



Resilience Capability - Monitoring and Reporting

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

The establishment, management and maturity of an enterprise wide resilience capability requires that a reporting and monitoring framework exists. This should include:

- Governance Body – A pro-active board or committee that the reporting goes to for actioning, follow up and resolution.
- Feedback mechanism – A way for the governance body to provide feed back to the business and accountability to the business.
- Business Area Resilience Owner – An owner responsible for resilience capability and activities in a given area of business to make sure the reporting and required activities occur.
- Audit Function – A function for auditing resilience capability.

An effective framework covers three aspects of resilience reporting:

- Resilience Capability Reporting – Addresses the resilience capability of the enterprise against a minimum resilience standard, i.e. is a business area able to respond to a crisis?
- Resilience Risk Reporting – Details the acceptance of the resilience risks and what is being done to address them, i.e. is the resilience capability (ability to manage a crisis) commensurate with the gaps in business sustainability and the risk exposure.
- Iceberg Reporting – Executive summary of the major risks and issues impacting a business, i.e. what are the big ticket items impacting the enterprise and can we manage them if they occurred?

Further details around the development and management of an enterprise wide resilience capability are presented in this document.



Table of Contents

- 1 Introduction 3
- 2 Reporting 3
 - 2.1 Resilience Capability Reporting 3
 - 2.1.1 Minimum Requirement 3
 - 2.1.2 Question Answered 4
 - 2.1.3 Reporting 4
 - 2.1.4 Report Content 4
 - 2.1.5 Reporting Definitions 7
 - 2.2 Resilience Risk Reporting 8
 - 2.2.1 Question Answered 8
 - 2.2.2 Reporting 9
 - 2.2.3 Report Content 9
 - 2.2.4 Reporting Definitions 11
 - 2.3 Iceberg Reporting 12
 - 2.3.1 Question Answered 12
 - 2.3.2 Reporting 12
 - 2.3.3 Report Content 12
 - 2.3.4 Reporting Definitions 14
- 3 Monitoring 14
 - 3.1 Resilience Audit Function 14
 - 3.2 Tracking Capability 14
 - 3.3 Governance 15

List of Tables

- Table I. Suggested minimum requirement for developing and maintaining a resilience capability..... 6
- Table II. Illustration of a Resilience Capability Report..... 7
- Table III. Illustration of exceptions in a Resilience Capability Report. 7
- Table IV. List of traffic light definitions for Resilience Capability Report. 8
- Table V. Illustration of a Resilience Risk Report. 10
- Table VI. Illustration of exceptions in a Resilience Risk Report. 10
- Table VII. List of traffic light definitions for Resilience Capability Report. 12
- Table VIII. Extract of an example Iceberg report..... 13
- Table IX. Extract of an example resilience risk catalogue within an Iceberg report..... 14



1 Introduction

This White Paper presents some aspects of monitoring and reporting an enterprise wide resilience (risk management, crisis management, disaster recovery management and business continuity management) capability. Aimed at all levels of management across the enterprise, irrespective of industry sector, a pragmatic business driven approach is taken to monitoring and reporting an enterprise resilience capability.

Section 1 provides an introduction to this document. Section 2 details some general reporting issues as well as looking at the specific reporting of resilience including Resilience Capability Report, Resilience Risk Report and Icebergs Report. Section 3 looks at aspects of monitoring an enterprise resilience capability, including governance and a resilience audit function.

2 Reporting

Reporting of an enterprise resilience capability needs to be simple, pragmatic and deliver benefit to the business. Reporting that is onerous and that is seen as an after thought to regular business activities, will seldom be adopted by the business or be successful and sustainable. The purpose of the reporting is to deliver outcomes for the business, and to achieve this, an exceptions based approach is required.

Exceptions reporting is about noting the issues and what is being done to address them. Exceptions reporting is focuses on what is “going wrong” and how and when the issues will be sorted, i.e. they tend to convey bad news only. In addition to being effective in reporting issues, exceptions reporting has benefit in driving cultural change, accountability, ownership and changes the “good news only” syndrome that may exist in many large organisations. For resilience capability reporting the following are required:

- Governance Body – A pro-active board or committee that the reporting goes to for actioning, follow up and resolution.
- Feedback mechanism – A way for the governance body to provide feed back to the business and accountability to the business.
- Business Area Resilience Owner – An owner responsible for resilience capability and activities in a given area of business to make sure the reporting and required activities occur.
- Audit Function – A function for auditing resilience capability, see Section 3.1.

There are three aspects to reporting resilience:

- Resilience Capability Reporting – Addresses the resilience capability of the enterprise against a minimum standard (see Resilience Capability – Capability Management).
- Resilience Risk Reporting – Details the acceptance of the resilience risks (see Resilience Capability – Risk Management) and what is being done to address them.
- Iceberg Reporting – Executive summary of the major risks and issues impacting a business.

2.1 Resilience Capability Reporting

2.1.1 Minimum Requirement

Within enterprise resilience capability, the key resilience areas need to be present and a minimum capability specified (see Resilience Capability – Capability Management) around them, Table I. Although other requirements can be added to this minimum, this would not change the approach and principles used for the reporting.



2.1.2 Question Answered

A report is designed to answer one specific question and this is the purpose and focus of the report. Whilst a report may also address other questions, having one report addressing too many questions leads to confusion and ambiguity.

The Resilience Capability Report answers the question:

- Is a business area able to respond to a crisis?

If a business area meets the minimum criteria, then it should be able to adequately respond to a crisis.

If a business area does not meet the minimum criteria, then what is being done to address the issues?

2.1.3 Reporting

The reporting should be:

- At set intervals, e.g. three times a year, or should special circumstances require.
- Against progress made according to the minimum resilience requirement.
- Dependent upon a financial year, i.e. last year's data do not roll across.

2.1.4 Report Content

The report should include:

- Report Name – Name of the report, e.g. Company xx Resilience Capability Report.
- Report Date – Date of the report produced.
- Resilience Capability Summary – A summary of resilience capability by activity, rated against the minimum standard.
- Exceptions – Specific issues around a resilience capability reported on an exceptions basis as required.
- Definitions – Definitions of the scales used, e.g. Red / Amber / Green in the report.
- Addendum – Specific issues and reports as required.

The report presents the resilience capability for given business areas against the minimum requirements, Table II. An enterprise wide summary and overall assessment can also be reported, Table II.

Although the reporting definitions may vary, a simple Red / Amber Green rating is readily understood and easily applied. For a Red / Amber Green rating, the following principles apply:

- Green – All criteria to be met for Green to apply.
- Amber – Amber over rides Green, i.e. if anyone criteria Amber - rate Amber.
- Red – Red over rides Amber, i.e. if anyone criteria Red - rate Red.

Although this may seem strict, the approach ensures integrity to the process, whilst focusing on the issues.



Resilience Activity	Description	Occurrence	Reporting
Risk Management	Review of resilience risks and acceptance or mitigation of these risks	Annual review, in line with financial year, and/or when a major change in business environment occurs.	Report resilience risks as part of routine risk reporting. Semi-annual reporting of acceptance or mitigation.
Business Sustainability Management	Identification and management of gaps in business sustainability based on the resilience risks identified.	Annual review, in line with financial year, and/or when a major change in business environment occurs.	Annual reporting of business sustainability capability.
Business Management in a Crisis	Strategies (framework) and priorities for managing the business through a crisis (business and/or enterprise level).	Annual review, in line with financial year, and/or when a major change in business environment occurs.	Annual reporting of revised strategy and framework.
Crisis Management	Development and/or review of plans, policies and procedures.	Annual review, in line with financial year. Review when a major change in business environment occurs. Review when lessons from testing and training need to be included.	Annual reporting of revised plans, policies and procedures.
Capability Management	Desktop Exercises	Senior leadership in each business area and executive leadership across the enterprise, conduct two desktop scenario exercises a year. Suggest an hour for each one. One exercise aligns with end of financial year planning and the other is conducted as appropriate.	Reporting of the exceptions from the exercise as conducted.
	Integrated Exercises	Two cross enterprise integrated exercises per year.	Reporting of the exceptions from the exercise as conducted.



Resilience Activity	Description	Occurrence	Reporting
	Call Out Test	Annual test to invoke crisis management structures, including crisis management team. Test to be commensurate with business need and risks.	Reporting of the exceptions from the exercise as conducted.
	Alternative Process Test	Annual test to invoke an alternative process for a loss of system (process, function or entity) and sustain operations. Test to be commensurate with business need and risks.	Reporting of the exceptions from the exercise as conducted.

Table I. Suggested minimum requirement for developing and maintaining a resilience capability.



As the capability matures, the criteria can be extended and tightened. Although weightings can be used for in averaging and for critical versus less critical areas, it is best to start simple and develop the complexity as the capability matures.

Business Area	Risk Management	Business Sustainability	Business Management in a Crisis	Crisis Management Plans	Leadership Desktop Sessions	Call Out Test Compliant	Alternative Process Test Compliant	Integrated Exercises	Overall Assessment
Business 1	A	A	R	G	A	TBA	R	G	R
Business 2	G	G	R	G	G	G	N/A	G	R
Enterprise	A	A	R	G	A	G	R	G	R

Table II. Illustration of a Resilience Capability Report.

The exceptions reporting around the resilience capability are as shown in Table III.

Business Area	Issues Identified	Actions Required	Owner	Resolution Date	Progress
Operations	Owner for resilience capability to be appointed	Outcomes from restructure to be determined before further progress can be made	GM Operations	Mar-09	A
Business 2	Business sustainability analysis not completed	GM for business area to secure funding of a resource to conduct analysis	GM 2	Mar-09	R

Table III. Illustration of exceptions in a Resilience Capability Report.

2.1.5 Reporting Definitions

Irrespective of the definitions adopted, they need to be detailed in the report. An example is as shown in Table IV.

Category	Flag	Definition
Progress	R	No progress and/or major slippage in schedule



Category	Flag	Definition
	A	Limited progress and/or slippage in schedule
	G	Proceeding to schedule
Overall Assessment	R	Business shows: <ul style="list-style-type: none"> Limited ability to bounce back. Leadership is weak around resilience management. Plans and strategies do NOT meet minimum requirements. Limited capability to effectively respond to an emergency. Culture is not aligned to that required of the Enterprise.
	A	Business shows: <ul style="list-style-type: none"> Capability to bounce back. Leadership is addressing resilience management. Plans and strategies are being addressed to align with Enterprise practice. Capability to effectively respond to an emergency. Culture is aligning to that required of the Enterprise.
	G	Business shows: <ul style="list-style-type: none"> Good capability to bounce back. Leadership is pro-active in resilience management. Plans and strategies meet minimum requirements. Good capability to effectively respond to an emergency. Culture readily aligns to that required of the Enterprise.

Table IV. List of traffic light definitions for Resilience Capability Report.

2.2 Resilience Risk Reporting

2.2.1 Question Answered

A report is designed to answer one specific question and this is the purpose and focus of the report. Whilst a report may also address other questions, having one report addressing too many questions leads to confusion and ambiguity.

The Resilience Risk Report answers the question:

- Are the risks a business faces commensurate with their ability to respond and to sustain business?



It is not the risk per se that is the issue, it is the ability to sustain business and to manage a crisis for a given level of risk that is significant.

If a business area has a strong resilience capability and a sustainable business operation then it is well placed to manage the business through a crisis.

If a business area has a strong resilience capability but has a high-risk exposure and a low business sustainability capability, then the business is vulnerable.

If a business area has a weak resilience capability, a high-risk exposure and a low business sustainability capability, then the business is highly vulnerable. For a core business operation, this would be unacceptable and resources would be allocated accordingly to address.

2.2.2 Reporting

The reporting should be:

- At set intervals, e.g. three times a year, or should special circumstances require.
- Against changes in risk, business sustainability and progress made according to the minimum resilience requirement.
- Dependent upon a financial year, i.e. last year's data do not roll across.

2.2.3 Report Content

The report should include:

- Report Name – Name of the report, e.g. Business area xx Resilience Risk Report.
- Report Date – Date of the report produced.
- Overall Assessment – An overall statement of the ability to sustain business and to manage a crisis for that level of risk.
- Sustainable Contingency Assessment – An overall statement on the gaps in business sustainability (obtained from the Business Sustainability Management details).
- Resilience Capability – A rating of the resilience capability of the business area (obtained from minimum resilience criteria and Resilience Capability Report).
- Risk Assessment – For the resilience risks, identify gaps in business sustainability and an acceptance or mitigation of that risk.
- Exceptions – Specific issues around risk mitigation reported on an exceptions basis as required.
- Definitions – Definitions of the scales used, e.g. Red / Amber / Green in the report.
- Addendum – Specific issues and reports as required.

For a given business area, the report presents the risks, the gaps in business sustainability and the acceptance or mitigation of the risk, Table V. A report is compiled for each business area.

Although the reporting definitions may vary, a simple Red / Amber Green rating is readily understood and easily applied.



Resilience Category	Resilience Risk	Business Sustainability	Actions for Resolution
Industry Risks	Industry specific risk	G	Accept current regime
	Industry specific risk	R	Accept current regime
Business Risks	Loss of People	R	Accept current regime
	Loss / Denial of Building	R	Accept current regime
	Loss / Denial of Information	R	Major upgrade of IT systems underway
	Loss / Denial of Communication	R	Accept current regime
	Loss of Plant & Equipment	A	N/A
	Loss of Suppliers and/or 3 rd Parties	A	Accept current regime
	Loss of Infrastructure	N/A	N/A
	Process Change	N/A	N/A
Event Risks	Global / Regional War	N/A	Enterprise Response
	Health Emergency	N/A	Enterprise Response
	Physical Attack on People or Assets	N/A	Enterprise Response
	Natural Disasters	N/A	Enterprise Response

Table V. Illustration of a Resilience Risk Report.

The exceptions reporting around risk mitigation are as shown in Table VI.

Risk	Issues Identified	Actions Required	Owner	Resolution Date	Progress
Loss / Denial of Systems (Information)	Core systems need to be backed up and recovery plans developed	Project manager to be replaced and timeframe for implementation revised	GM Operations	Mar-09	A

Table VI. Illustration of exceptions in a Resilience Risk Report.



2.2.4 Reporting Definitions

Irrespective of the definitions adopted, they need to be detailed in the report. An example is as shown in Table IV.

Category	Flag	Definition
Progress	R	No progress and/or major slippage in schedule
	A	Limited progress and/or slippage in schedule
	G	Proceeding to schedule
Operational Sustainability	R	Major gaps between business critical system (process, operation or entity) with alternative processes invoked and recovery time (>12 hours)
	A	Significant gaps between business critical system (process, operation or entity) with alternative processes invoked and recovery time (4-12 hours)
	G	Minor gaps between business critical system (process, operation or entity) with alternative processes invoked and recovery time (2-4 hours)
Resilience Capability	R	Business shows: <ul style="list-style-type: none"> Limited ability to bounce back. Leadership is weak around resilience management. Plans and strategies do NOT meet minimum requirements. Limited capability to effectively respond to an emergency. Culture is not aligned to that required of the Enterprise.
	A	Business shows: <ul style="list-style-type: none"> Capability to bounce back. Leadership is addressing resilience management. Plans and strategies are being addressed to align with Enterprise practice. Capability to effectively respond to an emergency. Culture is aligning to that required of the Enterprise.



Category	Flag	Definition
	G	<p>Business shows:</p> <ul style="list-style-type: none"> • Good capability to bounce back. • Leadership is pro-active in resilience management. • Plans and strategies meet minimum requirements. • Good capability to effectively respond to an emergency. • Culture readily aligns to that required of the Enterprise.

Table VII. List of traffic light definitions for Resilience Capability Report.

2.3 Iceberg Reporting

The Resilience Capability Report and the Resilience Risk Report are valuable tools within the business and provide a basis for a final report – the Iceberg Report. As its name suggests, the Iceberg Report is about “icebergs” the big ticket items that the Executive need to know about and action.

2.3.1 Question Answered

The Iceberg Report answers the question:

- What are the big ticket items impacting the enterprise and can we manage them if they occurred?

Similar to the Resilience Risks Report, it is not the risk per se that is the issue, but it is the ability to sustain business and to manage a crisis for a given level of risk that is significant. The Iceberg Report is in essence a summary of the Resilience Risk Report, the Resilience Capability Report and other operational risks impacting business aggregated up through the exceptions reporting. Only those issues that rate a Red, maybe Amber, rating would appear on the Iceberg Report.

2.3.2 Reporting

The reporting should be:

- At set intervals, e.g. three times a year, or should special circumstances require.
- Against changes in risk, business sustainability and progress made according to the minimum resilience requirement.
- Dependent upon a financial year, i.e. last year’s data do not roll across.

2.3.3 Report Content

The report should include:

- Report Name – Name of the report, e.g. Business area xx Resilience Risk Report.
- Report Date – Date of the report produced.
- Icebergs – details of the risks (icebergs – major operational risks and resilience risks), the impacted business, the business sustainability, the resilience capability and what is being done to address the icebergs.



- Definitions – Definitions of the scales used, e.g. Red / Amber / Green in the report.
- Addendum – Specific issues and reports as required.

The report paints a picture of the major items impacting upon the enterprise, both operational and resilience related, and what is required of Executive Leadership to address, Table VIII.

Risk	Business Area	Owner	Operational Sustainability	Resilience Capability	Issues Identified	Actions Required	Resolution Date	Progress
Loss of Systems (Information and Communication)	Enterprise	CEO	R	A	Overall performance is not commensurate with business need. Core systems are not backed up and recovery times are less than required by the business.	Board to approve a renegotiation of out-sourcing contracts.	TBA	R
Loss of Building	Business 1	COO	R	A	Core operational area has no disaster recovery capability commensurate with business need	Solution has been determined but approval of expenditure on solution required	TBA	A
Customer Service and Offering	Business 2	COO	A	A	Access to capital is delaying the acquisition of new plant and equipment with higher cost and impacted services	COO seeking Board approval for additional expenditure	TBA	A

Table VIII. Extract of an example Iceberg report.

A catalogue of resilience risks and any related issues for the risk, Table IX, may exist to serve as a prompt.



Resilience Category	Resilience Risk	Risk Overview
Business Risks	Loss of People	No issues identified.
	Loss / Denial of Building	No issues identified.
	Loss / Denial of Systems (Information)	See Icebergs.
	Loss / Denial of Systems (Communication)	See Icebergs.
	Loss of Plant & Equipment	No change in conditions.
	Loss of Suppliers & 3 rd Parties	No issues identified.
	Loss of Infrastructure	No issues identified.
	Process Change	No issues identified.

Table IX. Extract of an example resilience risk catalogue within an Iceberg report.

2.3.4 Reporting Definitions

Irrespective of the definitions adopted, they need to be detailed in the report. In this example, the definitions from the Resilience Risk Report, Table IV, are applicable.

3 Monitoring

Underlying the reporting is the tracking or monitoring within the business of what resilience activities are being undertaken and what is being done to meet the minimum resilience enterprise requirement.

3.1 Resilience Audit Function

Similar to an audit function, the results, particularly the exceptions, of the resilience activities (tests, exercises and plan review etc.) need to be reported and followed up accordingly. Whether a group as part of the audit function or a stand-alone group is created to manage conformance to a minimum resilience capability, is a business call. Either way, such a capability needs to exist.

3.2 Tracking Capability

A simple tracking tool, common to many audit operations, is required for reporting issues and items for action and follow up that arise from monitoring the resilience capability. Whether it is a simple spreadsheet, a database or a more powerful application, the following information is the sort of details that need to be tracked:

- Issue Number - A number for tracking an issue.
- Date Raised – The date an issue was raised.



- Source Activity – The name of the activity, from the minimum resilience capability, that created the issue, e.g. call out test or leadership desktop exercise.
- Activity Details – Further details around the activity, e.g. the scenario of the test.
- Compliance Issues – The exceptions reported, e.g. crisis plan not align with minimum enterprise standard.
- Issue Owner – Who in the business owns the issue.
- Business Area – Name of the impacted business area.
- Business Impact – An assessment of the impact to the business from not addressing the issue: Extreme, High, Medium or Low.
- Resolution Date: Expected date for resolution of the issue.
- Issues Status – The status of the issue: Open, Closed, Re-opened or Deactivated. In line with standard audit practice: once raised, an issue cannot be deleted.
- Auditors Name – Name of the person who raised the issue.
- Comment – A general comment field for further details.

As items are reported, they are raised and tracked by the resilience audit function to assure the minimum resilience capability is met.

3.3 Governance

Like any other business operation that is monitored and audited for compliance, a pro-active board or committee for governance purposes is required. As well as overseeing the overall resilience capability and development across the enterprise, this entity needs to receive the reports, action, follow up and have the mandate to resolve resilience related issues.

Developing, managing and maturing a resilience capability is core competency that needs to be pro-actively managed.

