Government of Malta

Reference: GMICT X 0120
Version: 1.0
Publication: 24 June 2016
Effective: 24 June 2016

Business Continuity Framework

This document is part of the GMICT Policy Framework
http://ictpolicies.gov.mt
Underlined terms are defined in the Vocabulary.

Purpose

To:

- protect against
- reduce the likelihood of occurrence of
- prepare for instances of
- respond to
- recover from

incidents that have the potential to exceed the Maximum Tolerable Period of Disruption (MTPD) of Critical ICT Services within the Public Sector.

It is based upon prevailing best practices in the field of Business Continuity, namely:


Scope and Applicability

The scope of this framework includes the articulation and subsequent testing of Business Continuity Plans for Critical ICT Services within the Public Sector.
## Table of Contents

- Purpose ................................................................................................. 1  
- Scope and Applicability ........................................................................ 1  
- Table of Contents .................................................................................. 2  
  1. Roles and Responsibilities ................................................................. 3  
  2. Approach to Develop & Manage Business Continuity Plans ............... 5  
    2.1 Identification of Critical ICT Services and Critical Assets ............... 5  
    2.2 Selection of Controls ....................................................................... 6  
    2.3 Implementation and Management of Business Continuity Plans ....... 7  
- References .............................................................................................. 9  
- Appendix A – List of Shared Critical ICT Services .................................. 10  
- Modification History ............................................................................... 11  
- Issuing Authority ................................................................................... 11  
- Contact Information ............................................................................... 11
1. Roles and Responsibilities

The Agent is responsible for:

1. Articulating and testing Business Continuity Plans for Shared Critical ICT Services provided by the Agent to the Public Sector
2. Providing assistance to the Public Sector on what should be included in Business Continuity Plans articulated for Line of Business Critical ICT Services and ensuring that they are not in conflict with other plans compiled for Shared Critical ICT Services
3. Coordinating Business Continuity testing for Line of Business Critical ICT Services used by more than one Ministry / Public Sector Entity
4. Implementing Business Continuity solutions (identified by the Agent) to manage Critical Assets identified within the Public Sector
5. Establishing an effective working relationship with the Critical Infrastructure Protection Unit (CIP).

A designated function within respective Ministries / Public Sector Entities shall be responsible for the articulation, endorsement and implementation of Business Continuity requirements relating to Line of Business Critical ICT Services that the Ministry / Public Sector Entity is responsible for. Nevertheless, the Agent shall provide the required direction and assistance to ensure that:

1. the relevant degree of consistency is in place with respect to the way that these requirements are catered for
2. relevant stakeholders (including but not limited to suppliers) are appropriately involved throughout the process.

The designated Data Protection Officer within the Ministry / Public Service Entity shall be properly and in a timely manner involved in all issues which relate to the protection of personal data, making sure adequate procedures are implemented to ensure compliance with all relevant Data Protection legislation.

The Agent’s Business Continuity function is responsible for:

1. Documenting and communicating the approach adopted for the implementation of Business Continuity
2. Aligning the the Agent’s implementation of Business Continuity with the requirements of the relevant international standard – ISO22301
3. Governing the identification of those ICT services provided by the Agent that are considered as critical through a structured business impact analysis
4. Establishing through the Agent’s respective service owners the dependencies and the components making up each Shared Critical ICT Service
5. Directing the Agent’s respective service owners to ensure that risks pertinent to the Shared Critical ICT Services are identified and managed in line with the established Enterprise Risk Management process
6. Directing the Agent’s respective service owners to ensure that the Disaster Recovery Plans for the Agent’s Shared Critical ICT Services are compiled (using the Disaster Recovery Procedure Template that accompanies this Framework) and tested to verify their accuracy
7. Articulating a Business Continuity Plan (in line with the Business Continuity Plan Template that accompanies this Framework) for the Shared Critical ICT Services provided by the Agent
8. Planning and coordinating, through the respective service owners, disaster recovery and/or business continuity tests that involve and/or span multiple Shared Critical ICT Services

Security Marking: Unclassified: Public
Services provided by the Agent. During these exercises, the Business Continuity function shall:

- Ensure that the exercise activities remain focused on the agreed agenda
- Provide participants with the necessary information prior to the commencement of the exercise
- Provide exercise oversight, including supervising the exercise, monitoring the sequence of events and controlling the timeline
- Control and manage all activities during the exercise but not provide solutions during the discussion
- Conduct debrief or feedback sessions with participants following the exercise
- Instigate decisions in case of unforeseen circumstances during the exercise
- Lead the analysis of exercise information and assisting in the preparation of the post-exercise report to capture key lessons learned.

The owners of the Agent’s Shared Critical ICT Services are responsible for:

1. Keeping respective critical infrastructure diagrams up to date
2. Articulating respective Disaster Recovery Plans
3. Verifying, through periodic tests, that these plans are sound and provide the following information to the Business Continuity function following each test carried out:
   - Date and time of test
   - Objectives of test
   - Description of the major events that took place during the test
   - Test results
   - Any deviations from the documented procedure
   - Recommended actions for consideration
2. Approach to Develop & Manage Business Continuity Plans

The approach adopted in the development and management of Business Continuity Plans consists of the following three phases:

1. Identification of Critical ICT Services and Critical Assets
2. Selection of Controls
3. Implementation and Management of Business Continuity Plans

2.1 Identification of Critical ICT Services and Critical Assets

An initial baseline is being adopted to establish an index of criticality for a number of shared ICT Services provided by the Agent to the Public Sector. Public Sector Entities may (but are not constrained to) consider this same model when establishing the criticality of their Line of Business Critical ICT Services.

1. The list of services provided by the Agent to the Public Sector and that are to be evaluated through this model was identified. It should be noted that this list was not considered exclusive and is subject to revision.
2. The following are the critical dimensions being used to influence the service criticality index:

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Life Threatening</td>
<td>A service whose failure or malfunction may result in the death or serious injury to people.</td>
</tr>
<tr>
<td>b. Affects National Security Profile</td>
<td>A service whose failure may impact the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline.</td>
</tr>
<tr>
<td>c. Politically Sensitive</td>
<td>A service whose unavailability may have an impact on the political posture, correctness and credibility in a national, EU and international context.</td>
</tr>
<tr>
<td>d. Affects EU Context or Profile</td>
<td>A service whose unavailability may have an impact on Pan-European relationships, obligations and position.</td>
</tr>
<tr>
<td>e. Has Strong Social Impact or Reach</td>
<td>A service whose unavailability may impact the wider citizen community.</td>
</tr>
<tr>
<td>f. Mission Critical</td>
<td>A service whose unavailability may lead to the inability to provide core business and enabling operations.</td>
</tr>
<tr>
<td>g. Increases Regulatory Compliance Risk</td>
<td>A service whose unavailability may lead to situations which inhibit the ability to meet legal, contractual and/or certification obligations.</td>
</tr>
<tr>
<td>h. Increases Financial Risk</td>
<td>A service whose unavailability may lead to situations which introduce additional financial obligations and/or limit revenue generation.</td>
</tr>
</tbody>
</table>
i. Affects Scope of Service

A service whose unavailability may lead to widespread impact.

3. The following table shows criticality values allocated to each of these dimensions. Depending on the dimensions relevant to the service, a value may be assigned to each ICT Service.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life Threatening</td>
<td>256</td>
</tr>
<tr>
<td>Affects National Security Profile</td>
<td>128</td>
</tr>
<tr>
<td>Politically Sensitive</td>
<td>64</td>
</tr>
<tr>
<td>Affects EU Context or Profile</td>
<td>32</td>
</tr>
<tr>
<td>Has Strong Social Impact or Reach</td>
<td>16</td>
</tr>
<tr>
<td>Mission Critical</td>
<td>8</td>
</tr>
<tr>
<td>Increases Regulatory Compliance Risk</td>
<td>4</td>
</tr>
<tr>
<td>Increases Financial Risk</td>
<td>2</td>
</tr>
<tr>
<td>Affects Scope of Service</td>
<td>1</td>
</tr>
</tbody>
</table>

4. The Agent currently only regards as critical those ICT Services whose criticality index is greater than or equal to an established baseline. The outcome of this exercise is endorsed by the Agent’s Service Management Committee and is included in Appendix A. It shall be revised annually to ensure it remains current. Respective service owners may recommend changes to this list of Shared Critical ICT Services. The final decision rests with the Agent’s Service Management Committee and is based on the outcome of the Business Impact Analysis carried out by the Agent’s Business Continuity function.

The Maximum Tolerable Period of Disruption (MTPD) for each Critical ICT Service is then determined followed by the identification of the dependencies that the Critical ICT Services have on the supporting assets used for their provision. This helps the Ministry/Entity focus its respective Business Continuity efforts on the Critical Assets that it relies on.

The next step is the identification of the Recovery Time Objective and Recovery Point Objective for each Critical Asset.

2.2 Selection of Controls

During this phase, risks that may exist within the infrastructure that supports the provision of Critical ICT Services are identified. This enables the subsequent identification and documentation of appropriate controls (along with the rationale for selecting each control) to mitigate these risks.

Examples include controls that:

1. Require staff members to understand their security roles and responsibilities such as security awareness, training and periodic reminders provided to staff members.
2. Enforce documented and monitored procedures for protecting the Ministry/Entity’s information when working with external organisations (eg: suppliers, subcontractors)

3. Require that all systems that provide Critical ICT Services are up to date with respect to patches and recommendations in security advisories

4. Require that there is a documented backup procedure and backup plan that are routinely updated and periodically tested.

2.3 Implementation and Management of Business Continuity Plans

The prioritisation for implementing the selected controls is derived from the recovery priority of the identified Critical Assets. As a matter of principle however, the implementation of controls protecting the facilities of respective Ministry/Entities shall be assigned a high priority, irrespective of the assigned recovery priority. This is because the corresponding controls for facilities involve the physical and environmental protection that consequently protects personnel’s health and safety.

Relevant Business Continuity Plans are then compiled and shall collectively contain:

1. Defined roles and responsibilities of people and teams having authority during and following an incident
2. A process for activating the response
3. Details to manage the immediate consequences of potential scenarios that may lead to a disruptive incident
4. Details on how and under what circumstances the Ministry/Entity will communicate with employees, key interested parties, emergency contacts and the media
5. How the Ministry/Entity will continue or recover its prioritised Critical ICT Services within predetermined timeframes for each identified scenario
6. How to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident.

Once the plans are agreed, they are communicated to the Ministry/Entity’s personnel. This allows the opportunity for any flaws in the plans to be exposed and ensures that all the roles and responsibilities are understood.

The Business Continuity Plans are regularly tested to ensure that they are consistent with the intended objectives. Exercises and tests are based on appropriate scenarios that are well planned with clearly defined aims and objectives and produce formalised post-exercise reports that contain outcomes, recommendations and actions to implement improvements. These tests are conducted at planned intervals and when there are significant changes within the Ministry/Entity or to the environment in which it operates.

Business Continuity Plans are evaluated at least annually or when significant changes occur in order to ensure their continuing suitability, adequacy and effectiveness.
The following figure provides an overview of this approach:

1. Identification of Critical ICT Services
2. Identification of MTPD (Maximum Tolerable Period of Disruption)
3. Identification of Critical Asset List
4. Identification of RTO & RPO (Recovery Time Objective & Recovery Point Objective)
5. Identification of Single Points of Failure & risks to Critical Assets
6. Identification of controls to mitigate these risks
7. Selection & prioritization of controls to be implemented
8. Articulation of Business Continuity Plans
9. Implementation of selected controls
10. Communication of Business Continuity Plans
11. Testing of Business Continuity Plans
12. Annual evaluation of Business Continuity Plans
References

3. Asset Value, Threat/Hazard, Vulnerability and Risk
4. A Risk Based Modeling of Interdependencies in Critical Infrastructures through UML
5. A Reference Model for Profiling Critical Infrastructure Systems
### Appendix A – List of Shared Critical ICT Services

The following is the list of Shared Critical ICT Services identified by the Agent:

<table>
<thead>
<tr>
<th>Email Service</th>
<th>Internet Service</th>
<th>Web Hosting Service</th>
<th>File Sharing Service</th>
<th>NIDMS (Integration Layer &amp; Qualified CA)</th>
<th>ECMS (Enterprise Collaboration Management System)</th>
<th>eID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Virtual Hosting

Active Directory, DNS & DHCP

Wide Area Network
(Core Network, GOVNET II & MAGNET II)

MITA Data Centre Facilities
Modification History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td>Initial publication</td>
</tr>
</tbody>
</table>

Issuing Authority

This document has been issued with the authority of the Malta Information Technology Agency.

Contact Information


Any suggestions, queries or requests for clarification regarding Government ICT Policies, Directives and Standards may be forwarded to ictpolicies@gov.mt.