous review and reporting of resilience capability
1.1 Enterprise View of all Risks	2.1 Readiness Strategy	3.1 Response Strategy	4.1 Governance Structure
1.2 Catastrophic Risk Management	2.2 Stakeholder Management	3.2 Exercise Development	4.2 Reporting
1.3 Emerging Threats	2.3 Plans & Procedures	3.3 Response Capability	4.3 Surveys
1.4 Critical Dependancies	2.4 Equipment, Facilities & Tools	3.4 Communications	4.4 Benchmarking
1.5 Scenario based Modelling	2.5 Training & Awareness	3.5 PIRs & Learning Centres	4.5 Audit

Indicators used to measure Organisational Resilience

RISK

The cornerstone of building a resilience capability is having sound risk management processes that are understood and used across the organisation. ISO 31000:2009 is an internationally recognised standard and is used across all industries. This standard remains a robust and 'world class' approach to risk management and is embedded within many organisations to varying degrees.

Resilience requires 'going beyond' risk management and is achieved by having a strong culture of risk management as well as an adaptive culture and capability to respond.

The key areas within the RISK component of the Resilience Framework are:

- 1.1 Integrated and consistent approach to managing all known strategic, operational and financial risks
- 1.2 Identification and management of 'catastrophic' risks
- 1.3 Identification and management of emerging threats and opportunities
- 1.4 Management of risks related to third parties including: critical suppliers, Joint Venture partners and Government agencies
- 1.5 Scenario based modeling

1.1 An integrated and consistent approach to managing all strategic, operational and financial risks from a project level up to the Board is an essential part of resilience. The practical application of managing and maintaining an enterprise-wide view of all known risks – with an increasingly diverse risk profile – remains a challenge for any large and complex organisation.

1.2 Recent events have highlighted the need for organisations to identify types of risks that could be considered '**catastrophic**', '**iceberg**', '**extreme events**' or '**significant disabling events**'.

The consequences that define 'catastrophic' events are usually related to community impact, brand and financial impact or loss of life. They are also usually, low probability and high consequence events. Some events or risks may be too difficult or expensive to mitigate but the high-consequence nature of these events requires that:

- 'Catastrophic' / extreme event risks are identified, monitored and reported to the Board
- 'Catastrophic' risks are treated differently to other risks already being managed
- The capability to respond to these risks is developed and maintained

These types of 'catastrophic' or 'extreme event' risks usually require a 'significant and co-ordinated response' across an organisation or with external parties, including JV partners, Government agencies.

The capability to respond to extreme events is an essential part of building and maintaining organisational resilience.

1.3 Management of emerging threats – The on-going uncertainty from global markets and the large number of natural disasters that have occurred around the world in recent years has prompted the need to look beyond known risks that their organisations face and to develop contingency plans for emerging threats.

Many of the principles of risk management can be used to address the issue of emerging threats. Teams need to be able to quickly identify, monitor and build contingency plans for a range of potential emerging threats. A formal, structured and consistent approach to managing emerging threats will provide confidence to the teams and assurance to key stakeholders.

Indicators used to measure Organisational Resilience (cont)

1.4 Management of risks related to critical suppliers and third parties – The increasingly complex and interconnected operating environment requires the risks related to third parties to be more effectively managed. A mature risk management culture extends the focus outside of the organisation into understanding the risks and vulnerabilities of critical suppliers and other third parties.

Information from critical suppliers on their capability to respond to particular disabling events is necessary. The opportunity within the Resilience framework is to understand the vulnerabilities that this presents and to build strong networks with key suppliers and third parties.

1.5 Scenario based modelling and planning has been used in varying degrees over the years and its value and application as a mainstream business activity is increasing. Scenario planning is a powerful way to guide decision makers by providing a context in which they can make decisions. By considering a range of possible futures, decisions are better informed and strategy based on a deeper insight is more likely to succeed.

Scenario planning can add situational awareness and adaptability as it provides better insight into how different factors affecting an organisation can affect each other. It can reveal linkages between apparently unrelated factors and can provide greater insight into the forces shaping the future, delivering competitive advantage.

Scenarios help teams understand their environment, share knowledge, consider the future and assess strategic options. Information is better evaluated within a scenario planning framework and it allows a team to react to emerging circumstances and develop a call to action where necessary.

READINESS

The READINESS indicators look at the current level of preparedness to respond to a range of risks and changes to the organisation. The READINESS section involves pre-planning for disruptions, 'shocks' and the development of plans, the use of technology, training and awareness and alternate site arrangements.

The key areas within the READINESS component within the Resilience Framework are:

- 2.1 Readiness strategy
- 2.2 Stakeholder Management
- 2.3 Plans and procedures
- 2.4 Equipment, facilities and tools
- 2.5 Training and Awareness

2.1 Having a **Readiness Strategy** that includes an overarching approach to creating resilience across a large and complex organisation is essential. Most organisations have a diverse number of plans operating across different levels and with different objectives. In some cases the objectives of the plans are not clear, there are gaps and overlaps with other plans and the content of the plans may not be known or understood.

There is a significant cost associated with the development and management of multiple plans and without an overarching strategy the plans can be ineffective. Plans also need also to be aligned where necessary with critical suppliers, Joint Venture Partners and key agencies.

2.2 Stakeholder Management is a core competency for resilient organisations. A common and consistent process should be used for the identification and management of key stakeholders, internal and external.

Pre-considered strategies to manage and communicate with stakeholders such as staff, regulators, customers, shareholders, media and the community should be understood and documented.

Indicators used to measure Organisational Resilience (cont)

In understanding the organisations external key stakeholders, there is the opportunity to develop strong networks with key suppliers, agencies and other third parties. Establishing formal lines of communication and entering into Mutual Assistance Agreements [MAA's] are all measurable elements of effective stakeholder management.

2.3 Plans should reflect the current risk profile of the organisation and should as a minimum include: Crisis Management Plans; Crisis Communications Plans; Business Continuity Plans; Disaster Recovery Plans; Emergency Management Plans.

Plans need to be tested on a regular basis and there needs to be clarity on the intended audience, triggers to activate the plans, escalation process, response model/s, alternate sites; minimum staffing requirements etc. On-going management and training on the plans is essential.

2.4 The trend towards off-shoring key business processes has resulted in the need for contingency planning and testing against a range of scenarios. Increasingly the regulators want assurance of the capability of the organisation to restore critical functions and processes.

The dependency on technology in some sectors has meant that there is a requirement to demonstrate **disaster recovery capabilities and alternate site arrangements**. Most organisations have designated location/s where their response teams would meet when activated, and a nominated alternate location if the primary location is affected by the event or not available.

A **Crisis Management Handbook, to be used as an aide memoire**, is necessary where teams are operating in different regions. A Handbook will also provide consistency where a 'significant and co-ordinated' response is required involving a number of teams.

The effective use of technology can aid a team in maintaining an adaptive capability. Rapid notification of information, access to internal data, media information, communications and facilities will all assist an organisation to communicate efficiently and effectively and make key decisions.

2.5 Training and awareness is critical to develop the knowledge and skills of individuals and teams to perform their respective roles. Teams should be made aware of the plans that exist and the tools available.

This should include:

- User Training – competency-based training for individuals and teams who need to undertake key roles for example members of a Crisis Management Team or Crisis Chair
- Practitioner Training – for people with a role to play in developing the organisation's capability
- General Awareness – for all staff.
- The training of staff should fit within the usual staff development training programs and be included within the induction process, where possible.

RESPONSE

The RESPONSE indicators look at how well the team are trained and how useful the plans, tools, technology and facilities are. The RESPONSE indicators assess the capability that has been developed within the READINESS component against a range of potentially 'catastrophic' risks or events.

The RESPONSE section also includes the Learning and Development that comes from dealing with real events and complex simulations.

The key areas within the RESPONSE focus area of the Resilience Framework are:

- 3.1 Response Strategy
- 3.2 Testing and Exercising
- 3.3 Communications
- 3.4 Crisis Management Skills
- 3.5 Learning and Development

One of the key measurable components within the response assessment is the ability for the individuals and teams to demonstrate critical thinking capabilities.

Indicators used to measure Organisational Resilience (cont)

An organisation may have exhaustive and effective risk management processes, detailed plans, highly skilled individuals but if the teams come together in a crisis and are unable to demonstrate 'critical thinking' they may not be effective in managing the situation.

Critical thinking skills, developed at all levels within an organisation and evident during BAU, times of change and through a crisis is the most effective leading indicator of Organisational Resilience.

3.1 Response strategy – The specific risks that the organisation is facing will be detailed and managed on an on-going basis through various teams. The details of how the organisation will respond to a crisis or major disruption will be documented in the plans within the READINESS section.

The response strategy involves the strategic approach to building capability and can include a range of activities depending on the current risks, vulnerabilities and skills of the teams. A consistent approach is needed and the response strategy should include:

- An understanding the current and desired capabilities of key response teams by skills and experience
- Understanding the known 'catastrophic risks' and the current and desired capability to respond
- Options and strategies on how best to build the capability based on desktop scenarios, hypotheticals or multi-faceted exercises

3.2 Testing and exercising process – Testing and exercising is the process of applying the team and individual skills in an operating environment through simulation, rehearsal, desktops or workshops.

A thorough process needs to be followed and includes key activities such as:

- Scoping
- Development
- Execution
- Reporting

Within the steps above there needs to be a structured and consistent approach to understanding: the drivers for that particular exercise/event; stakeholders to be involved; previous experience; elements to be tested and elements to be trained; tools, plans and facilities to be used and a detailed post-event report to review how the team worked against the key objectives set.

3.3 Effective communications underpins any resilience related activities. Post-incident reviews and enquiries consistently show that effective communications during a crisis is particularly challenging and difficult to achieve. The reach and speed of social media has added a new dimension to managing communications and meeting community and stakeholder expectations.

The value of social media needs to be understood and used where possible. Key indicators for benchmarking communications capabilities within this framework include: stakeholder matrix with pre-considered communications messages and time expectations, for a range of known stakeholders; speed of internal notifications and communications; strategies for monitoring and managing social media; having KPI's related to getting messages out.

Indicators used to measure Organisational Resilience (cont)

3.4 Crisis Management Leadership – Exercising and testing allows teams to focus on dealing with an escalating and/or uncontrolled situation. These indicators review the Leadership and critical thinking of the teams by their:

- Situational awareness – understanding of the facts and assumptions
- Ability to prioritise
- Understanding of impacts across the business
- Decision making
- Ability to develop tactical and strategic plans under the pressure of a tight timelines.

The testing and exercising allows the organisation to:

- Provide a framework to develop critical thinking capabilities
- Build on key leadership skills for junior and senior managers
- Improve understanding of the strategic business issues for key managers
- Strengthen key relationships across the organisation and remove restrictive silos
- Create ownership as key managers are involved in the assessment, planning and response to the key risks for an organisation

3.5 Learning and Development - A robust Learning and Development process ensures outcomes and recommendations are shared across and organisation, and to inform the adjustments to policies and guidelines. Mature organisations will have:

- Clear post incident report and follow up methodology
- Use of a common debrief/review template used across the business
- Established methodology and responsibilities to assess incidents, and lessons from like or same industry

ASSURANCE

Global financial and political uncertainty, the increased number of natural disasters, combined with the changes to Directors responsibilities and liabilities have all resulted in greater assurance being sought by Governments, Boards and Regulators.

In some instances the risk profiles for organisations has changed based on strategic direction and in others the awareness or 'appetite for risk' has changed. All have created the need for greater visibility of current capabilities and lagging indicators of organisational Resilience are no longer accepted at many levels within Governments and Business.

Lessons learnt from recent events have shown that being better prepared and having better controls could have resulted in improved outcomes.

The key areas within the ASSURANCE focus area of the Resilience Framework are:

- 4.1 Governance Structure
- 4.2 Reporting
- 4.3 Surveys
- 4.4 Benchmarking
- 4.5 Audit

4.1 Governance Structure – The management and maintenance of Organisational Resilience should be integrated into the Management System and reported on at the most senior levels.

An effective governance structure gives a formal process to raise issues, resolve conflicts, and enable collaboration and to ensure a consistent application of the overarching policy across the organisation and its related entities.

Indicators used to measure Organisational Resilience (cont)

Similar to other functions such as OHS, in order to be effective Resilience must be embedded within operating businesses, business units and subsidiaries. This ensures the ownership and responsibility for managing these risks and preparing resilience strategies lies with the areas who 'own the risk'.

4.2 Reporting – Existing risk management reporting structures, systems and processes should be adopted and adapted to incorporate resilience-related risks wherever possible and include reporting up to Board and Risk Review committees as required. Reporting should include;

- Consistent and integrated reporting on all Strategic, Operational and Financial risks; Catastrophic Risks; Emerging threats and Critical suppliers/third parties
- Reporting on all aspects of READINESS including: currency of plans; alignment of plans; usability of plans; training and development
- Reporting on all aspects of RESPONSE capability including: current skills of team/s; past and proposed exercising program; current capabilities to respond to specific known risks and emerging threats; crisis leadership and critical thinking capabilities

Reporting of business areas against one another using common criteria is an effective way of highlighting areas of vulnerability as well as identifying areas of excellence that should have broader application.

4.3 Surveys – A key indicator for organisational resilience is confidence within the business that includes:

- Confidence in own ability; team abilities; leadership; and the Executive
- Confidence from External stakeholders, the Board and the Executive in the teams that sit within them

Surveys can be used following major events, simulations or during BAU to gauge the current levels of confidence and feedback can be used to design future training and exercising programs.

4.4 Benchmarking can be used as a way to highlight the key areas of competency or vulnerabilities. It is important that the indicators chosen are relevant to the team, organisation and key stakeholders. Benchmarking can take place by:

- Developing your own data on particular areas of focus and measuring that information over a period of time
- Comparing your key indicators with those from another business unit within your organisation
- Comparisons with similar groups in similar industries
- Comparisons with similar groups in different industries
- International benchmarking

4.5 Audits – Internal audit activities are the formal functions that nominated teams or managers perform for specific business units. They typically are planned in accordance with the audit schedule, and may include:

- Self-Assessments
- Observations
- Compliance checks including spot checks
- Crisis and Incident Management audits

External audits can provide an independent view and higher levels of assurance.

Case studies

Qantas

Qantas is the world's second oldest airline and employs over 35,000 people and has a network spanning 182 destinations in 44 countries. In 2011 revenue was over $15 Billion and more than 40 million passengers travelled with Qantas and its subsidiaries. Qantas, like many within the aviation sector, have faced an unprecedented number of global and local risks and disruptions to their business.

- Qantas have had a focus on building and maintaining their Resilience capability since 2007, driven by the Senior Leadership team and reporting to the Board
- The resilience indicators and framework are integrated into the Qantas Management System
- A robust set of tools and facilities that are used across the Group
- An exercising program that includes a range of strategic, operational and financial risks across the Group

Westpac Banking Corporation

Westpac is Australia's first company and is currently listed as one of the top 5 companies on the Australian Stock Exchange with assets worth $670 Billion and a market capitalisation of $61 Billion. Westpac currently employs over 38,000 people and services more than 12 million customers.

- Heavily governed by the regulators they have an enormous investment in business continuity and disaster recovery capability including data mirroring and high-availability systems
- Sound risk management processes and monitoring of 'extreme event' scenarios
- Crisis exercise program involving their Business Unit CMTs through to their Executive level CMT. This program is characterised by a thorough process to select complex and challenging scenarios, that are highly relevant to the respective crisis team including the market, political and regional challenges that each of the business units are currently managing
- Common crisis management tools that are used across all levels of the organisation. These tools are adjusted and improved as a result of lessons learnt, real events and from the robust exercising program

NSW State Emergency Services

NSW State Emergency Service is recognised as the most versatile and widely used emergency service organisation in New South Wales with 10,000 volunteers across the state, responding to and supporting their communities during emergencies. NSW SES service all of NSW and deploy interstate and internationally when required. In 2012 111 Local Government areas declared natural disasters. In many communities, these were the largest floods experienced since early 1970'S and in some case their history.

- As an Emergency Response unit the SES teams are well versed in emerging threat analysis and management and this remains a high focus area
- Training and the use of tools are a central part of the maintaining the capability of 10,000 volunteers from 228 units across 17 regions.
- Improved flood data, flood modelling and the experience of the teams are all drawn upon for the on-going monitoring of threats to the community and during periods of operation
- NSW SES have maximised their learning through assessments of their capability against other Agencies nationally and internationally, particularly from the key findings following the Queensland Floods and Victoria bush fires

Summary Resilience Benchmark Report

	No	Criteria	Group	Region A	Region B	Business Unit A	Business Unit B
RISK	1.1	Enterprise view of Risk	Effective	Effective	Minor Weakness	Minor Weakness	Effective
	1.2	Catastrophic Risk Management	At Risk	At Risk	At Risk	At Risk	At Risk
	1.3	Emerging Threats	Development Required	Development Required	Development Required	Development Required	Development Required
	1.4	Critical Dependencies	Effective	Effective	Minor Weakness	Effective	Minor Weakness
	1.5	Scenario Based Modelling	Development Required	Development Required	Development Required	Development Required	Development Required
READINESS	2.1	Readiness Strategy	Development Required	Minor Weakness	Minor Weakness	Development Required	Minor Weakness
	2.2	Stakeholder Management	Outstanding	Minor Weakness	Effective	Minor Weakness	Effective
	2.3	Plans & Procedures	Effective	Effective	Effective	Minor Weakness	Minor Weakness
	2.4	Equipment, Facilities & Tools	Minor Weakness	Development Required	Development Required	Development Required	Development Required
	2.5	Training & Awareness	Development Required	Outstanding	Outstanding	Development Required	Minor Weakness
RESPONSE	3.1	Response Strategy	Effective	Minor Weakness	Effective	Effective	Minor Weakness
	3.2	Exercise Development	Development Required	Outstanding	Outstanding	Minor Weakness	Development Required
	3.3	Communications	Effective	Minor Weakness	Effective	Effective	Minor Weakness
	3.4	CM Leadership & Critical Thinking	Effective	Minor Weakness	Minor Weakness	Minor Weakness	Minor Weakness
	3.5	PIRs & Learning Centres	Development Required	Development Required	Minor Weakness	Development Required	Development Required
ASSURANCE	4.1	Governance	Minor Weakness	Development Required	Development Required	Development Required	Development Required
	4.2	Risk Reporting	Effective	Effective	Effective	Effective	Effective
	4.3	Surveys	Minor Weakness	Minor Weakness	Minor Weakness	Minor Weakness	Minor Weakness
	4.4	Benchmarking	Development Required	Development Required	Development Required	Development Required	Development Required
	4.5	Audit	Outstanding	Effective	Outstanding	Outstanding	Effective

OUTSTANDING	An area of excellence in process and capability that should be further reviewed for broader application
EFFECTIVE	Processes and procedures meet International and organisational Standards and no improvements have been identified
MINOR WEAKNESS	Processes and procedures are at an acceptable level with isolated minor weakness and could undermine systems and controls or operational efficiency
DEVELOPMENT REQUIRED	Significant weakness likely to compromise the process or procedures. May lead to financial or operational loss, safety or compliance breach, environmental or reputational damage if not resolved
AT RISK	Key Controls absent or not effective, highly likely to compromise systems or internal controls or operational efficiency. May lead to significant operational losses, safety or compliance breach, environmental or reputational damage