Risk information – Property

Business continuity management and contingency planning

vero
Committed to your success

The information in this document provides general guidance only. It provides general information on business continuity management planning. We have not considered your business' particular circumstances and any Government restrictions due to COVID-19 (which may change), and so you may need to consider how this applies in your circumstances or if you need to seek appropriate professional advice. For any queries about insurance cover, please contact your insurer or insurance broker.

Introduction

Business Continuity Management (BCM) and Contingency Planning are important components of an organisations overall risk management strategy. Implementation of a BCM program will help identify critical processes or activities, threats to these processes or activities as well as the provision of working plans designed to restore the company to an acceptable level of activity following a major loss. The process of designing and developing a tailored BCM program creates an opportunity to thoroughly examine your business objectives, operating environment and dependencies.

Other benefits of managing Disruption-Related Risk effectively

- Demonstration of good governance and accountability to internal and external stakeholders
- Protect and advance your brand value
- Protect market share and customer base
- Remain compliant with relevant legislative or other obligations
- Gain a deeper understanding of how your business works, possibly gaining a competitive advantage (for example, improvement on efficiency, building awareness of the potential for disruption and maintaining a focus on objectives and critical functions).

Standards

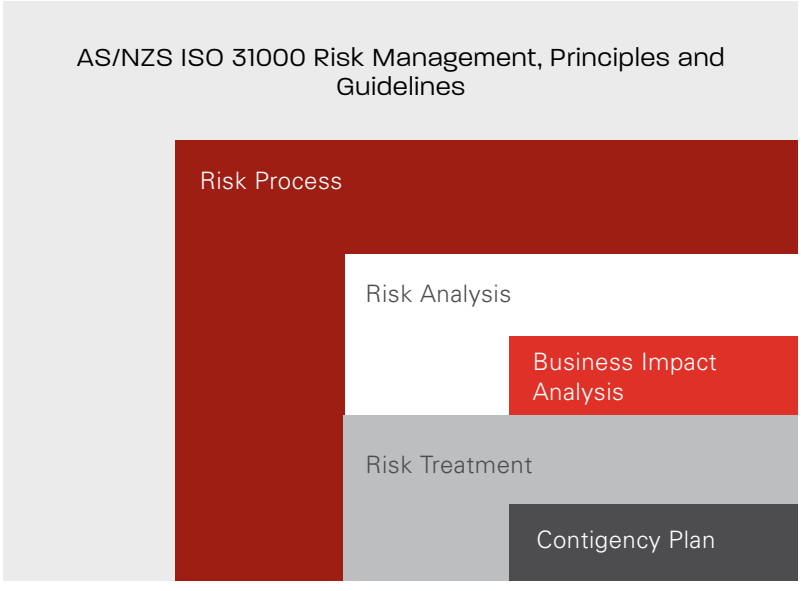
AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines is a globally accepted standard for managing all forms of risks.

AS/NZS 5050:2010 Business Continuity – Managing disruption-related risks explains how to use AS/NZS ISO 31000 and provides a framework to identify and manage disruption-related risks, HB 292:2006 A Practitioners Guide to Business Continuity Management provides an overview of some generally accepted BCM practices including examples of relevant checklists, templates and tables.

Building a BCM Framework will help answer the following questions

- What could happen?
- So what does it mean to me?
- What is critical to continuing our business?
- What do we have to do before, during and after a catastrophe or major incident?

AS/NZS ISO 31000 Risk Management, Principles and Guidelines



vero.com.au

V8840b 17/04/20 A COVID-19

Key terms

Business Impact Analysis (BIA) – Detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the resulting consequences. This may include consideration of the organisation's business functions, people, processes, infrastructure, resources, information, interdependencies and the nature and extent of capability loss over time.

Business continuity – The uninterrupted availability of all key resources supporting essential business functions.

Contingency plan – Any plan of action that allows an organisation to respond to events should they occur. This includes all plans that deal with stabilisation, continuity of critical business functions and recovery. Some types of contingency plans may have been described as a Business Continuity Plan, Business Recovery Plan, Disaster Recovery Plan or Recovery Plan.

Contingent capability – Supplementary resources provided specifically to enable an organisation to respond to events should they occur.

Crisis management team – A dedicated team (usually internally resourced) that is required to divert a proportion of their attention, time, energy and resources away from normal operations to managing an untoward event that potentially or actually results in a disruption to the day-to-day operations of part or whole of the organisation.

Critical business function – A business function or part thereof identified as essential for survival of the organisation and achievement of its critical objectives. A business function that has the effect of protecting critical interests or the community or another stakeholder to which a duty is owed, may qualify as a critical business function.

Disruption-related risks – Risk arising from the possibility of disruptive events.

Maximum Acceptable Outage (MAO) – The maximum period of time that an organisation can tolerate the disruption of a critical business function.

Recovery Time Estimate (RTE) – The estimated period of time required to restore a particular level of functionality after taking into account any uncertainties (the period is measured from the commencement of restoration activity and not from the commencement of the disruptive event).

Through chain – End-to-end chain through which value is created, realised or transferred, encompassing the inputs, activities and outputs of the supply, process and distribution chains, including information, knowledge, resource and financial flows.

Risk analysis

Part of the process for managing disruption-related risks is to conduct a risk analysis. This is normally approached in two stages, the initial risk analysis and the 'Business Impact Analysis'.

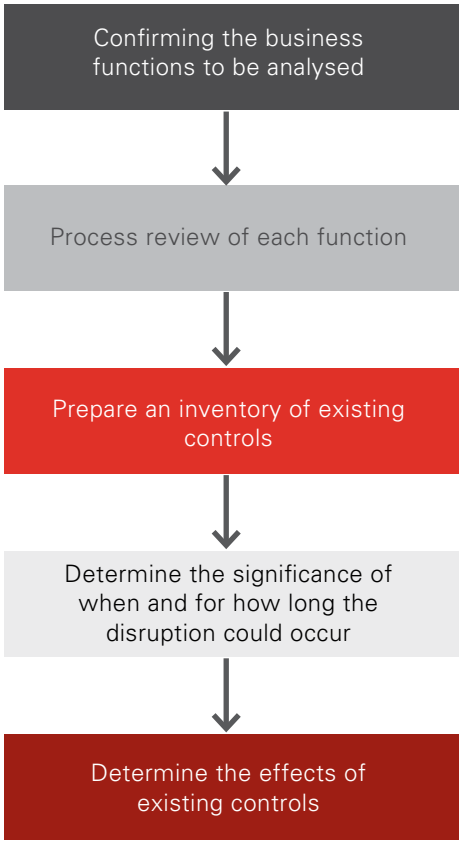
Stage 1

The **initial risk analysis** should include building a clear understanding of –

- The business functions and processes (and the importance of each of these functions in terms of the organisation's objectives);
- The location and distribution of infrastructure and resources;
- The vulnerabilities of the systems, physical structures and locations in which business activity occurs (taking into account any risk controls already in place);
- Any internal or external dependencies (including but not limited to infrastructure, utilities, human expertise, knowledge and experience, suppliers and customers).

Stage 2

The Business Impact Analysis or **BIA** provides detailed insight into the extent, timeframes and mechanisms of disruptive consequences and their likelihoods. Due to the varying size and complexity of most businesses, a tailored approach is often necessary to extract the relevant information. Personnel who are responsible for specific processes within the business function should be consulted. One consideration may be the justification to keep critical spares on site. There are five key steps in conducting the BIA, which are summarised on the following chart.



Contingency plan (CP) and contingent capability

Contingency planning is a form of risk treatment and is intended to improve the organisation's ability to respond quickly and optimally to disruptive events should they occur. The development of any additional contingent capability should be considered.

These include items such as providing back-up facilities, built-in redundancy, alternative supply arrangements or additional resource, say, in the form of a "Crisis Management Team".

There is no standard content for a contingency plan, however, a recommended list of contents is shown in the following table:

Content	Description
1. Introduction	
1.1 Organisational details	Name of organisation, location, areas specifically covered by the plan, etc.
1.2 Objectives	Key organisational objectives that the plan is addressing.
1.3 Purpose	Specific purpose of the plan.
1.4 Critical business function	Details of the critical business function, process, critical asset, etc. to which the CP refers.
1.5 Assumptions	Key assumptions made in developing the plan, e.g. availability of key resources, constraints on scope of the plan etc.
1.6 Processes	Processes, subprocesses, etc. that comprise the critical business function, or support the use of the asset/facility.
1.7 Activation and stand down	Events, outage times, etc. that serve as triggers for the activation and deactivation of the CP. Arrangements, processes etc. for activation and stand down.
1.8 Responsibility	Named individual(s) with responsibility for the creation.
1.9 Version control and maintenance	Version number of the plan, date of creation, date of next review, details of reviews authorisations, sign-off of plan etc.
2. Operational requirements	
2.1 Critical success factors	What level of capability the critical business function, asset etc. must achieve. Specific contractual and regulatory delivery requirements should also be specified.
2.2 Interdependencies	Key internal and external interdependencies.
2.3 Outage times	Where relevant identify minimum acceptable outage times and/or required recovery time for critical functions, processes, resources etc.
2.4 Compliance	Compliance requirements and other obligations that have to be met following activation of the plan (e.g. regulatory, policy, contractual obligations etc.)
3. People	
3.1 Structure	Structure and reporting relationships of the team operating under the plan.
3.2 Roles and responsibilities	Roles and responsibilities of named key managers and staff.
3.3 Contact details	Business and after hours contact details of key managers, staff, suppliers, customers and other stakeholders. Wherever possible each key role should also have a deputy identified and alternate suppliers listed.

Content	Description
4. Continuity arrangements	
4.1 Coordination	Arrangements for coordination between plans and across multiple locations.
4.2 Accommodation	Details of alternate/backup site arrangements.
4.3 Resources	Types and quantities of resources required to support the activation and implementation of the CP. The plan should specify if dedicated resources are required or if access to shared resources is available. Include: ▼ People ▼ Information and documentation ▼ Accommodation ▼ Plant and property ▼ Budget ▼ Assets and other equipment ▼ Telecommunications ▼ IT systems and applications
4.4 Workarounds and alternate solutions	Identify tasks that can still be undertaken following a disruption, those tasks that cannot be undertaken and alternate solutions to those tasks to still achieve acceptable outcomes.
4.5 Continuity management tasks	Identify additional activities that have to be undertaken in response to the disruption (i.e. activities beyond those associated with routine activities), for example assessment of the impacts of the disruption, coordination of asset reallocation, staff briefings to be held, etc.
5. Communications	
5.1 Communications	Summary of communications requirements following activation of the plan
6. Appendices	
6.1 Other plans	Details of other related plans, availability, location and access.
6.2 Checklists	Activity checklists, aides-memoires, etc.
6.3 Maps and drawings	Location maps, site maps, architect drawings, layouts, etc.

Conclusion

BCM should be developed as part of the organisation's overall risk management plan. Development of an organisation's BCM and applicable Contingency Plans require a deep understanding of the organisation's objectives, operating environment and any dependencies of the business (for example, the relationship with suppliers and customers).

Good BCM practices should incorporate contingency preparedness for unforeseen events. It should equip the organisation with the capacity to:-

- Stabilise any disruptive effects as soon as possible
- Continue or resume quickly any business functions that are critical to the organisation's objectives
- Recover to normal operations in a timely manner
- Take advantage of any opportunities created by the event
- Take on any additional risk with confidence
- Reduce the likelihood and consequence that could cause a disruptive event in the first place.