# IT SERVICE CONTINUITY MANAGEMENT PLAN

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version:</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>

**Comment [BV1]:** All fields in this document marked by square brackets [] must be filled in.

**Comment [BV2]:** The document coding system should be in line with the organization’s existing system for document coding; in case such a system is not in place, this line may be deleted.
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Basic document template</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS ........................................................................................................... 3
2. REFERENCE DOCUMENTS ................................................................................................................ 3
3. IT SERVICE CONTINUITY PLAN ........................................................................................................ 3
   3.1 PLAN CONTENT .......................................................................................................................... 3
   3.2 IT SERVICE CONTINUITY ORGANIZATION AND ORGANIZATIONAL CHANGE ......................... 3
   3.3 IT SERVICE CONTINUITY REQUIREMENTS .................................................................................. 4
   3.4 ITSM PLAN ACTIVATION; PLAN DEACTIVATION ........................................................................ 5
   3.5 MAJOR LOSS OF SERVICE ........................................................................................................ 6
   3.6 IT SERVICE CONTINUITY RECOVERY OPTIONS ........................................................................ 6
   3.7 COMMUNICATION ..................................................................................................................... 6
   3.8 IT SERVICE CONTINUITY PLAN TESTS ..................................................................................... 7
4. VALIDITY AND DOCUMENT MANAGEMENT ..................................................................................... 7
5. APPENDICES ..................................................................................................................................... 7
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 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

- IT Service Continuity Management process
- Service Level Management process
- [Business plan]
- Communication Procedure

3. IT Service Continuity Plan

3.1 Plan content

This Plan is written based on results of risk assessment and risk treatment, Business Impact Analysis (see Business Impact Analysis and Recovery in Appendix) results and the Business Plan.

Assessments and analysis are done together with the Business Continuity Management process and [role description] 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 required to resolve the situation. Members of the IT Service Continuity Management Team are:

<table>
<thead>
<tr>
<th>Member Name, Last name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

The IT Service Continuity Management Team is managed by the IT Service Continuity Manager. [role description] 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].

Comment [BV3]: Delete if there is no Business plan.
Comment [BV4]: ***OPTION*** Delete this if you are implementing ITIL and not ISO 20000.
Comment [BV5]: ***OPTION*** Delete this if you are implementing ITIL and not ISO 20000.
Comment [BV6]: Delete if Business Plan does not exist.
Comment [BV7]: Reformulate this if there is no Business Continuity Management process in place. If that is the case, then do not use the clause.
Comment [BV8]: ***OPTION*** Delete this section if you are implementing ISO 20000 and not ITIL.
Comment [BV9]: This is usually a high level of authority.
During the disaster recovery process, [IT Service Management organization name] changes its structure as follows:

<table>
<thead>
<tr>
<th>Group name</th>
<th>First name, Last Name</th>
<th>Group name</th>
<th>First name, Last Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive group</td>
<td>[First name, Last Name]</td>
<td>Executive group</td>
<td>[First name, Last Name]</td>
</tr>
<tr>
<td>[First name, Last Name]</td>
<td>[First name, Last Name]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordination group</td>
<td>[First name, Last Name]</td>
<td>Coordination group</td>
<td>[First name, Last Name]</td>
</tr>
<tr>
<td>[First name, Last Name]</td>
<td>[First name, Last Name]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.3 IT Service Continuity requirements

IT Service Continuity requirements are derived from:
- Risk assessment and risk treatment – see Risk Assessment and Treatment in Appendix
- Business Impact Analysis and Recovery in Appendix
- Recovery in Appendix

3.3.1 Risk assessment and risk treatment

Risk assessment assesses the level of the threat (i.e. disruptive incident) and the extent to which impacts are likely to occur. It is conducted through the Risk Assessment and Treatment Table (see Risk Assessment and Treatment in Appendix). The risk assessment process is coordinated by [job title], and conducted by service owners.

The impacts are classified as follows:

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marginal impact</td>
<td>Duration of the disruptive incident causes negligible damage to the organization.</td>
</tr>
<tr>
<td>Low impact</td>
<td>Duration of the disruptive incident causes damage to the organization.</td>
</tr>
<tr>
<td>High impact</td>
<td>Duration of the disruptive incident causes huge damage to the organization.</td>
</tr>
<tr>
<td>Catastrophic impact</td>
<td>Duration of the disruptive incident causes severe damage to the organization, so that it will be of the organization, and will have to shut down its operations permanently.</td>
</tr>
</tbody>
</table>
3.3.2 Business impact analysis

Business impact analysis is implemented according to the Business Impact Analysis table (see Business Impact Analysis and Recovery in Appendix). Business impact analysis is performed after the risk assessment has finished, so that the information about required resources can be gathered during risk assessment.

3.4 ITSCM Plan activation; plan deactivation

[role description] activates and deactivates the ITSCM Plan. This plan is coordinated with [role description].

Service recovery and Business Impact Analysis and Recovery (see Business Impact Analysis and Recovery in Appendix) document. When recovering a service, or several services, [role description] ensures that the following approach is taken:
- Services are recovered according to the recovery priority
- Relevant resources are available
- Third parties are contacted and involved for the services which include third parties
- Minimum service functionality is established
- Access is granted to those users with highest priority
- Agreed service response time is achieved
- Maximum service level is established

Recovery plans (see Appendix 3) for particular services are activated exclusively by the decision of [role description]. If he/she assesses that a particular service will be interrupted for a period longer than the recovery objective for that service, the decision of [role description] may be written or oral.

Independent from the service, [role description] needs to ensure that the following activities are undertaken:
- Backup media are available and data are retrieved
- Documentation, particularly the IT Service Continuity Plan, procedures and workstation images are stored on recovery site
- Relevant persons involved and present on recovery site
- All third-party agreements (including service level agreements and disaster recovery plans) are contacted
- A list of all persons (both internal and external) involved in IT Service Continuity Management are available on recovery site
- The Configuration Management Database (CMDB) is available on recovery site

Recovery plans may be deactivated by [role description] 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. [role description] is responsible to raise a Request for Change (see Change Record and Request for Change in Appendix of Change Management) if changes to the plan are needed.
3.5 **Major loss of service**

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

- [role description] notifies IT Service Continuity Manager
- IT Service Continuity Manager uses "Business Impact Analysis and Recovery" document, i.e. the affected service's worksheet inside the document, and modifies the IT Service Continuity plan by:
  - ensuring that needed resources are available
  - ensuring that defined actions are taken
  - granting access rights to persons with highest priority
  - ensuring response time objectives are met

3.6 **IT Service Continuity recovery options**

Every continuity-related service has a defined recovery option (see Business Impact Analysis and Recovery in Appendix). The following recovery possibilities exist:

<table>
<thead>
<tr>
<th>Recovery option</th>
<th>Recovery site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual workarounds</td>
<td></td>
</tr>
<tr>
<td>Gradual recovery</td>
<td></td>
</tr>
<tr>
<td>Fast recovery</td>
<td></td>
</tr>
</tbody>
</table>

When there are more services that need to be recovered, [role description] defines priority of invocation. Business Impact Analysis and Recovery (see Business Impact Analysis and Recovery in Appendix) contains a list of services and their respective priorities. Recovery priorities are defined on a scale of 1-5; 1 is the highest priority.

3.7 **Communication**

The following means will be used for communication between the IT Service Continuity Management Team and persons involved in recovery activities, and between recovery activities themselves (the first one from the list is to be used first; in case it is not available, the next one is used):

1. mobile phones (business and private)
2. telephones (business and private)
3. e-mail sent from business or private computers
4. messaging services – e.g. Skype
5. couriers (employees of the organization or specialized services)
6. [another service where they are stored and who has the right to use them]
7. [another service where they are stored and who has the right to use them]
8. [satellite phones – state where they are stored and who has a right to use them]
3.8 IT Service Continuity Plan tests

[role description] is responsible for ensuring that the IT Service Continuity plan is tested and reviewed (see IT Service Continuity Plan Test and Review Report in Appendix) as follows:

- Once a year for services with defined recovery priority
- Every two years for services with defined priority 3 and 4
- Every three years for services with defined priority 5
- After major changes

[role description] reviews the IT Service Continuity Plan after the Plan is

4. Validity and document management

This document is valid as of [date].

Owner of this document is [job title], who must at least [frequency] once a year.

This document is distributed by [role description], in both paper and electronic forms, to the following persons:

<table>
<thead>
<tr>
<th>Name, Last name</th>
<th>E-mail</th>
<th>Office</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Appendices

- Appendix 2: Business Impact Analysis and Recovery
- Appendix 3: Risk Assessment and Treatment
- Appendix 4: IT Service Continuity Plan Test and Review Report

[job title]

[name]