



# **Resilience Capability - Critical Systems Analysis**

## **Briefing Document**

Keith Sherringham

**Copyright © IMS Corp. All rights reserved.**

IMS Corp.  
Asia - Pacific Headquarters  
Lvl 17 44 Market Street  
Sydney NSW 2035  
Australia

Tel: +61 (0)412 16 18 70  
Email: [info@imscorp.com.au](mailto:info@imscorp.com.au)  
Web: [www.imscorp.com.au](http://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.

# Table of Contents

- 1 Introduction .....2
- 2 Critical Systems Analysis .....2
  - 2.1 Purpose of Critical Systems Analysis .....2
  - 2.2 Completion of Critical Systems Analysis .....2
  - 2.3 Contingencies .....2
  - 2.4 Common Requirements .....2
- 3 Elements of a Critical Systems Analysis .....2
- 4 Contingency Analysis .....5
- 5 Critical Buildings .....6
- 6 Terminology .....7
  - 6.1 Terms .....7
  - 6.2 Periods .....7
  - 6.3 Significance to Business .....8
  - 6.4 Policy and Procedure Documentation .....8

# List of Tables

- Table I. Information for a Critical Systems Analysis.....5
- Table II. Information for contingency analysis in a Critical Systems Analysis.....6
- Table III. Information for key buildings in a Critical Business Analysis. ....7



# 1 Introduction

This document details how a comprehensive and authoritative set of business system requirements for business continuity planning or disaster recovery management can be gathered using the accompanying Excel spreadsheet xx\_crit\_sys.xls. This document is to be used by those undertaking a Critical Systems Analysis and/or providing information for a Critical Systems Analysis. The purpose of this document is to provide a guideline only for collation of Critical Systems Analysis information.

## 2 Critical Systems Analysis

### 2.1 Purpose of Critical Systems Analysis

A Critical Systems Analysis is a document created by an area of business in an organisation and details the key dependencies (systems, processes or entities) for critical business functions. The document serves as a guide in decision making for business continuity, disaster recovery and crisis management.

### 2.2 Completion of Critical Systems Analysis

The initial Critical Systems Analysis is completed by having a designated party conduct interviews with key people in the business and in ICT to collate the required information and populating the xx\_crit\_sys.xls spreadsheet. A peer review of the document is also required.

A Critical Business Analysis should be completed prior to completing a Critical Systems Analysis.

A Critical Systems Analysis should be reviewed annually and/or when there is a major change in business environment by having the respective parties review and update the xx\_crit\_sys.xls spreadsheet.

### 2.3 Contingencies

Whilst addressing the critical systems and gaps in the sustainability of systems, an identification of “what the business contingency is” should also be identified. It is the gap in the business contingency and the time to recover a system that is important.

### 2.4 Common Requirements

The common requirements of a Critical Systems Analysis include:

- Data are presented in an Excel spreadsheet for ease of searching and filtering.
- Content to be written in English with correct grammar and spelling.
- Document to be easy to read and informative for end users.
- Standard document information should be tracked including date of last edits.
- Document should focus on critical issues.

## 3 Elements of a Critical Systems Analysis

The main elements of a critical systems analysis relate to the following:

- System Details – Key information about the system include its business criticality.



- Environment – Details around the environment in which the system is housed.
- Backup – Details on systems backup.
- System Recovery – Addresses whether a system can be effectively recovered to meet business needs.
- Data Recovery - Addresses whether data can be effectively recovered to meet business needs.
- Specification – Further systems information including systems dependencies.
- Other Information – Any other information that is significant to the recovery of a system.

Use the “critical\_systems” tab in the xx\_crit\_sys.xls spreadsheet. The information required is as shown in Table I.

Category	Field	Details
System Details	System Name	Full name of the system, e.g. Oracle Financials.
	System Purpose	State the purpose of the system, e.g. door access control and monitoring or payroll.
	Disaster Recovery	Detail the disaster recovery currently in place for the system, e.g. automatic failover to redundant server in Melbourne or Supplier provided.
	Capacity Constraints	Detail any known capacity constraints, e.g. servers currently at 95% capacity and unable to take additional load.
	Support Contract	Detail any support contracts in place, e.g. 24*7 onsite support from IBM.
	Redundancy	Detail any redundancy that exists in the system, e.g. clustered and load balanced servers with hot swappable disks.
	Significance	Detail the significance to the business. Select form list (Critical, Important, Routine, Non-Essential).
Environment	Housed	Detail where the system is housed. Select form list (Computer Room, Data Centre, Switch Room, Under Desk, Unknown, N/A).
	Location	Detail the location of the system. Select from list (Onsite, Offsite, Supplier, Unknown, N/A).
	Dual Cordage	Do the servers for the system use redundant power supplies? Select form list (Implemented, Absent, Unknown, N/A).
	Dual UPS	Are the servers for the system provided with dual uninterruptable power supply (UPS)? Select from list (Absent, Implemented, Unknown, NA).
Backup	Ghost Images	Do ghost images or similar exist for the servers on which the system reside and what is their status? Select form list



Category	Field	Details
		(Absent, Operational, Outdated, Unknown, N/A.)
	Type	Detail the principal backup type for the system. Select from list (Full, Partial, Incremental, None, N/A).
	Storage Location	Detail the location for storage of the data backup. Select from list (Onsite, Offsite, Supplier, Unknown, N/A).
	Frequency	Detail the frequency of the backup for the system. Select from list (Hourly, 12-hours, Daily, None, Weekly, Unknown, N/A).
Systems Recovery	Recovery Time	State the estimated recovery time for the system. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days).
	Procedures	Detail the procedures that exist for recovery of the system. Select from list (Absent, Operational, Outdated, Unknown, N/A).
	Last Tested	State the date when system recovery was last tested. A blank date assumes unknown or not done in the last 2-years.
Data Recovery	Recovery Time	State the estimated recovery time for the data. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days).
	Procedures	Detail the procedures that exist for recovery of the data. Select from list (Absent, Operational, Outdated, Unknown, N/A).
	Last Tested	State the date when data recovery was last tested. A blank date assumes unknown or not done in the last 2-years.
Specification	Supplier	Who is the supplier of the system and any other key details, e.g. ABC Pty. Ltd.
	Operating System	What operating system supports the application / system? Include version control details, e.g. Solaris 6.3.5.
	Hardware Requirement	Detail any specific hardware requirements required by the system. The focus is on the unique.
	Critical Dependencies	List any systems and other dependencies that underpins the system, e.g. uses data feed from Australian Customs.
	Critical Systems Impacted	List any other critical systems that rely upon this system, i.e. if this system goes down what else goes down?
	Primary Host Name	Name of the primary host (server) for the application.
	Configuration	Detail the procedures that exist for recovery of the system. Select



Category	Field	Details
	Documentation	from list (Absent, Operational, Outdated, Unknown, N/A).
Other Information	Contact	Name of the contact or subject matter expert that provided the details.
	Comment	Any additional information that is very important to the ability to recover the system.

Table I. Information for a Critical Systems Analysis.

## 4 Contingency Analysis

A Contingency Analysis details what the business contingency is when a system (process, function, entity) is lost and for how long the contingency can be maintained. A contingency that cannot be maintained for more than 6-hours at about 80% of business as usual capacity is not really a contingency.

Use the “contingency” tab in the xx\_crit\_sys.xls spreadsheet. The information required is as shown in Table II.

Field	Details
Business Function	Name the business function that would be impacted. This should be critical business functions only, e.g. accounts payable or payroll.
Business Significance	Detail the significance to the overall business of the business function. Select form list (Critical, Important, Routine, Non-Essential).
System (process, function or entity)	Name of the system used by the critical Business Function, e.g. Oracle Financials.
Significance to Business	Detail the significance of the system to the business function. Select form list (Critical, Important, Routine, Non-Essential).
Maximum Acceptable Outage	State how long (approximately) a business function can sustain a loss of system (process, function or entity) for, before the loss significantly impacts the business. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days).
Sustainable Contingency (>6 hours)	Describe the contingency to be used in the event that a system is lost, e.g. for a failure of the door access and control system a statement like “place security guards on key doors and access points” would be appropriate. A statement of manual process is not sufficient. A contingency should be maintained for more than 6-hours at about 80% of business as usual capacity.
Contingency Tested	State the date when the contingency was last tested. A blank date assumes unknown or not done in the last 2-years.
Estimated Recovery Time	State how long (approximately) it would take to recover a system (process, function or entity). Select from list (<2 hours, 2-4 hours, 4-12



Field	Details
	hours, 12-24 hours, 1-2 days, 2-5 days, >5 days).

Table II. Information for contingency analysis in a Critical Systems Analysis.

## 5 Critical Buildings

For information on critical buildings use the “critical\_buildings” tab in the xx\_crit\_bus.xls spreadsheet. The information required is as shown in Table III.

Category	Field	Details
Building Significance	Building Name	Enter the name or code of the building.
	Building Type	State the building type. Select from list (Depot, Factory, Hangar, Office, Operations Centre, Plant, Shop, Special Use, Terminal, Warehouse).
	Significance to Business	Detail the significance to the business. Select form list (Critical, Important, Routine, Non-Essential).
Building Capacities	Emergency Capacities (lighting stairwells etc)	Detail the emergency capacities of the building, e.g. emergency lighting in stair wells. Aim is to establish if minimal regulatory requirements are met.
	UPS Duration	Detail the Uninterruptable Power Supply (UPS) duration for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Generator Duration	Detail the duration of the backup generators for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Backup Power Duration - Lighting	Detail the duration of the lighting on backup power for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Backup Power Duration - Plant	Detail the duration of any plant operations on backup power for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Backup Power Duration - Air-conditioning	Detail the duration of the air-conditioning on backup power for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Backup Power Duration –	Detail the duration of equipment on backup power for the building under normal work load. Select from list



Category	Field	Details
	Equipment	(<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Water Supply Duration	Detail the water supply duration for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Gas Supply Duration	Detail the gas supply duration for the building under normal work load. Select from list (<2 hours, 2-4 hours, 4-12 hours, 12-24 hours, 1-2 days, 2-5 days, >5 days, N/A).
	Special Equipment Required	Detail any special equipment required by the business in that building, i.e. if we were to duplicate the capabilities of the building what specialities would be required.
	Backup Connectivity	Describe the network backup connectivity to the building, e.g. dual backbone at different entry points.

Table III. Information for key buildings in a Critical Business Analysis.

Where required, duplicate the name of the business function. Some may choose to do all buildings for completeness with the appropriate significance to business rating.

## 6 Terminology

The following terms and references are used in this Critical Systems Analysis.

### 6.1 Terms

The following terms are used:

- 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.
- Recovery Time – The stated time to recover a system (process, function or entity).
- Sustainable Contingency – A contingency to be implemented in the event of a loss of system (process, function or entity) that can be sustained for more than 6-hours at about 80% of business as usual level.

### 6.2 Periods

Use the following periods as a guide:

- <2 hours
- 2-4 hours
- 4-12 hours
- 12-24 hours



- 1-2 days
- 2-5 days
- >5 days

An upper criterion of 5-days is used because:

It is about buying time to manage a crisis whilst more sustainable alternatives are implemented.

If an impact is not seen before 5 days, then it is a very low priority.

If something takes more than 5-days to recover then what are the alternatives?

## 6.3 Significance to Business

Use the following periods as a guide:

- **Critical** – Must have systems (function, processes or entities) to support the most important business functions, i.e critical business operations come to a halt without it.
- **Important** – Necessary systems (function, processes or entities) to support the most important business functions, i.e critical business operations can work around the loss for a reasonable period of time while the problem is fixed.
- **Routine** – A system (function, processes or entities) that is background to critical business functions, i.e. critical operations keep going for extended periods of time without it.
- **Non-Essential** – Something that critical areas of business are NOT reliant upon or can function without for an extended period of time.

## 6.4 Policy and Procedure Documentation

Whether it is an operational procedure, a policy on data backup or an emergency evacuation card, a range of documentation on policies and procedures are required. Use the following as a guide to identify the operational readiness of the documentation:

- **Absent** – Little or no current and quality documentation exists.
- **Operational** – Documentation is current, has been signed-off and people can pick up and use to deliver the required outcomes.
- **Outdated** – Documentation exists but has not been kept Operational.
- **Unknown** – The status of the documentation or its existence is unknown.

In essence, if documentation can be readily retrieved from a shelf or from a document management system, and the documentation is current, has been approved and allows people to effectively perform the required task(s), then it is considered “Operational”. Document that is not classified as “Operational” is deemed to be inadequate for the needs of business continuity and disaster recovery.

