IT SERVICE CONTINUITY AND AVAILABILITY MANAGEMENT PROCESS

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

©2013 This template may be used by clients of EPPS Ltd. www.20000academy.com in accordance with the License Agreement.
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. POLICY ................................................................................................. 3
   3.1. AVAILABILITY .................................................................................. 3
4. PROCESS .................................................................................................. 4
   4.1. INITIATION ..................................................................................... 4
   4.2. REQUIREMENTS AND STRATEGY ........................................................ 4
   4.3. ONGOING OPERATION ....................................................................... 4
   4.4. INVOCATION ................................................................................... 5
   4.5. SERVICE CONTINUITY AND AVAILABILITY MONITORING AND TESTING .. 5
5. ROLES AND RESPONSIBILITIES ............................................................... 5
   5.1. IT SERVICE CONTINUITY MANAGER .................................................. 5
   5.2. AVAILABILITY MANAGER ................................................................. 5
6. MEASUREMENT AND METRICS .................................................................. 6
   6.1. MEASUREMENT ............................................................................... 6
   6.2. METRICS ......................................................................................... 6
   6.3. CRITICAL SUCCESS FACTORS (CSF) AND KEY PERFORMANCE INDICATORS (KPI) ................................................................. 7
7. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT .............. 7
8. VALIDITY AND DOCUMENT MANAGEMENT .............................................. 7
9. APPENDICES ............................................................................................ 8
1. **Purpose, scope and users**

The aim of this document is to define the purpose, scope, principles and activities of the IT Service Continuity and Availability Management process.

This document is applied to the entire SMS.

Users of this document are all employees of [organization name], as well as all external parties who have a role in the SMS.

2. **Reference documents**

- Information Security Management Process
- Service Level Management Process
- Supplier Management Process
- Business Relationship Management Process
- Change Management Process
- ISO/IEC 20000-1:2011, clause 6.3

3. **Policy**

ITSCM supports [organization name]'s Business Continuity and Availability Management, in such a way that it provides at least a minimum service level to business services.

>[role description] is responsible for ensuring that the following goals are achieved:

- IT Service Continuity Management Plan (ITSCM) is produced, implemented and maintained; see ITSCM Plan in Appendix
- Availability Plan is produced, implemented and maintained; see Availability Plan in Appendix
- Business Impact Analysis (BIA) is performed
- Risk assessment is conducted
- IT Service Continuity and Availability requirements and goals form an integral part of contracts with suppliers and customers (i.e. Service Level Agreement)
- Business Continuity plan and targets are assessed and IT Service Continuity and Availability agreements are reviewed as part of reviews and audits
- Provides guidance for all other processes on all availability-related issues.
- Manages service- and resources-related availability with the goal that service availability achievements meet set targets
- Assists in diagnosis of all availability-related incidents, and problems
- Ensures that proactive availability management is performed and respective measures defined

3.1. **Availability**
Availability of the service is calculated as follows:

\[ \text{Availability (\%) = } \frac{\text{Agreed Service Time (AST) - downtime}}{\text{AST}} \times 100 \]

4. Process

4.1. Initiation

[role description] is responsible to define the following:

- Scope of the IT Service Continuity and Availability Management process
- Management of organization’s site
- Requirements regarding the compliance to following standards and regulations: [ISO 27001]
- Process structure which will establish IT Service Continuity and Availability Management process and structure

4.2. Requirements and strategy

[role description] is responsible to identify and agree on, with customer and interested parties, IT Service Continuity and Availability requirements based on:

- Risk assessment (see BIA Assessment and treatment in Appendix) – risk assessment and risk management regarding continuance and availability of services
- Business Impact Analysis (BIA) (see BIA and Recovery in Appendix)
- Service Level Agreements (SLA) and service requirements – SLA requirements and any
  requirements of the services in scope of ITSCM.
  requirements in Appendix of Service Level Agreement Process
  see Service Level Agreement and Service Level Requirements in Appendix of Service Level Agreement Process

BIA, risk assessment and SLA requirements are an integral part of the ITSCM Plan (see ITSCM Plan in Appendix).

4.3. Ongoing operation

[role description] is responsible for ensuring that the following activities are performed:

- Review and audit – ensures that the ITSCM Plan and Availability Plan are maintained, i.e. up to date, and performs an audit [once a year] of the ITSCM Plan and Availability Plan to ensure that the plans are accurate.
- The IT Service Continuity and Availability Manager is part of the Change Advisory Board.
- Change Management – analyzes all normal changes, evaluates their impact on the ITSCM Plan and documents any changes in the Change Plan. (see Request for Change and Authority name inside your organization.)
4.4. Invocation

[role description] issues the invocation of the plan (see Business Impact Analysis and Recovery in Appendix) is clear to all persons involved in ITSCM.

4.5. Service continuity and availability monitoring and testing

[role description] is responsible for ensuring that:

- Availability of the service is monitored, the results recorded and compared with agreed targets; see Availability Measurement Report in Appendix
- Unplanned non-availability is investigated and necessary actions are taken
- Availability Plan is tested against the availability requirements; see BIA (requirements) and Recovery and Availability Measurement Report (results) in Appendices
- ITSCM plan is tested against the service continuity requirements; see IT Service Continuity Plan Test and Review Report (results) and BIA and Recovery (requirements) in Appendices
- ITSCM Plan and Availability Plan are re-tested after major changes
- Continual review and improvement of Service Continuity Plan (see Service Improvement Plan in Appendix of Continual Service Improvement Process) when deficiencies are found, in:
  - ITSCM and Availability Plan test results
  - Invocation of ITSCM Plan

5. Roles and responsibilities

5.1. IT Service Continuity Manager

[role description] assigns the IT Service Continuity Manager role.

Responsibilities of IT Service Continuity Manager:

- Overall responsibility for carrying out activities within the scope of ITSCM
- Coordinates with other Service Management roles
- Responsible for reporting and managing information
- Manages work of Service Continuity Management staff
- Develops and maintains ITSCM management process and procedures
- Performs risk assessment
- Ensures that ITSCM plans and activities are in line with BCM
- Performs risk management
- Attends Change Advisory Board (CAB) meetings if needed
- Performs quality review of all procedures

5.2. Availability Manager

[role description] assigns the Availability Manager role.
Responsibilities of Availability Manager:

- Overall responsibility for carrying out activities within the scope of Availability Management
- Coordinates with other Service Management roles
- Plans and manages tool requirements needed to support Availability Management process
- Responsible for reporting and managing information
- Works closely with the Availability Management staff
- Develops, maintains and improves Availability Management process and procedures
- Ensures that newly developed or changed services deliver availability as required, taking into consideration that a minimum level of availability is implemented
- Takes part in investigation and diagnosis of incidents and problems regarding
- Takes part in IT infrastructure design, specifying availability requirements of hardware and software components
- Specifies the reliability, maintainability and serviceability requirements for components supplied by the supplier and external suppliers
- Monitors actual achievements against agreed achievements of IT services and components with regard to availability parameters
- Attends Change Advisory Board/CAB meetings when appropriate

6. Measurement and metrics

6.1 Measurement

[role description] is responsible to produce reports.

Reports are sent to the Service Level Manager on a monthly basis.

[role description] is responsible for ensuring that:

- reports are produced monthly, with quarterly and yearly summaries
- reports are evaluated
- measures for improvement are defined

6.2 Metrics

Metrics reports are produced monthly, with quarterly and yearly summaries. Metrics to be reported:

- Number of invocations started
- Number of successful/unsuccessful test results
- Service performance as defined in Availability Measurement Plan (see Availability Measurement Plan in Appendix) measured through: Availability, Reliability, Maintainability and Serviceability
- Number of downtimes
6.3. Critical Success Factors (CSF) and Key Performance Indicators (KPI)

[role description] is responsible to define CSFs and respective KPIs. Achievements against KPIs are monitored and evaluated by [role description].

<table>
<thead>
<tr>
<th>Critical Success Factor</th>
<th>Key Performance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invocation plan is efficient.</td>
<td>Reduction in number of failures during invocation plan initiation</td>
</tr>
<tr>
<td>Availability of components, IT infrastructure and services provided at minimum costs.</td>
<td>Reduction in service unavailability (as a percentage)</td>
</tr>
<tr>
<td>Manage availability and reliability of IT service</td>
<td>Improvement in MTBF, MTBSI, MTRS</td>
</tr>
<tr>
<td></td>
<td>Reduction in failure of third-party performance, MTRS (as a percentage)</td>
</tr>
<tr>
<td></td>
<td>Reduction in system unavailability (as a percentage)</td>
</tr>
</tbody>
</table>

Comment [BV16]: This is an example of CSFs and KPIs. Each organization must develop its own CSFs and KPIs depending on organization maturity and environmental circumstances. Achievements against KPIs must be monitored and used in other processes and as a basis for improvement.

7. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Service Continuity Plan</td>
<td>[tool name or network folder]</td>
<td>[job title]</td>
<td>This record is changed through the Change Management process by Change Authority.</td>
<td>IT Service Continuity Plan is updated. Old versions are archived.</td>
</tr>
<tr>
<td>Availability Reports</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Availability Manager</td>
<td>Reports are kept for [...].</td>
</tr>
<tr>
<td>Availability Measurement</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Availability Manager</td>
<td>Reports are kept for [...].</td>
</tr>
</tbody>
</table>

Comment [BV17]: Overall responsibility for ITSCM. Usually IT Service Continuity Manager.

Comment [BV18]: Change if needed.

Comment [BV19]: Usually Availability Manager

Comment [BV20]: Change if needed.

Comment [BV21]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

Comment [BV22]: Usually Availability Manager

Comment [BV23]: Change if needed.

Comment [BV24]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

Comment [BV25]: This is only a recommendation; adjust frequency as appropriate.

8. Validity and document management

This document is valid as of [date].

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

- Appendix 1: ITSCM Plan
- Appendix 2: BIA and Recovery
- Appendix 3: Risk Assessment and Treatment
- Appendix 4: IT Service Continuity Plan Test and Review Report
- Appendix 5: Availability Measurement Report
- Appendix 6: Availability Plan

[signature]

Comment [EV26]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.