



Resilience Capability - Risk Management

White Paper

Keith Sherringham

Copyright © IMS Corp. All rights reserved.

IMS Corp.
Asia - Pacific Headquarters
Suite 5, 275 Maroubra Road
Maroubra
Sydney NSW 2035
Australia

Tel: +61 (0)2 9314 2908
Fax: +61 (0)2 9314 2908
Email: info@imscorp.com.au
Web: www.imscorp.com.au

© Copyright IMS Corp. All rights reserved.

All referenced trademarks are those of their respective owners.

This document is for information purposes only and any advice given is of a general nature only and may not be applicable to an individual or a specific situation. IMS Corp. accepts no responsibility for any consequential loss or damage arising from the use of this document.

Abstract

Development of a resilience capability within a business requires a pragmatic business driven approach that includes an identification of and management of the risks impacting business. By their nature, resilience risks (such as loss of people or loss of infrastructure) are those risks that are unlikely to occur but should they occur, they would have a significant impact upon business operations. Unlike many other risks, resilience risks cut across all areas of business and are not highly dynamic. In essence, a resilience risk only changes when it becomes an issue.

Whilst resilient risks are important to a business, it is the capability of a business to sustain operations using an alternative system (process, function or entity) whilst a recovery is implemented, which is of importance for core business operations.

Further details around aspects of risk identification and management and business sustainability are presented in this document.



Table of Contents

- 1 Introduction 3
- 2 Resilience Risks 3
 - 2.1 Risk within Business 3
 - 2.2 Types of Resilience Risk 3
 - 2.3 Classification and Rating 5
 - 2.4 Risk Mitigation and Consequence Minimisation 5
- 3 Business Sustainability 6
- 4 Review 7

List of Figures

- Figure 1. Elements of risk 4

List of Tables

- Table I. Common resilience risks. 5
- Table II. Example of business sustainability 7



1 Introduction

This White Paper presents aspects of risk identification and management within the development of a resilience capability within organisations. Taking a pragmatic business driven approach, the key issues around resilience risks are presented, together with an identification of business sustainability. It is the gaps between the ability to sustain business using an alternative system (process, function or entity) whilst a recovery is implemented that drives the setting of priorities for core business operations.

Section 1 provides an introduction to this document. Section 2 addresses resilience risks and their role within business, whilst Section 3 details business sustainability using the risk based approach. Section 4 identifies the review of risks and business sustainability required for the regime to be effective.

2 Resilience Risks

2.1 Risk within Business

The first element to consider within resilience is risk. On a routine basis, business manages risks and a risk and issues based approach¹ is often standard practice across many areas of business. This risk based approach looks at what can impact business, the significance is assessed, determine any actions to address the risk or to accept the risk and then implement any changes required. The decisions are usually justified by cost. This same approach applies to managing resilience risks.

By their nature, resilience risks are those risks that are unlikely to occur but should they occur, they would have a significant impact upon business operations. Resilience risks can occur in any areas of business and are often an extension of existing risk classification groups, e.g. operational risk or regulatory risk. The management of resilience risks has both an immediate impact upon the business, as well as a strategic impact. Consequently, resilience risks are often aligned to strategic issues and decisions.

It is a mixture of routine operational risks as well as resilience risks that impact upon business, Figure 1.

2.2 Types of Resilience Risk

Within business both generic or common resilience risks and industry specific risks exist, Table I. Whilst the industry specific risks, e.g. aviation and a loss of fleet or construction and a building collapse, may technically reside within the generic resilience risks, operational practicality requires that these risks be specifically identified.

When identifying resilience risks, the cause needs to be considered in isolation from the risk, e.g. the risk of a loss / denial of building could be as simple as the locks failing or a street evacuation through to a natural disaster damaging the building on a long term basis.

One risk may lead to many other risks, e.g. a natural disaster can cause a loss of building and a loss of people. The identification of resilience risk is based on the factors impacting, e.g. a natural disaster is likely to have different factor impacting this risk than those of a loss of people.

¹ A risk – something that has the potential to impact upon the ability to achieve an outcome. An Issue – something that is impacting upon the ability to achieve an outcome, i.e. a risk has become an issue. An issue may not change the likelihood and/or consequence of a risk occurring.





Figure 1. Elements of risk.

Resilience Category	Resilience Risk
Industry Risks	Industry specific risk
	Industry specific risk
Business Risks	Loss of People
	Loss / Denial of Building
	Loss / Denial of Information
	Loss / Denial of Communication
	Loss of Plant & Equipment
	Loss of Suppliers and/or 3 rd Parties
	Loss of Infrastructure
	Process Change
Event Risks	Global / Regional War
	Health Emergency



Resilience Category	Resilience Risk
	Physical Attack on People or Assets
	Natural Disasters

Table I. Common resilience risks.

2.3 Classification and Rating

Two features of resilience risks that differentiate them from other business risks: their classification and rating.

- **Classification-** Risk practitioners often classify risk into categories, e.g. market risk or operational risk. By their nature, resilience risks cut across all areas of business and all other categories of risk. A loss of building can impact upon strategy, markets, operational as well as Information Communication Technology (ICT) risk. Recognition of the cross-business nature and impacts of resilience risks is more significant than their classification.
- **Rating –** Similarly, risk practitioners like to classify risk based on likelihood of occurrence and impacts or consequences. By definition, resilience risks are high impact but are low likelihood of occurrence. Unlike other forms of risk that are often highly dynamic, resilience risks seldom change and nor does their rating. In essence, a resilience risk only changes its rating when it becomes an issue.

2.4 Risk in Context

Resilience risks need to be viewed in context, i.e. what critical business functions are going to be impacted and any critical dependencies these functions have relating to the risk. Consider a significant loss of people. The following details are of value:

- **Risk Details –** Any details around the risk, e.g. factors that are currently serving to increase the risk such as re-negotiation of employment contracts leading to increased risk of strike action.
- **Critical Functions –** Detail any critical business functions that would be impacted. The interest is in the critical functions only.
- **Critical Dependencies –** Detail any critical dependencies (system, process, function or entity) that the critical areas of business depend on relating to the risk.

Examples are presented in Table II, together with details of risk mitigation and any response actions required to minimise consequences.

Resilience Category	Resilience Risk	Risk Details	Critical Functions	Critical Dependencies	Mitigation Required	Response Required
Business Risks	Loss / Denial of Building	Detail the risk	List critical functions only	List critical dependencies	Accept risk or detail action to mitigate	Detail actions to address for response to incident
	Loss of People	Enterprise agreements to be re-negotiated.	Call centres	List critical dependencies	Accept risk	Train alternative workforce



Resilience Category	Resilience Risk	Risk Details	Critical Functions	Critical Dependencies	Mitigation Required	Response Required
	Loss of Plant & Equipment	Aging of assembly line	Processing plant	N/A	Intensify inspection regime	N/A

Table II. Resilience risks in context, including mitigation and consequence minimisation (response required).

2.5 Risk Mitigation and Consequence Minimisation

Beyond knowing a risk, is a decisions of whether to accept a risk and/or any actions to be taken to mitigate a risk. In addition, any issues to be addressed in responding when a risk becomes an event also need to be identified.

- **Risk Mitigation** - Like any other form risk, the consequences of resilience risks becoming an issue can be mitigated, i.e. measures implemented to minimise the occurrence of a risk. Consider the example of a house burning down. By trimming the branches of the trees around the house and by regularly burning off any excess leaf debris in the area in the winter months, the likelihood of a fire occurring is mitigated. Similarly, actions can be taken to mitigate the occurrence of resilience risks but at some point however, further investment of effort and resources is not justified and the resilience risks just have to be accepted.
- **Consequence Minimisation** – The consequences of resilience risks can also be minimised. Consider the example of a house burning down. The previous regime described not only acts to mitigate the occurrence of fire but also serves to reduce the consequences should fire occur. Having an insurance policy is an example of an action to minimise the consequences but not to mitigate the risk of fire. Similarly, actions can be taken to minimise the consequences of resilience risks but at some point however, further investment of effort and resources is not justified and the resilience risks just have to be accepted.

3 Business Sustainability

Whilst the recognition and management of resilience risks is important to business, it is not the risks per se that are important but the capability of a business to sustain operations should a risk become an issue. This business sustainability is a function of the period of outage, the time to recover and ability to operate an alternative for the system (process, function or entity) impacted.

The following terms are identified:

- **Maximum Acceptable Outage** – States how long a business can sustain a loss of system (process, function or entity) for, before the loss significantly impacts the business.
- **Outage with Sustainable Contingency** – States how long a business can sustain a contingency for, before the loss and the contingency significantly impact the business. A contingency must be sustainable for more than 6-hours.
- **Acceptable Information Loss** – States how much information can be lost to a system (process, function or entity) before the loss of information causes a significant impact upon the business. This is a mixture of information lost and time to recover.
- **Current Recovery Time** – The stated time to recover a system (process, function or entity).

Business sustainability is important for the critical or core business areas only (the must haves to sustain business) because this shows the gaps in business sustainability and where resources need to be allocated to ensure a continuity of core business functions.



As a guide, the following time periods are of interest:

- <2 hours.
- 2-4 hours.
- 4-12 hours.
- 12-24 hours.
- 1-2 days.
- 2-5 days.
- >5 days.

Whilst the critically varies for all business, e.g. aviation companies can cease to exist within days, a critical business operation that can be sustained for days is of lower concern because this gives plenty of time to address alternatives, even if an extended recovery time exists. Critical operations that can only be sustained for a short period time are cause for concern, particularly where there is a long recovery time.

Consider the example shown in Table III for denial of information. The patient monitoring system is a critical system that not only takes days to recover, but operations can only be sustained for a short period, if any. This would be an area of concern for a business and resource should be allocated to address accordingly. Conversely, the inventory management system can be recovered in a period of time that is commensurate with the ability to sustain an alternative process (Table III).

Resilience Risks	Risk Details	Maximum Acceptable Outage	Outage with Sustainable Contingency (>6 hours)	Acceptable Information Loss	Current Recovery Time
Loss / Denial of Information	Patient monitoring system	<2 hours	2-4 hours	>12-24 hours	>5 days
	Inventory management system	12-24 hours	1-2 days	N/A	1-2 days

Table III. Example of business sustainability

Such a simple analysis allows the critical areas to be identified and the gaps in business sustainability recognised. From this analysis:

- An informed decision of risk acceptance can be made.
- Priorities can be set accordingly for resolution of issues.
- A guide to actions in a crisis for decision making is seen.

4 Review

Whilst both the resilience risks and the related business sustainability are subject to change, the changes are unlikely to occur very often. An annual review and/or a review when major changes in business environment occurs, is often sufficient.

