Integrating Disaster and Business Continuity Planning

FinPro Conference 2012, Creswick Victoria

John Salter, Director Emergency Preparedness Capacity Builders
www.disasterresilience.com

Abstract

Many communities have been recently exposed to extreme events – from bushfires to floods. For Local Government, a challenge has been to resource emergency management requirements while continuing to delivering core services. This paper outlines an approach developed and validated with several bushfire and flood effected Councils which integrates disaster management with business continuity. The model uses a risk approach which focuses on due diligence performance criteria. Decisions are based on the criticality and vulnerability of resources before an extreme event (to build organizational resilience) - and the criticality of and impact on resources after an extreme event (to nimbly deploy resources to meet needs). The decision making method – for deployment of resources to address both the emergency and the continuity requirements - relies on a single, high level crisis management team. The model has been validated by strong performance in real events.

Plans vs. Planning


The scope of the Standard is in two parts:

1. To plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system;

2. To protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents when they arise.
If the emphasis is on the documentation of yet another “plan, do, check, act” system, then the Standard will be seen as a burden rather than an enabler – a significant risk in a marketplace already crowded with standards, systems and guidelines.

If the Standard is used to support planning – active collaboration to achieve sound outcomes – with only the minimum necessary documentation – then it is more likely to attract interest and deliver traction.

If we are mindful and use a strategic approach, we should address the key due diligence issue – or “coroner’s test”: i.e. “what you ought to know and do – about risks and their management”. The set of crucial decision points that should be addressed in every disaster management and business continuity management situation, are about:

1. what is the risk (detection),
2. what does the risk mean (recognition and interpretation),
3. who has an interest (communication to multiple stakeholders), and
4. who should do what (organization of a collaborative system).

Specific objectives will emerge according to the nature and scope of the particular disaster or crisis.

**Key Terms**

Words and their meanings – or their different meanings – are important when developing context and establishing shared understandings. This enables communication and avoids the “Tower of Babel” syndrome whereby many languages contribute to project failure.
So in checking some terms, let us start with “disaster”. First, while focused on pain thresholds and capacity to cope, the term disaster is contextual – your thresholds and capacity to cope may not be the same as mine.

Second, it is important to recognize that hazard events are not necessarily disasters. Yes, hazards contribute to risk, but an extreme event only becomes a disaster when it impacts something we attribute value to (our “care-abouts”).

**Same hazard event – Different consequences**

Incorporating a focus on vulnerability opens up a rich vein of considerations - about what might be the most appropriate thing(s) to do to “protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents when they arise” (ISO 22313).

A risk based approach focuses on the likelihood of consequences – not the likelihood of hazard events.

While a risk based approach sits comfortable with an “all hazards” approach, it should be recognized that an “all hazards” approach is a civil defence construct – applying largely to response, relief and recovery arrangements which can benefit from such efficiencies. In a more comprehensive risk based approach there needs to be a recognition that “fire is not water” – and that prevention strategies for each need to be tailored.
The framework within which the risk based approach is applied is often referred to as PPRR – or Prevention, Preparedness, Response and Recovery. This P²R² heuristic device was introduced in the 1980’s as an instrument of American foreign policy to encourage third world nations away from reliance upon a post disaster “hand up for hand out” approach. It is not a simple linear construct – though it has constrained thinking by being used in that simple, indeed simplistic manner. A more useful display of the relationship between the four words is displayed here.

Line one in the diagram below reflects the purpose – or business case – of business continuity planning. To mitigate before and after a disruption event.

KEY
1. The impact and period of disruption as a consequence of an emergency is reduced with enhanced mitigation measures in place.
2. The impact of an emergency without adequate preparedness and prevention (mitigation) strategies.
Government needs to address several service delivery issues in a disaster. Support to the community is likely to be a function of both mandated responsibilities and politically endorsed initiatives in response to expectations – and at the same time, it will be expected that key services will be delivered. This calls for the design and development of appropriate “structure”.

Structure, introduced into operations by design, is both a means of limiting error, and of clarifying choices for action by multiple participants over time in complex environments … the challenge lies in designing structure in ways that achieve stability without restricting flexibility. (L. Comfort)

An approach which integrates business continuity and crisis management is characterized by three elements:

1. A focus on the things you rely on to run your business effectively – the assets, people, skills, information (electronic / non electronic), technology (including plant and equipment), premises and supplies which underpin your critical activities.
2. Adding value by the incorporation of a significant mitigation component – which empowers you to reduce your vulnerability before an incident – to build resilience into the structures and functions of your business.
3. Support of the decision making processes to manage the consequences of impact after an incident – in a nimble and informing manner.

Over the last few years we have worked with several governments challenged by the need to respond to disasters and continue service delivery. Recently, the structure developed with the Nillumbick Shire (Victoria) was recognized as a worthy finalist in the 2012 LGPro Category 1 Awards for “Innovative Management Initiative” based on validated performance during a disruption event.
The nine step methodology is outlined below.

1. Resources
   - people
   - premises
   - providers
   - processes
   - profile

(a) Map resource profiles for each critical activity

2. Risk
   Pre-event risk is a function of resource criticality and resource vulnerability

(b) Vulnerability Report

3. Risk Management
   Action planning to reduce vulnerability of resources

(c) Mitigation Plan

4. Resilience
   Entity is now more able to withstand impacts

5. IMPACT
   Event which threatens business

(d) Map and communicate impact consequences - ASAP

6. Risk
   Post-event risk is a function of resource criticality and resource capability

(e) Impact Report

7. Crisis Management
   Action planning to reduce the impact (on business)

(f) Response and Recovery Plan

8. Priority Action Plan
   Crisis management team decides action to take, record and monitor until risk levels are acceptable
Foundational to the approach is mapping the organization – especially the resources it relies on to deliver its key “must deliver” services.

This can be done by using general tools (such as six sigma / lean SIPOC) – or by using a focused tool which concentrates on fifteen questions.
Data addressing the fifteen questions can be collected and stored in a variety of ways – in workshops or one on one interviews with managers – by paper, Excel spreadsheets, or an Access Database.

<table>
<thead>
<tr>
<th>PEOPLE</th>
<th>PREMISES</th>
<th>PROCESSES</th>
<th>PROVIDERS</th>
<th>PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Staff:</td>
<td>Buildings:</td>
<td>IT:</td>
<td>Reciprocal Arrangements:</td>
<td>Customers and Reputation:</td>
</tr>
<tr>
<td>What staff do you require to carry out the Key &quot;must deliver&quot; Product / Service?</td>
<td>What locations does this Key &quot;must deliver&quot; Product / Service operate from? (Primary site, alternative premises)</td>
<td>What is it essential to carry out this Key &quot;must deliver&quot; Product / Service?</td>
<td>Do you have any reciprocal agreements with other organisations?</td>
<td>Who are your key stakeholders?</td>
</tr>
<tr>
<td>Skills / Expertise / Training:</td>
<td>Facilities:</td>
<td>Documentation:</td>
<td>Contractors / External Providers:</td>
<td>Legal Considerations:</td>
</tr>
<tr>
<td>What skills / level of expertise is required to undertake this Key &quot;must deliver&quot; Product / Service?</td>
<td>What facilities are essential to carry out this Key &quot;must deliver&quot; Product / Service? Do you need these to be located at a specific site?</td>
<td>What documentation / records are essential to carry out your Key &quot;must deliver&quot; Product / Service, and how are these stored?</td>
<td>Do you tender key services out to another organisation? If so - to whom and for what?</td>
<td>What are your legal, statutory and regulatory requirements?</td>
</tr>
<tr>
<td>Minimum Staffing Levels:</td>
<td>Equipment / Other Resources:</td>
<td>Systems &amp; Communications</td>
<td>Suppliers:</td>
<td>Vulnerable Groups:</td>
</tr>
<tr>
<td>What is the minimum staffing level with which you could provide some sort of service?</td>
<td>What equipment / other resources are required to carry out your Key &quot;must deliver&quot; Product / Service?</td>
<td>What systems and means of communication are required to carry out your Key &quot;must deliver&quot; Product / Service?</td>
<td>Who are your priority suppliers and whom do you depend on to undertake your Key &quot;must deliver&quot; Product / Service?</td>
<td>Which vulnerable groups might be affected if your organisation fails to carry out this Key &quot;must deliver&quot; Product / Service?</td>
</tr>
</tbody>
</table>

The “Value” comes from adding a risk assessment layer – before impact – which informs capacity and resilience building opportunities.
After impact – the value comes from only one impact attribution being required to be entered – against the effected resource (which will vary by hazard events) – and this then informs decision makers by tailored reports.
Closing reflections

1. The tent in Thomas Sheard’s The Arab Blacksmith, c.1900, Bendigo Art Gallery is a timely metaphor for risk management frameworks. It’s your tent. All elements are necessary to be sufficient – cloth, poles and pegs – shape it to your context – your “crowd size”, wind direction and sun exposure.

2. There are no magic “silver bullet” solutions.

3. Methodology: Gap assess your capability with an agreed approach (an approach based on the vulnerability of resources and focused on supporting informed decision making). Going down a “Standards referenced” path may be useful, but it is probably not necessary.

4. Tool: Any “solution” needs to perform against the methodology above – ticking all of the “quality process boxes”. It is the glove that fits the hand.