**Table of Contents**

[1. Introduction 3](#_Toc12451036)

[1.1 Purpose 3](#_Toc12451037)

[1.2 Scope 3](#_Toc12451038)

[1.3 Definitions and acronyms 3](#_Toc12451039)

[2. Recovery strategy 4](#_Toc12451040)

[3. Recovery objectives 4](#_Toc12451041)

[4. Recovery team 4](#_Toc12451042)

[5. Recovery team checklist 5](#_Toc12451043)

[6. Recovery procedures 6](#_Toc12451044)

[7. Supporting information 6](#_Toc12451045)

**Document Control**

**Document Version History**

This table shows a record of significant changes to the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approvals**

This table shows the approvals on this document for circulation, use and withdrawal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Title/Authority** | **Approval Remarks** |
| 1.0 |  |  |  |  |
| 1.1 |  |  |  |  |

# Introduction

[The introduction of the IT Service Continuity Plan (ITSCP) provides an overview of the entire ITSCP. It includes the purpose, scope, definitions, acronyms, references, and overview of the ITSCP.]

## Purpose

To support the overall Business Continuity Management (BCM) by ensuring that the required IT infrastructure and IT services risk are managed with minimum business agreed business continuity related levels.

## Scope

[Identify all IT services that are within the scope of the ITSCP.]

ITSCM focuses on those events that the businesses consider significant enough to be

treated as disaster. Less significant events are dealt with as a part of incident management process.

The ITSCM primarily covers the IT asset and facility supports the all business process activities.

## Definitions and acronyms

**BIA**: Business Impact Analysis is the activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include suppliers, people, other business processes, IT services etc.

**Disaster recovery invocation guideline**: A document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a Disaster.

**Fast recovery**: A recovery option that is also known as hot standby. Fast recovery normally uses a dedicated fixed facility with computer systems and software configured ready to run the IT services. Fast recovery typically takes up to 24 hours but may be quicker if there is no need to restore data from backups.

**Gradual recovery**: A recovery option that is also known as cold standby. Gradual recovery typically uses a portable or fixed facility that has environmental support and network cabling, but no computer systems. The hardware and software are installed as part of the IT service continuity plan. Gradual recovery typically takes more than three days, and may take significantly longer.

**Immediate recovery**: A recovery option that is also known as hot standby. Provision is made to recover the IT service with no significant loss of service to the customer. Immediate recovery typically uses mirroring, load balancing and split-site technologies.

**Reciprocal arrangement**: A recovery option. An agreement between two organizations to share resources in an emergency – for example, high speed printing facilities or computer room space.

**Recovery**: Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After recovery, further steps may be needed before the IT service can be made available to the users (restoration).

**Recovery plan**: Recovery Plans are created mainly by Availability and IT Service Continuity Management. The plans contain detailed instructions for returning specific services and/or systems to a working state, which often includes recovering data to a known consistent state.

**RPO**: Recovery Point Objective is the maximum amount of data that may be lost when service is restored after an interruption. The recovery point objective is expressed as a length of time before the failure. For example, a recovery point objective of one day may be supported by daily backups, and up to 24 hours of data may be lost. Recovery point objectives for each IT service should be negotiated, agreed and documented, and used as requirements for service design and IT service continuity plans.

**RTO**: Recovery Time Objective is the maximum time allowed for the recovery of an IT service following an interruption. The service level to be provided may be less than normal service level targets.

**Vital** **business function**: A Function of a Business Process which is critical to the success of the Business.

# Recovery strategy

[Identify the services, systems, infrastructure or facilities to be recovered by alternate services, systems, infrastructure, or facilities.

Identify how long recovery will take.

Identify the required recovery time for specific elements.

Identify when the recovery of specific services, systems, infrastructure, or facilities was last tested.]

# Recovery objectives

**RTO for Service A**: <<< Define the maximum time allowed for the recovery of an IT service following an interruption. >>>

**RPO for Service A** <<< Define the maximum amount of data that may be lost when service is restored after an interruption. >>>

# Recovery team

This section describes the other services, responsible person, dependencies and expected response time for recovering this service.

| **Service** | **Responsibility** | **Dependencies** | **Expected Response Time** |
| --- | --- | --- | --- |
| Service A | A | [Identify all service, system, infrastructure, or facility dependencies so that recovery plans can be invoked in the appropriate order.]  E.g.: Power supply | Duration in minutes or hours |
| Service B | B | [Identify all service, system, infrastructure, or facility dependencies so that recovery plans can be invoked in the appropriate order.]  E.g.: Network connectivity / DNS service | Duration in minutes or hours |
| Service C | C | [Identify all service, system, infrastructure, or facility dependencies so that recovery plans can be invoked in the appropriate order.]  Network connectivity and operational status of video infrastructure | Duration in minutes or hours |
| Service D | D | [Identify all service, system, infrastructure, or facility dependencies so that recovery plans can be invoked in the appropriate order.]  E.g.: Network connectivity and operational status of video infrastructure | Duration in minutes or hours |

# Recovery team checklist

<<< [Use the following checklist to indicate the execution of key activities. Add additional tasks as needed.] >>>

|  |  |  |
| --- | --- | --- |
| **Task** | **Target Completion Date** | **Actual Completion Date** |
| Confirm recovery invocation |  |  |
| Initiate disaster communication and assemble Recovery Team |  |  |
| Identify top issues and contact Crisis Management Team |  |  |
| Initiate transport of recovery media to recovery site |  |  |
| Identify status reporting procedures |  |  |
| Communicate reporting procedures to Recovery Team |  |  |
| Start recovery actions |  |  |

# Recovery procedures

<<< [List all recovery procedures to be followed. This may refer to documentation where such procedures are kept. >>>

# Supporting information

<<< [The supporting information makes the ITSCP easier to use. It includes:

* Index
* Appendices
* Supporting documents >>>