Company X

IT Disaster Recovery Plan

(BCP0005)

Document version control

Version	Date	Author(s)	Summary of changes

Document approvals

Approving body	Roles	Version

Document distribution

Referenced documents

Title	Location	Version

Document Review History

Reviewed By	Title	Date

Table of Contents

1. INTRODUCTION

1.1. Policy Statement

> ***A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.***
>
> **AS/NZS ISO/IEC 17799:2001 Clause 11.1**

It is the policy of Company X to develop and maintain enterprise-wide disaster recovery plans (DRP's) for Company X's IT services. These will provide Company X with the opportunity to recover from a catastrophic event, be it accidental, man-made or natural, and resume IT operations in an efficient and effective manner.

This DRP is designed to reduce the risks of COMPANY X failing to continue to operate the IT element of business critical functions in the face of various crisis situations. It is recognized that the probability of a severe disaster is low, however the existence of a DRP is considered vital should an emergency occur.

The ultimate goal of the DRP is to allow COMPANY X IT facilities to resume essential business operations at an alternate location within a predictable time.

1.2. Scope of this Plan Document

This document outlines the steps to be taken to restore COMPANY X's IT facilities in a controlled manner and in line with defined business application priorities. It is not a Business Continuity Plan since it only addresses the IT component of business applications. Business Continuity Plans are the responsibility of the relevant business units.

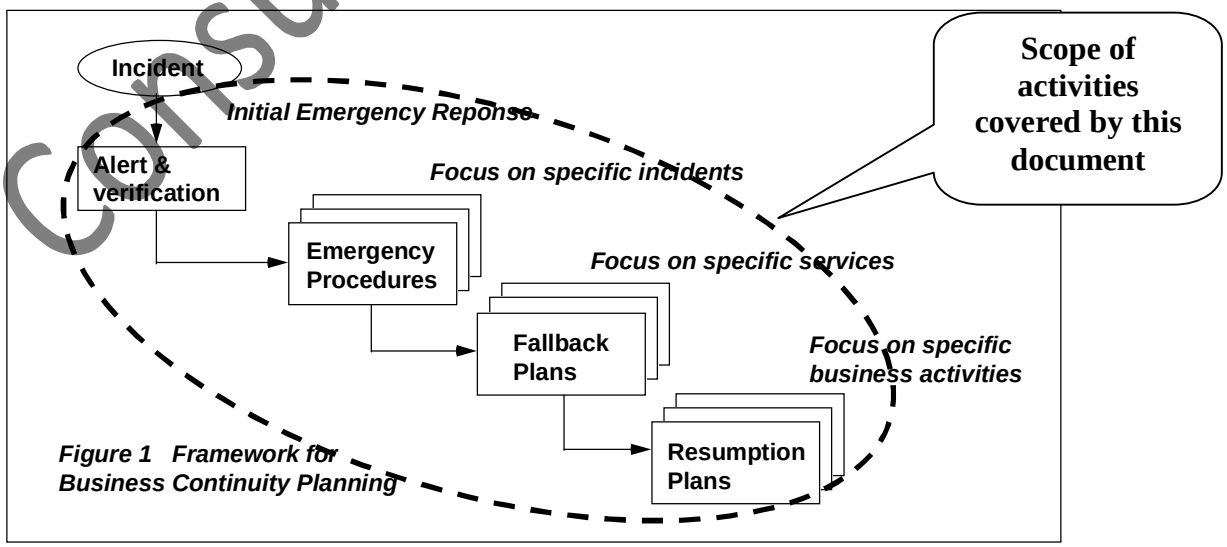


Figure 1 Framework for Business Continuity Planning

1.3. Disaster Scenarios

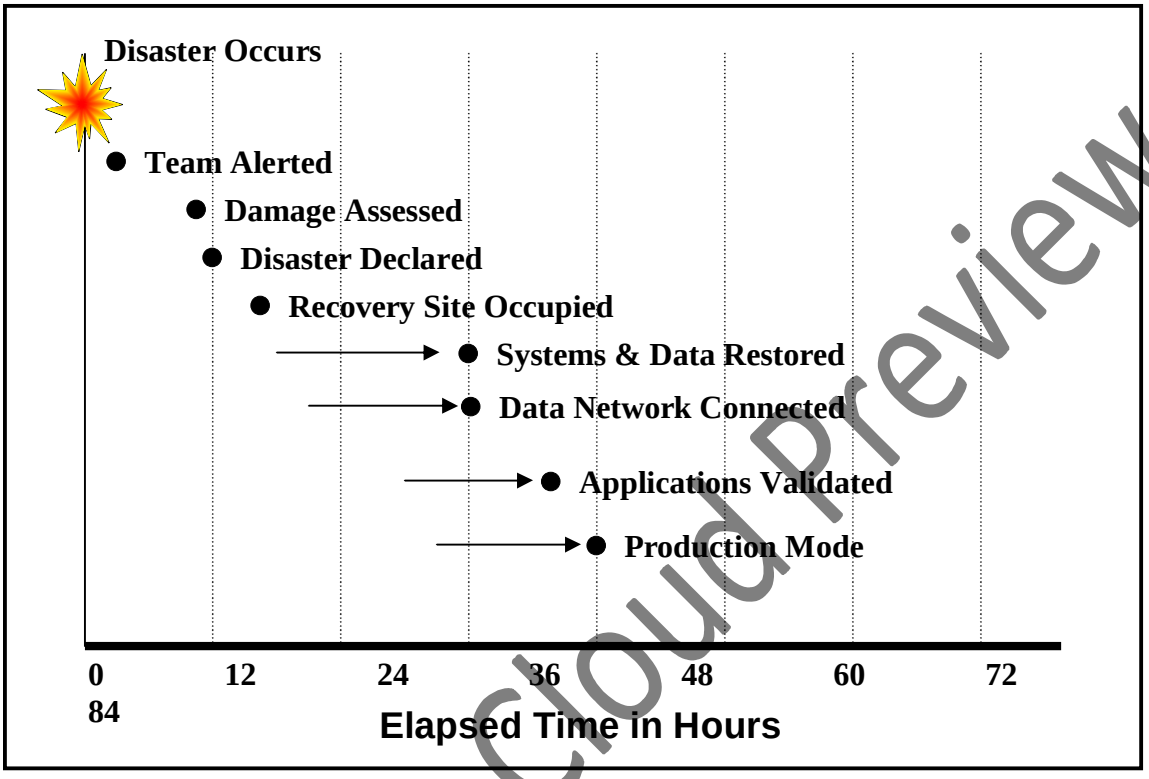
All scenarios assume that the disaster is likely to continue for more than two working days.

Facility	Scenario A	Scenario B	Scenario C
Secondary Data Centre	✓	✓	✓
COMPANY X Computer Room 1	✗	✗	✗
COMPANY X Computer Room 2	✗	✓	✓
COMPANY X general office facilities	✗	✗	✓

✓ Facility is accessible and operable ✗ Facility is inaccessible and inoperable

1.4. Conceptual Recovery Time Line

The graphic below depicts the typical progression of steps and activities anticipated within a well-orchestrated disaster recovery plan.



NOTE: Clients should not expect any production COMPANY X computing services to be available within the first 48 hours after a disaster declaration. All client business recovery plans should include this as a basic planning assumption.

1.5. Assumptions

This Disaster Recovery Plan has been prepared with these assumptions:

Facilities

- The recovery will be controlled from an IT Control Centre in Head Office.
- An alternative IT Control Centre location will be established if Head office is unavailable.
- A contingency site will be established and will become the interim office Headquarters for Company X under Scenarios A and B (i.e. Head Office unavailable for general office accommodation). The steps involved in establishing this site are not included in this Disaster Recovery Plan.