[Organization logo]

[Organization name]

IT SERVICE CONTINUITY MANAGEMENT PLAN

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Change history

Date	Version	Created by	Description of change
	0.1	20000Academy	Basic document template

Table of contents

1. Purpose, scope and users

The purpose of the IT Service Continuity Plan is to define precisely how [organization name] will recover or continue the operation of IT services, applications, systems or components to the agreed level based on business requirements.

This plan is applied to all critical activities inside the scope of the IT Service Continuity Management.

Users of this document are all staff members, both inside and outside the organization, who have a role in IT service continuity.

2. Reference documents

- ISO/IEC 20000-1:2018, clause 8.7.2.
- IT Service Continuity Management Process
- Service Level Management Process
- [Business Plan]

3. IT Service Continuity Plan

3.1 Plan content

This Plan is written based on the results of risk assessment and risk treatment, Business Impact Analysis results, and the [Business Plan].

Assessments and analyses are done together with the Business Continuity Management process and [job title] as the contact person on the business side.

3.2 IT Service Continuity organization and organizational change

If IT service continuity plans are activated, a working body called the IT Service Continuity Management Team is formed, which is authorized to make any decisions to resolve the situation. Members of the IT Service Continuity Management Team are:

Member Name, Last Name	Member's Responsibility

The IT Service Continuity Management Team is managed by the IT Service Continuity Manager. [Job title] will perform the function of IT Service Continuity Manager, and in the case of his/her absence, the function will be performed by [job title].

During the disaster recovery process, [IT Service Management organization name] changes its structure as follows:

Organizational unit name	Member name	Organizational unit name	Member name
[Executive group name]	*[First name, Last Name]*	Recovery Team A name	*[First name, Last Name]*
	[First name, Last Name]		*[First name, Last Name]*
[Coordination group name]	*[First name, Last Name]*	Recovery Team B name	*[First name, Last Name]*
	[First name, Last Name]		*[First name, Last Name]*

Commented [20A12]:

3.3 IT Service Continuity requirements

IT Service Continuity requirements are derived from:

- Risks and Opportunities Register
- Business Impact Analysis – see Business Impact Analysis and Recovery in Appendix
- Service Level Agreements and service requirements defined in the Business Impact Analysis and Recovery.

Commented [20A13]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "05_Risk_Management".

3.1.1 Risk assessment and risk treatment

Risk assessment assesses the level of a threat (i.e., disruptive incident) and the impact and probability of the associated risk. Risk assessment is implemented through the Risks and Opportunities Register. The risk assessment process is coordinated by the IT Service Continuity Manager, and risk assessment for individual services is conducted by service owners.

Commented [20A14]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "05_Risk_Management".

Commented [20A15]:

Commented [20A16]:

3.1.2 Business impact analysis

The IT Service Continuity Manager coordinates the process of business impact analysis. Business impact analysis is implemented according to the Business Impact Analysis table included in the Business Impact Analysis and Recovery.

Business impact analysis is performed after the risk assessment has finished, so that the information about required resources can be gathered during risk assessment.

The IT Service Continuity Manager is responsible to complete the Business Impact Analysis and Recovery document and keep it updated.

3.4 ITSCM Plan activation; plan deactivation

[job title] activates and deactivates the ITSCM Plan. Activation and deactivation of an ITSCM plan is coordinated with [job title].

Service recovery resources and actions are described in the Business Impact Analysis and Recovery document. When recovering a service, or several services, the IT Service Continuity Manager ensures that the following approach is taken:

- Services are recovered according to the recovery priority
- Needed resources are available
- Third parties are contacted and involved for the services which include third parties
- Minimum service functionality is established

Commented [20A17]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, etc.

Commented [20A18]:

- ~~Access is granted to those users with highest priority~~
- ~~Agreed service response time is achieved~~
- ~~Maximum service level is established~~

Recovery plans, as defined in the Risks and Opportunities Register for particular services, are activated exclusively by the decision of the IT Service Continuity Manager if he/she assesses that a ~~particular service will be interrupted for a period longer than the recovery time objective for that service defined in the Business Impact Analysis. The decision of the IT Service Continuity Manager may be written or verbal.~~

Independent from the service, the IT Service Continuity Manager needs to ensure that the following activities are undertaken:
- Backup media are available and data are retrieved
- Documentation, particularly ITSCM Plan, procedures and workstation images are stored at recovery site
- ~~Required personnel are mobilized and present at recovery site~~
- ~~All third-party organizations that have a role in recovery activities are contacted~~
- ~~List of all persons (both internal and external) involved in IT Service Continuity Management are available on recovery site~~
- ~~Configuration Management Database (CMDB) is available on recovery site when access to normal service locations is prevented~~

Recovery plans may be deactivated by the IT Service Continuity Manager for individual services when ~~they determine that all conditions for the resumption of business activities have been met. Recovery plans are deactivated by resuming normal business activities.~~

~~Changes to the plan are under the control of the Change Management Process. The IT Service Continuity Manager is responsible to raise a Request for Change (RFC) if changes to the plan are needed.~~

3.5 Major loss of service

In case of major loss of service, the following procedure is valid:

- ~~Incident Manager notifies IT Service Continuity Manager~~
- ~~IT Service Continuity Manager uses "Business Impact Analysis and Recovery" document, i.e. affected service's worksheet inside the document, and invokes IT Service Continuity plan by ensuring:~~

  - needed resources are available
  - defined actions are taken
  - access rights are granted to persons with highest priority
  - response time objectives are met

3.6 IT Service Continuity recovery options

~~Every continuity-related service has a defined recovery option. The following recovery options exist:~~

Recovery option	Recovery site

When there are more services that need to be recovered, the IT Service Continuity Manager defines

3.7   Communication

The following means will be used for communication between the IT Service Continuity Management

1. Mobile phones (business and private)
2. Telephones (business and private)
3.
4.
5.
6.
7.
8.

[Job title] in the IT Service Continuity Management Team is responsible for coordinating communication with all employees involved in the recovery activities.

4. Validity and document management

This document is valid as of [date].

Owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

This document is distributed by the IT Service Continuity Manager, in both paper and electronic form, to the following persons:

Name, Last name	E-mail	Office

Comments:

Commented [20A23]:

Commented [20A24]:

Commented [20A25]:

Commented [20A26]:

Commented [20A27]:

Commented [20A28]:

Commented [20A29]:

Commented [20A30]:

Commented [20A31]: You can adjust these according to your company practices.

Commented [20A32]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, etc.

Commented [20A33]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, etc.

Commented [20A34]: This is only a recommendation; you can adapt the frequency according to your company practices.

Commented [20A35]: Enter office address where paper form of the IT Service Continuity Plan should be delivered.

[organization name]

5. Appendices

- Appendix 2 – Business Impact Analysis and Recovery
- Appendix 3 – IT Service Continuity Plan, Test and Review Report

[Job title]
[Name]

_____
[Signature]

Commented [20A36]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.