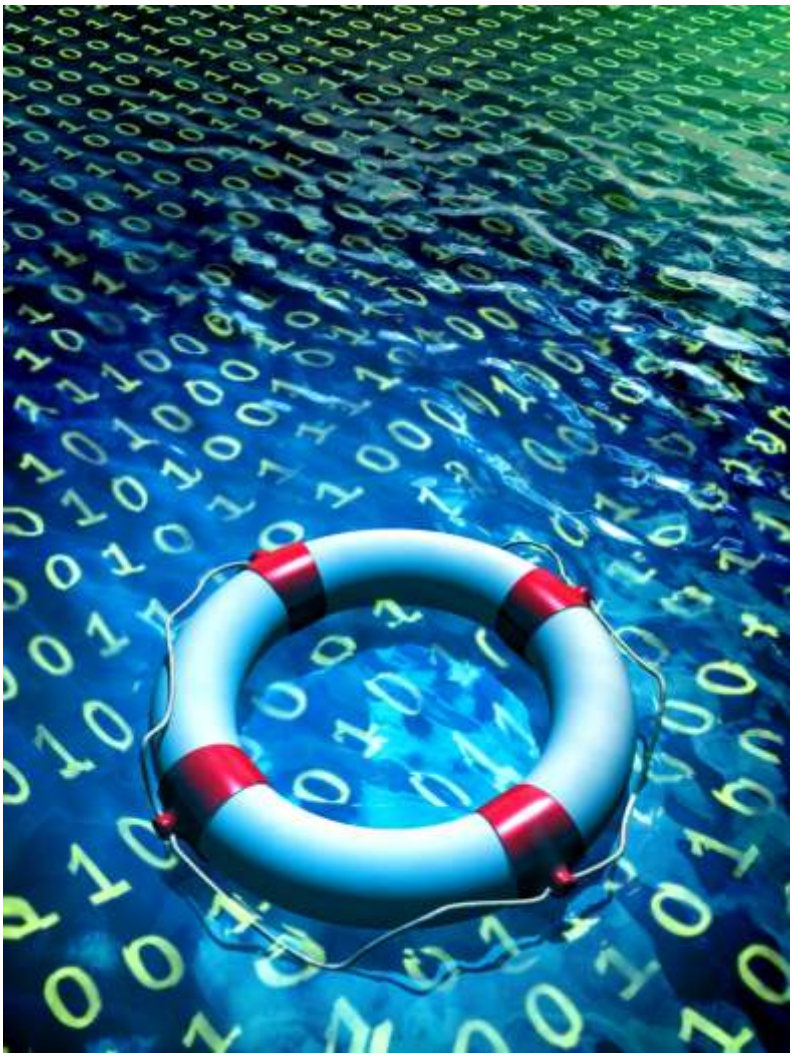

## About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

## Contact details:

For contacting ENISA or for general enquiries on BCP for SMEs, please use the following details:

e-mail: Dr. L. Marinos, Senior Expert — louis.marinos@enisa.europa.eu

Charalambos Koutsouris, Seconded National Expert, charalampos.koutsouris@enisa.europa.eu

Internet: http://www.enisa.europa.eu/



Document Revision: 1.0

## Contents

# Annex G – Useful Templates

This section of the report presents the necessary templates which the Assessment Teams should use in order to execute the proposed Business Continuity Management approach. For each template the Name and description of the template is provided as well the phase(s) and step(s) where the template is used / reused.

## Risk Profile Evaluation Table – Phase 1, Step 1

| Risk Areas | High | Medium | Low |
|---|---|---|---|
| **Legal and Regulatory** | The organization handles sensitive/personal customer information as defined by the EU Data Protection Law.<br>Retention of the aforementioned data is mandatory by Government Regulations. Loss and / or destruction of this data will lead to significant legal fines from Regulatory Bodies.<br>Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings will result in non-frivolous lawsuits. | The organization handles personal customer information as defined by the EU Data Protection Law.<br>Loss and / or destruction of the aforementioned data will lead to legal fines from Regulatory Bodies.<br>Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings may result in non-frivolous lawsuits. | The organization does not handle personal data of individuals other than those employed by the organization.<br>Retention of the aforementioned data is not mandatory by Government Regulations. Loss and / or destruction of the data will not lead to legal fines from Regulatory Bodies.<br>Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings may result in frivolous lawsuits. |
| **Productivity** | Services and operational processes are highly dependent on information systems, applications and third party services.<br>Interruptions to the provisioning of these services or to operational processes will generate intolerable direct or indirect impact to productivity. Significant expenses and effort are required to resume business and recover from market loss.<br>Provision of these services with manual procedures at the agreed quality is not possible. | Services and operational processes are highly dependent on information systems, applications and third party services.<br>Interruptions to the provisioning of these services or to operational processes have severe impact. However the organization can continue operations by switching to backup (e.g. manual) procedures for a limited period of time without significantly affecting its productivity. | Services and operational processes are not directly dependent on information systems, applications and third party services.<br>Interruptions to the provisioning of these services or to operational processes is tolerable since the organization is performing most critical operations with other means (e.g. manually) or can continue operations by switching to manual procedures for a period of time without affecting its productivity. |
| **Financial Stability** | Unavailability of products and services of less than one day lead to a major one time financial loss and cannot be tolerated.<br>Yearly revenues are directly related to the continuous and uninterrupted provision of on-line services (i.e. sales are performed online). | Unavailability of products and services of less than one day lead to a significant one time financial loss.<br>Yearly revenues are indirectly related to the continuous and uninterrupted provision of online services (i.e. products and Services are supported with on-line | Unavailability of products and services of less than one day lead to no or marginal one time financial loss.<br>Yearly revenues are not directly or indirectly related to the continuous and uninterrupted provision of on-line services.<br>Unavailability of online presence |

| | | | |
|---|---|---|---|
| | Unavailability of online presence will lead to direct financial loss as major services are provided by using e-business applications.<br>Fines that may incur due to non-compliance with legal and regulatory requirements may lead to intolerable financial loss. | services).<br>Unavailability of online presence will not lead to direct financial loss as services provided on-line can be provided by using alternative means (e.g. semi-automated, manually, etc.).<br>Fines that may incur due to non-compliance with legal and regulatory requirements are possible but will not affect financial stability. | will not lead to direct or indirect financial loss as services provided online can be provided by using alternative means (e.g. semi-automated, manually, etc.).<br>No or marginal fines will incur due to non-compliance with legal and regulatory requirements. If any, they cannot affect financial stability. |
| **Reputation and Loss of Customer Confidence** | Unavailability of service has direct impact on reputation, resulting thus in significant loss of customers using products and services though automated interfaces. | Unavailability of service has direct impact on reputation, resulting thus in considerable loss of customers using products and services though automated interfaces. | Unavailability of service cannot have impact on reputation, remaining thus unnoticed or marginally noticed by customers. |

**Table 1: Risk Profile Evaluation Table**

## Risk Profile Selection Table – Phase 1, Step 2 – Phase 3, Step 1

The risk profile selection table is the output the organizational risk determined by the Assessment Team during step 1 illustrating the identified risk levels in the predefined risk areas; **the highest risk identified in a risk class defines the overall business risk profile.**

| Risk Profile Selection Table | | |
|---|---|---|
| **Risk Areas** | **Risk Level** | **Risk Profile** |
| Legal and Regulatory | | |
| Productivity | | |
| Financial Stability | | |
| Reputation and Loss of Customer Confidence | | |

**Table 2: Risk Profile Selection**

## Critical Business Function Profile Card – Phase 2, Step 1

| Critical Business Function Profile Card | | | |
|---|---|---|---|
| Critical Business Function | | Recovery Priority | |
| Who controls the function | | | |
| Who is responsible for delivering the function? | | | |
| Who is the user? (Who benefits / needs this function? / why is it critical?) | | | |
| How is it used? | | | |

**Table 3: Detailsof the critical Business Function "Finance"**

## Critical Business Function Table – Business Continuity Scope – Phase 2, Step 1

The Assessment Team compiles a table listing the corporate critical business functions along with the rationale for selection and the recovery priority of each business function.

| Critical Business Function – Business Continuity Scope | | |
|---|---|---|
| Critical Business Function | Rationale for Selection | Recovery Priority (High, Medium, Low) |
| Production | | |
| Customer Relationship | | |
| Human Resource | | |
| Finance | | |
| New Product Acquisition / Development. | | |

**Table 4: Critical Business Functions of example organisation**

## Business Function Supporting IT Assets – Phase 2, Step 2

The Assessment Team selects the asset types, which are used to provide the selected critical business function(s) to the organization's employees identified during phase 2, step 1. The Assessment Team ends up with a matrix -for each identified critical business function- identifying the supporting assets used to provide the organization's business function(s).

| Critical Business Function Supporting IT Assets | |
|---|---|
| Critical Business Function Name | |
| Supporting Assets | |
| Hardware | |
| Network | |
| Back Office Application | |
| Client Facing Applications | |
| People | |
| Data | |
| Facilities | |

**Table 5: Critical Business Function Supporting IT Assets**

## Hardware/Network/Application Asset Identification Card – Phase 2, Step 3

The Assessment Teams produce asset identification cards in order to gather information produced during phase 2, steps 1 and 2. These cards will be used to select the appropriate asset based controls –Phase 3, Step 2- for the protection of the organization's critical assets.

| Asset Identification Card | |
|---|---|
| Card Creation/Update Date | |
| Asset Category | |
| Asset Name | |
| Asset Description | |
| Asset Owner | |
| Asset Location | |
| Asset Maintainer | |
| Aggregated Recovery Priority | |
| Supported Business Func#1 | |
| Assets role /usage in function | |
| Recovery Priority Requirement | |
| Asset users | |
| Supported Business Func#2 | |
| Assets role /usage in function | |
| Recovery Priority Requirement | |
| Asset users | |

**Table 6: Hardware/Network/Application Asset Identification Card**

## Data Asset Identification Card – Phase 2, Step 3 – Phase 3, Step 2

| Data Asset Identification Card | |
|---|---|
| Card Creation/Update Date | |
| Asset Category | |
| Asset Name | |
| Asset Description | |
| Asset Owner | |
| Asset Storage Location | |
| Asset Maintainer | |
| Aggregated Recovery Priority | |
| Supported Business Func#1 | |
| Assets role /usage in function | |
| Recovery Priority Requirement | |
| Asset users | |

**Table 7: Data Asset Identification Card**

## People Asset Identification Card – Phase 2, Step 3 – Phase 3, Step 2

| People / Suppliers Identification Card | |
|---|---|
| Card Creation/Update Date | |
| Name | |
| Organization and address (if not a company employee) | |
| Department | |
| Title (Role) | |
| Key BCM Responsibilities (If contractual obligations exist, put a reference to the contract) | |
| Office Telephone | |
| FAX | |
| Mobile | |
| Home Telephone | |
| E-mail | |

**Table 8: People Identification Card**

## Facilities Asset Identification Card – Phase 2, Step 3 – Phase 3, Step 2

| Facilities Identification Card | |
|---|---|
| Card Creation/Update Date | |
| Asset Category | |
| Asset Name | |
| Asset Description | |
| Asset Owner | |
| Asset Location | |
| Asset Maintainer | |
| Aggregated Recovery Priority | |
| Supported Business Func#1 | |
| Supported Business Func#2 | |
| Supported Business Func#3 | |
| Supported Business Func#4 | |
| Supported Business Func#5 | |

**Table 9: Facilities Asset Identification Card**

## Asset Requirements Analysis Summary – Phase 2, Step 3

| IT Asset | Function#1 Expedited Service Contract Fulfilment | Function#2 Finance | Function#3 Customer Relationship Management | Aggregated Recovery Priority |
|---|---|---|---|---|
| **Hardware** | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Client Facing Application** | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **People / Suppliers** | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Data** | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Facilities** | | | | |
| | | | | |

**Table 10: Asset Requirements Analysis Summary**

## Organisational Continuity Controls – Phase 3, Step 1

| Organizational Continuity Controls Card | | | |
|---|---|---|---|
| **Risk Areas** | **High** | **Medium** | **Low** |
| **Legal and Regulatory** | (SP1)<br>(SP2)<br>SP3.4<br>(SP4)<br>SP5.1 | SP1.1<br>(SP2)<br>SP3.4<br>(SP4) | SP1.1<br>SP2.3 |
| **Productivity** | (SP1)<br>(SP2)<br>(SP3)<br>(SP4)<br>(SP5) | (SP2)<br>SP3.4<br>(SP4) | SP2.1<br>SP2.2<br>SP5.2 |
| **Financial Stability** | (SP1)<br>(SP2)<br>(SP4) | (SP2)<br>(SP4) | SP2.1<br>SP5.2 |
| **Reputation and Loss of Customer Confidence** | (SP1)<br>(SP2)<br>(SP4)<br>SP3.4 | SP2.2<br>SP2.3<br>(SP4) | SP2.7 |

**Table 11: Organizational Continuity Controls**

## Asset Continuity Control Casrds – Phase 3, Step 2

| Asset Continuity Control Cards | | | |
|---|---|---|---|
| **Asset Category** | **High Risk Cards** | **Medium Risk Cards** | **Low Risk Cards** |
| **Hardware & Network** | CCC-1HN | CCC-2HN | CCC-3HN |
| **Application (Back Office – Client Facing)** | CCC-1A | CCC-2A | CCC-3A |
| **People** | CCC-1P | CCC-2P | CCC-3P |
| **Data** | CCC-1D | CCC-2D | CCC-3D |
| **Facilities** | CCC-1F | CCC-2F | CCC-3F |

**Table 12: Asset Continuity Control Cards**

## List of Asset Selected Controls– Phase 3, Step 3

| Asset Based Continuity Controls | | | |
|---|---|---|---|
| **Control** | **Asset & Priority** | | **Rationale for Selection** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table 13: List of Asset Selected Controls**

## Organizational Controls Gap Analysis Table – Phase 4, Step 1

The gap analysis table is the output of the gap analysis exercise performed by the Assessment Teams during phase 4, step 1. The table summarizes the results from the evaluation of the organization's current business continuity practices compared to the selected controls described on control cards.

| Organizational Continuity Controls | | | |
|---|---|---|---|
| **Control** | **Asset** | **Control Description** | **Do we currently follow the controls included in the control cards?** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table 14: Organizational Controls Gap Analysis List**

## Asset Controls Gap Analysis Table – Phase 4, Step 1

| Asset Based Continuity Controls | | | |
|---|---|---|---|
| **Control** | **Asset & Priority** | | **Do we currently follow the controls included in the control cards?** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table 15: Asset Gap Analysis List**

## Organizational Controls Actions List – Phase 4, Step 2

Following the gap analysis, the Assessment Team reads the controls (Annex A, B) and decides whether the organization will implement or not the continuity controls. This activity is documented into the Actions List table along with the necessary actions that the organization should execute for the implementation of the selected controls.

| Organizational Continuity Controls | | | |
|---|---|---|---|
| **Control** | **Asset** | **Control Description** | **Activity needed, Outcome expected, Deliverable Documentation** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table 16: Organizational Controls Actions List – Example**

## Asset Based Controls Actions List – Phase 4, Step 2

| Asset Based Continuity Controls | | | |
|---|---|---|---|
| **Control** | **Asset & Priority** | | **Activity needed, Outcome expected, Deliverable Documentation** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table 17: Asset Actions List – Example**

## Controls Prioritization Matrix – Phase 4, Step 2

| Controls Prioritization Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | Asset Categories | Hardware & Network | Applications | Data | People | Facilities |
| Recovery Priority | Low | Low | Low | Medium | Medium | High |
| | Medium | Medium | Medium | Medium | Medium | High |
| | High | High | High | High | High | High |

**Table 18: Controls Prioritization Matrix**

## BC Controls Implementation Plan – Phase 4, Step 2

The Assessment Team produces the controls implementation plan, prioritizing the necessary actions (phase 4, step 1) towards the controls implementation. The plan also includes the responsible party for the controls implementation and the expected date of their integration within the organization.

| BC Controls Implementation Plan | | | | |
|---|---|---|---|---|
| **Control** | **Responsible** | **External support required** | **Milestones Mm/Dd** | **Implementation Priority** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Table 19: BC Controls Implementation plan**

## Business Continuity Plan – Phase 4, Step 3

The Business Continuity Plan Template is produced by the execution of the proposed BCM approach. The Plan is created gradually as the Assessment Team executes the various steps. The BCP template exists as a separate document build from the example assessment of a fictitious company. The assessment steps taken to build this BCP are described in chapter 5 of this BCM approach's main document.

## Annex H – Asset Types List

| Asset Category | Description | Asset (types) |
|---|---|---|
| **Hardware** | Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or these that are exposed to the outside world for business functions or | Server<br>Laptop<br>Workstation<br>Storage<br>Security Devices (firewall, IDS / IPS, anti-spam etc) |
| **Network** | Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of component. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually un-trusted networks. | Routers<br>Gateways<br>Switches<br>Wireless Access Points<br>Network Segment (e.g. cabling and equipment between two computers)<br>Other (SAT, Laser) |
| **People** | People in the organization, including business, administration, HR and IT. Critical people are those that play a key role the delivery of product and operational processes. Importance should be given to critical roles that are considered irreplaceable or constitute a single point of failure. | Chief Technology / Information Director<br>Information Technology Manager<br>Database Development & Administration (manager, analyst, architect, administrator etc.)<br>Programming / Software Engineering (manager, engineer, programmer, tester etc.)<br>Technical Support (Help Desk Operator, technician etc.)<br>Systems Analysis & Integration (manager, analyst, integrator, specialist etc.)<br>Technical Writing (manager, writer, publication specialist etc.)<br>Network Design & Administration (manager, analyst, architect, administrator, technician etc.)<br>WEB Development & Administration (manager, developer, designer, administrator etc.) |
| **Back office Applications** | Applications that are key to or part of daily business operations. Disruption of such applications typically results in severe hindering or even unavailability of all dependent business processes. | Financial Control<br>Customer Care<br>Logistics<br>ERP<br>CRM |

| | | |
|---|---|---|
| | | Email |
| | | Internet |
| | | Custom Application |
| | | Intranet |
| | | Industry Application |
| | | Instant messaging |
| | | Security Software (antivirus, proxy, IDS) |
| | | Document Management System |
| **Client Facing Applications** | Applications that are key to or part of the product and service offerings. Disruption of such applications typically results in severe hindering or even unavailability of all dependent customer facing (i.e. front office) business services. | E-commerce |
| | | Internet Service Provisioning – Static, Public IP addresses, DNS service registration and management. |
| | | Email Service Provisioning |
| | | Web Portal |
| | | Web Site |
| | | Application / Data Hosting |
| | | FAX (including incoming call numbers) |
| | | Incoming telephone numbers and DDIs |
| | | Telecommunication Services (i.e. Phone over IP, Mobile telephony, SMS / MMS) |
| **Data** | Data used by the organization in order to perform its business operations, generated within the organization or imported by third parties and/or customers. | Customer Personal Data |
| | | Customer Financial Data |
| | | Corporate Employee Personal Data |
| | | Corporate Employee Financial Data |
| | | Corporate Financial Data |
| | | Corporate Marketing Data |
| | | Corporate Sales Data |
| | | System Technical / Transaction Data |
| | | System manuals |
| **Facilities** | All physical venues/locations including buildings, offices and rooms that the organization uses in order to provide its service/product offerings. | Headquarters |
| | | Secondary Premises |
| | | Branch Offices |
| | | Offices |
| | | Data Canter |

**Table 20: Asset List**

## List of Tables