**Contents**

[**1. Overview 3**](#_Toc97299455)

[**2. Purpose 3**](#_Toc97299456)

[**3. Scope 3**](#_Toc97299457)

[**4. Process 3**](#_Toc97299458)

[**5. Responsibilities 3**](#_Toc97299459)

[**5.1 Service Continuity Manager 3**](#_Toc97299460)

[**5.2 Service continuity Recovery Team 3**](#_Toc97299461)

[**6. Planning 4**](#_Toc97299462)

[**7. Risk analysis 4**](#_Toc97299463)

[**8. Risk Treatment Plan 5**](#_Toc97299464)

[**9. Disaster incident management team 5**](#_Toc97299465)

[**9.1 Salvage team 6**](#_Toc97299466)

[**9.2 Recovery action team 6**](#_Toc97299467)

[**10. Disaster recovery team 6**](#_Toc97299468)

[**11. Backup storage and security 7**](#_Toc97299469)

[**11.1 Recovery on backup data 7**](#_Toc97299470)

[**12. Failure analysis 7**](#_Toc97299471)

**DOCUMENT REVISION CONTROL**

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Approval remarks** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 1. Overview

Service continuity entails contingency planning for recovery in the event of a major disaster or incident that disrupts or destroys ICT services. It also entails risk assessment and the adoption of actions to reduce the chances of such an occurrence occurring in the first place.

# 2. Purpose

The goal of IT service continuity management (ITSCM) is to assist the organization's overall business continuity management by guaranteeing that the IT service provider can offer the bare minimum of operations and service levels in the event of a disaster.

# 3. Scope

Human resources, facilities, equipment, systems, applications, data, networks, and support functions and processes are all included in the scope of ITSCM, as are all IT infrastructure components and resources (internal and external) that are required to restore minimum acceptable service levels in the event of a disaster.

# 4. Process

* Initiation- It entails establishing policies, defining scope and terms of reference, planning projects, and allocating resources.
* Requirement- It involves a risk assessment and a business impact analysis.
* Implementation- Executing risk reduction measures, recovery option preparations, testing, and strategies are all part of it.
* Ongoing operation- It comprises education and awareness, ITSCM plan change management, and continual testing.
* A Test Report summarizes the testing and assessment actions carried out as part of any ITSM process.

# 5. Responsibilities

## 5.1 Service Continuity Manager

The Service Continuity Manager oversees maintaining service continuity. This person is usually in charge of the entire process, from start to finish, including plan development, continuing monitoring and assessment, and disaster response plans.

## 5.2 Service continuity Recovery Team

This team oversees conducting tests and incident drills, as well as continuously upgrading ITSCM. Technical employees, QA professionals or users for testing, and representatives from other departments who are responsible for maintaining lines of communication open between ITSCM and their teams are usually on the team.

# 6. Planning

| **Incident** | **How to respond** | **Critical systems** | **Backup** |
| --- | --- | --- | --- |
| Systems getting hacked | Identify the breach and Mae detailed records | Software’s, storage servers | Backup data every week |
|  |  |  |  |
|  |  |  |  |

# 7. Risk analysis

All risks will be evaluated to determine the range of possible project outcomes. Qualification will be used to evaluate which risks should be pursued and responded to, as well as which risks can be ignored.

| **Internal Risks** | | | |
| --- | --- | --- | --- |
| **Risk** | **Probability** | **Severity** | **Actions to mitigate risk** |
| New change in management may hinder organization performance due to change in policies | **Moderate** | **Major** | The concern will be discussed beforehand |
|  |  |  |  |
| **External risks** | | | |
| Political rallies and protest may delay supply of raw materials | **Low** | **Major** | Country director will interact with the local authorities to discuss the situation. In case of protest, a contingency plan will be prepared to store the raw materials at a storage facility |
| Failure of payment from vendors or clients | **Major** | **Moderate** | An agreement will be signed beforehand to prevent breach |

# 8. Risk Treatment Plan

A risk treatment plan is a document that outlines the steps that will be taken to reduce or eliminate risks associated with a project.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk Treatment plan** | | | | | | |
| **Risk Treatment/Action Plan** | **Responsible** | **Deadline** | **Risk Rating** | **Review/ Monitor** | **Insurance Status** | **Measurement and monitoring** |
|  |  |  |  |  | **Insurable**  **Insured** |  |
|  |  |  |  |  |  |  |

# 9. Disaster incident management team

The Disaster Incident Management Team will oversee making crucial decisions about the disaster's management. The team will consist of:

* Deputy Director of Operations
* Head of Service for Disaster-Affected Services IT Security Officer (team coordinator)
* Customer Service Manager
* Others at the management team's discretion.

This team set goals and proclaim when the catastrophe recovery process is accomplished.

## 9.1 Salvage team

The Salvage Team will quickly assemble to execute ad-hoc operations to examine the recoverability of resources and facilities in the disaster area.

## 9.2 Recovery action team

The Recovery Action Team assumes that the disaster will last for some time and begins planning recovery activities in a safe place right away. The team will receive a full list of pre-approved activities to complete. This is especially important in the initial few hours after a calamity.

| **Service impacted** | **Impacted areas** | **Team members impacted** |
| --- | --- | --- |
| Record management | Storage rooms | Auditors, Record managers |
|  |  |  |
|  |  |  |

# 

# 10. Disaster recovery team

A disaster recovery team is essential for ensuring that your business recovers quickly from any type of disaster.

| **Name** | **Phone** | **Mail** | **Role** | **Responsibilities** |
| --- | --- | --- | --- | --- |
| Nick Mathers | xxxx | xxxx | IT security officer | Responsible for the collection, management, and distribution of the DR Policy. |
|  |  |  |  |  |
|  |  |  |  |  |

# 11. Backup storage and security

Backups must be protected with appropriate security measures, which include all essential physical security controls, such as those relating to the safety and security of the backup media themselves – specifically, discs, tapes, and any other medium carrying backup data. This necessitates the usage of a secure and constantly monitored computer room or other designated space (facility) where only authorized individuals have physical access to the backups. As a result, the terms “secured” and “monitored” imply that the facility has the following physical and environmental security procedures in place.

* Security alarms that are operational during non-business hours, with alarm notifications directly responded by a third-party security agency or a local police department.
* Appropriate fire detection and suppression elements, including fire extinguishers in mission-critical areas.
* Appropriate power protection systems to ensure a continuous, balanced load of power to the facility where the backups are located.

## 11.1 Recovery on backup data

If the data is encrypted, make provisions for key management. At the very least [quarterly], and at the very least [yearly], disaster recovery processes must be tested. The [IT Head & Information Security Head] must be notified of the results of the recovery testing.

# 12. Failure analysis

| **Objective** | **Failure** | **Reason** |
| --- | --- | --- |
| Increase production of Electric vehicles by 25% | Missed the target by 10% thereby increase production capacity by 15% | Rise in semiconductor prices due to low production |
|  |  |  |
| **Suggested solutions** | | **Risks** |
| Government to provide tax incentives to facilitate production activities and reduce price of semiconductors | | Policies may change in the next 2 years due to change in government |
|  | |  |