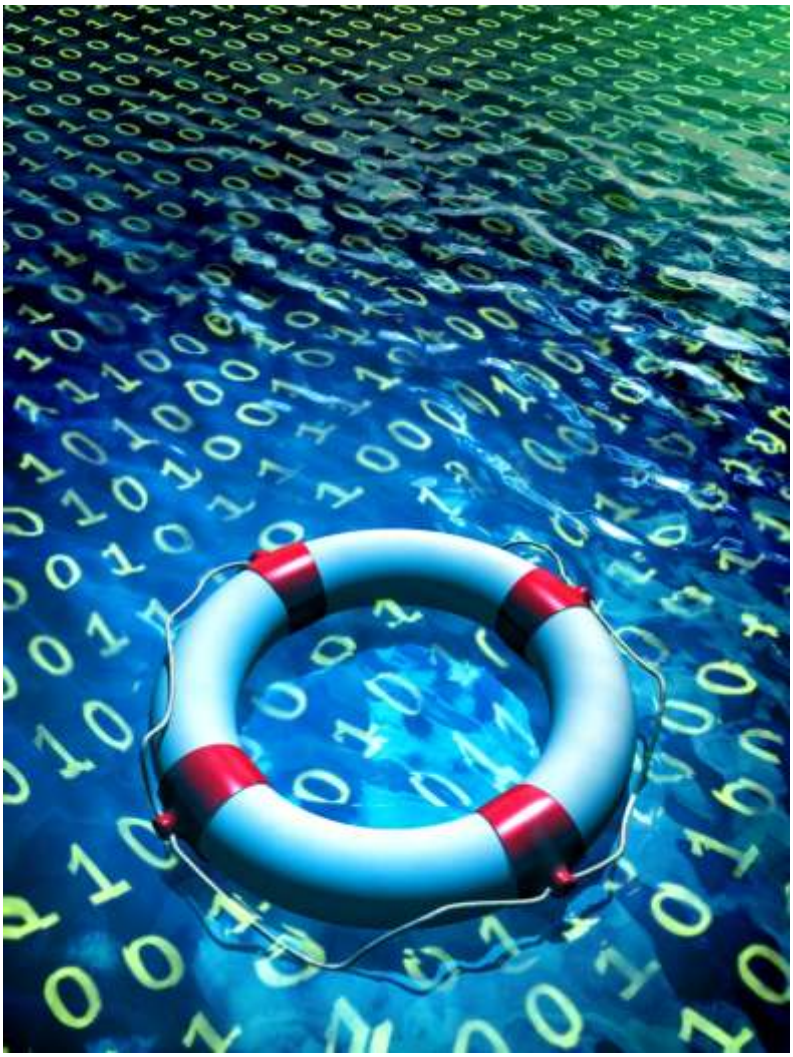

About ENISA

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

Executive Summary

This document is an ENISA deliverable aiming at facilitating a knowledge transfer of key IT security issues to Small Medium Enterprises (SMEs). This deliverable has been developed outside the ENISA work program and is based on the identified need of SMEs for a simplified approach to **IT Business Continuity**. After the simplified approach to Risk Management, this document is the second one that comes to cover basic IT security needs of SMEs.

The aim of this document is to provide a simplified and comprehensive view of IT Continuity/Business Continuity Management (BCM) for use within small and medium sized enterprises (SMEs). To achieve this goal, the present document has been structured in a modular way. It is made up of various parts each devoted to particular needs of stakeholders involved in the process of establishing a Business Continuity Plan (BCP) as part of their Business Continuity Management process.

The philosophy behind the generation of this material was to shield (non-expert) users from the complexity of the activities of BCM. In doing so, some complex security matters have been simplified to the minimum needed to achieve an acceptable level of business continuity.

There is no doubt that if a high level of availability is needed the full complexity of Business Continuity Management must be taken into account including a plunge into the fine details of corresponding measures and technology. In this regard, the ideas and approach presented here are thought to cover an acceptable level of availability for small organisations with reduced security budgets. More advanced forms of availability (e.g. such needed for critical infrastructure components) would require a more thorough treatment that is beyond the scope of this document.

The present material has been generated by anticipating the whole range of skills of different stakeholders involved in continuity management. The proposed Business Continuity Management process is structured by means of a simplified four-phase assessment approach. We do not assume any advanced knowledge of continuity and availability issues on the part of users of this material. Where this knowledge would be necessary, the present approach represents a “black box” offering a limited number of comprehensive choices.

Another criterion that has been taken into account is the cost effectiveness in all phases of Business Continuity Management. The present material can help decision makers to decide which approach is most suitable to their organisation for the assessment of availability risks, based on cost and performance indicators. Furthermore, in the case where self assessment has been selected, this document provides the necessary tools to perform same, without requiring previous experience in this area.

The simplified Business Continuity Management approach presented in this document is one example of good practice for assessing availability risks. It is assumed that other similar approaches/good practices exist which could be used instead. In this way the present approach is neither an attempt to replace existing standards nor to redefine good practices. Rather, it is designed to give interested SMEs a tool which they could not easily find elsewhere.

The application of the ideas presented here has been demonstrated using an example. The example is presented within the framework of the proposed simplified Business Continuity approach.

It is worth mentioning that this document is the second in a series of material that has been released by ENISA to generate awareness about Business Continuity for SMEs. In 2007, ENISA has developed a simplified approach to Risk Assessment / Risk Management for SMEs. The present document follows a similar approach and is compatible to the one of the simplified Risk Management approach. The later has been validated in a series of pilots with multiplier organisations and SMEs with significant success.

In a similar way, ENISA activities that will follow in the future embrace the validation of this material via pilot projects in SMEs, evaluation/review through expert teams, dissemination via professional and/or training associations, etc. Final objective is to have a version of this document that can be used by SMEs “as is”, that is, without further improvements/explanations/adaptations. For this reason, we refer to the present document as “beta version” meaning that additional improvements and adjustments will follow after various pilots, deployments and disseminations, leading thus in the middle term to the maturity of the presented material.

This document has been developed by the Risk Management Section of the Technical Competence Department of ENISA in cooperation with Obrela Security Industires (OSI).

Contents

1. Introduction

1.1 Scope

Small and Medium Enterprises (SMEs) are a priority focus area for government economic policy and are considered to be of key importance to socio-economic growth in European Union. SMEs are usually born out of entrepreneurial passion and limited funding, with business systems that are often heterogeneous and independent. Moreover, tangible and intangible business assets of SMEs are rudimentarily defined, and the value of their availability is often only partially known.

Business Continuity Management (BCM) is a process that provides a framework ensuring the continuity or uninterrupted provision of critical business functions and operations. It provides a basis for planning to ensure an organization's long-term survivability following a disruptive event towards the SME "business as usual" functions and services. **BCM can be considered as a risk treatment method, complementary of a wider Risk Management method, explicitly focused on the management and containment of continuity risks, introduced by certain natural or man-made threats that, if realized, can cause unavailability of services.**

Usually, due to the dynamic and ad hoc development of many SMEs, integration of business continuity issues is not systematically addressed in the building-up phase. Thus, policies and frameworks regarding business continuity planning are usually very rudimentary or even non-existent. It is often the case that the basic understanding of business continuity risk in SMEs does not extend much beyond environmental controls to safeguard from natural disasters such as power supply, fire, flood etc. Inadvertent threats pose some of the highest continuity risks to SMEs, and yet personnel training and awareness programmes are often neglected.

Far from blaming SME executives for not understanding the critical issue surrounding business continuity, research concludes that SME leadership needs to engage, understand and implement formal business continuity processes, including technical and organizational measures. Without such measures, their organizations may be severely impacted by inadvertent threats / deliberate attacks on their information systems, which could ultimately lead to business failure.

1.2 Purpose

Through the presented approach, SMEs will be able to define the appropriate activities towards the successful development, establishment and maintenance of a BCM framework within their business environment. **The outcome of this document will be a self-developed Business Continuity Plan (BCP) that SMEs could follow in order to ensure the continuity of their core business functions.**

The proposed business continuity management approach leads to a quick and encompassing identification and mitigation of continuity risks. This tailored model shall consist the foundation of SMEs business continuity planning, **based upon the:**

- Special needs and capacities of SMEs in terms of human, IT and budget resources
- Common continuity risk levels typically faced by SMEs.

The proposed BCM model focuses explicitly on ensuring and protecting **the availability of the core IT assets used to support and provide the organization's critical business functions** (i.e. production, customer relationship, human resource). It should be noted that confidentiality and integrity security requirements of the aforementioned IT assets are not in focus as the latter should be covered under a Risk Management / Risk Assessment process.

1.3 Related disciplines

Business Continuity Management **is complementary to a broader Risk Management (RM) Framework** aiming at the identification of the risks connected to the businesses and the consequences from their occurrence. Risk management embraces the need to manage risk around all the activities that enable an organization to survive, encompassing thus both internal processes and externally offered services. **Business Continuity Management encompasses the identification and risk mitigation for those activities upon which the organization depends for its survival, i.e. retain credibility and continue towards the fulfilment of business goals.** Through BCM, an organization can recognize what needs to be done before an incident occurs, ensuring that its people, reputation, assets, systems and information are secure and available.

As Business Continuity is considered to be an integral part of an overall Risk Management, the proposed BCM approach for SMEs goes along the lines of the necessary RA / RM activities as described in the ENISA deliverable "Information Package for SMEs". This compatibility seemed to be necessary in order to retain the possibility of integrating the Management of Continuity Risks with a Risk Management/ Risk Assessment approach, leading thus to a modular design of these ENISA deliverables.

2. Structure of Document

A modular structure has been given to this document in order to cover the diverse needs of various SME types. Depending on the needs of a particular SME and the extent to which it seeks to cope with business continuity, different parts of the document can be used.

For SMEs requiring an overview of business continuity management, for example, the generic part of this document will be useful (see Chapter 3, Guidance for the Decision Maker and Chapter 4, A simplified Approach: Overview).

Should an SME decide to implement its Business Continuity Management on its own, the parts of this document containing the detailed description of the business continuity method and the example will be relevant (see Chapter 5. Self Assessment Guidelines with one Example).

In the case of a self-assessment, the detailed material found in the annexes will be necessary in order to implement the proposed measures in the organization (see Annex A. organizational Continuity Control cards, Annex B. Asset based Continuity Control Cards and Annex F. Business continuity Plan Template).

To give a better view on how this document can be used, we provide some use cases based on the various target groups of this document:

- **People with managerial background** may consider chapter three targeting decision makers. It provides information about business continuity, while referring to the decision making process required for the establishment of a Business Continuity Plan. Interested managers may like to understand some of the details of the business continuity process as presented in Chapter 4.
- **Non-experienced members of an Assessment Team** will need to understand the proposed simplified business continuity management approach. They will need to consider some details and go through the developed example presented in Chapter 5.
- **Expert members of an Assessment Team** will need to read the entire approach and understand all relevant details. They will also need to be in the position to cope with the material presented in the annexes (e.g. presented measures, structure of the BCP, detailed tables for the BCP development, etc.).

3. Guidance for the Decision Maker

3.1 What a decision maker needs to consider

Today, the information created, processed, and used by an organization is one of its most valuable assets. The unavailability, loss or destruction of this asset can **severely impact** an organization, can lead to **breach of laws and regulations** and negatively **affect its brand name**.

Next to high availability of delivered services/products, main management responsibility is the protection of human life and valuable company assets. Proprietors and decision makers understand the current status of the environment within they operate in order to make well-founded judgments and investments.

However, the achievement of an acceptable level of mitigation of continuity risks is often neglected. Such risks might lead to critical situations when extrapolated to vital business, such as legal issues, customer dissatisfaction and negative overall impact on the organization. Thus, continuity risks may lead to more generic and more critical risk categories, such as:

- **Legal / Compliance Risks** arising from violations of compliance with laws and regulations (i.e. data retention). Legal or compliance risks can expose an organization to negative publicity, fines, penalties, payment of damages and annulations of contracts. **Loss or destruction of customer information (i.e. personal data) such as credit card information, financial information and health information can also raise potential risks from third party claims**. In addition, failure to meet SLAs requirements with customers regarding data service availability may result to significant lawsuits.
- **Productivity Risk** resulting from operational losses and **poor customer service delivery.** Such risks may emerge from **unavailability of basic production services and operation functions**. Such risks may be relevant to all production activities that contribute in some way to the overall delivery of a product or service. Productivity Risks are not confined only to the use of technology; they can be the result of organizational activities. The risks arising from inadequate or poorly controlled information systems used to support core business functions such as front office, accounting, or other units are also captured in this risk category. Inadequate management may result in high productivity risks including high operating costs, operational failures, poor management decisions, **lack of privacy and disruption of service to customers**.
- **Financial Stability Risks** arise through unavailability of delivered products and services towards the organization's customers. Such risks may lead to major financial losses having impact directly or indirectly on the financial stability of the organization, causing thus a failure to achieve stated goals and financial objectives.
- **Reputation and Loss of Customer Confidence** are the most difficult and yet one of the most important risks to quantify and mitigate. Such risks lead to the damage to the organization's reputation, an intangible but important asset. Will customers and / or other companies cooperate with a company once they read in the paper that a company's service quality is low or service delivery is regularly interrupted? Will top employees remain at a company so reputably damaged? And, what will be the reaction of the company's shareholders? What is the expected loss of future business revenue? What is the expected loss of market capitalization?

SMEs**,** due to their nature, inherit certain advantages and disadvantages in the field of business continuity management. **The great disadvantage of SMEs** is that the potential impact of the risks they face **is likely to be more destructive since the majority operate in specialised markets** where even a short interruption to normal business can have a disproportionate effect – totally halting output and letting customers down. In addition, due to shortages in resources (e.g. staff, financial, locations, etc.) it is more difficult for small firms to absorb the impact of business interruption, than it is in the case of bigger organisations.

On the other hand, due to their nature, SMEs **have two significant advantages** towards the planning of Business Continuity efforts:

- No one knows their own business better than SMEs, as they often rely on limited resources. In this regard, they are in the best position to know how their business would cope without supporting infrastructures (e.g. IT systems) for a given period of time (e.g. morning, a day, or a week).
- Due to the fact that SMEs are usually servicing a niche market, they are able to know if their customer base would be affected (e.g. go elsewhere or return) if customers' ability to do business with the SMEs is temporarily unavailable.

Spending time developing a Business Continuity Management Framework and defining the organization's Business Continuity Plan (BCP) will not only increase the likelihood of the organization's survival from a crisis or business interruption, but will also ensure the safety and protection of the SME **most critical asset, its people.**

3.2 What a decision maker needs to know

Protecting the future of a business, whatever its size, has to be one of the primary priorities for every business leader. **BS25999, BSI's standard in the field of Business Continuity Management, states that the Continuity Management is a holistic management process** that identifies in advance the potential impacts of a wide variety of disruptions to the organization's availability. This includes all necessary activities allowing the organization to tolerate the loss of part or all of its operational capability. BCM is a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- Proactively improves an organization's resilience against the disruption or interruption of its ability to supply its products or services;

- Provides a tried and proven method of restoring an organization's ability to supply its critical products and services to an agreed level, and
- Delivers a proven capability to manage a business interruption (incident) and protect the organization's reputation and brand.

In this regard BCM can help decision makers to:

- Understand the overall risk context within which the organization operates;
- Identify/document the critical business functions that the organization has to deliver
- Identify what barriers or interruptions can be encountered in trying to deliver these critical business functions;
- Understand how the organization can continue to deliver these functions should interruptions occur;
- Understand the likely range of outcomes when continuity controls and other mitigation strategies are implemented;
- Ensure that all staff understand their roles and responsibilities when a major disruption occurs;
- Build consensus and commitment to the implementation, deployment and exercising of business continuity;
- Integrate business continuity as part of routine "business as usual".

The main artefact of a BCM framework used to achieve business contingency is the organization's BCP. The objective of a BCP is to recover all critical business functions and minimize the impact for SME employees, customers and delivery. A BCP is not one document but rather a whole suite of coherent documents that form the organisation's response to an incident, from the moment of impact, to the resumption of the normal operations.

The smaller the business is, the more important it is to have a Business Continuity Plan in place. Any incident, no matter how small, is capable of causing impacts on the business and consequently the SME profitability. The size of any BCP will depend on the risks faced by each business. Organisations that have a business continuity plan are far more likely to survive the effects of a major incident than those that don't. Further, depending on the sector, customers may be obliged to use suppliers who comply with certain security/continuity standards. Thus, for certain sectors there might be a commercial benefit to consider, as **companies with business continuity plans are more attractive to do business with.** For example, large businesses that rely on the outsourced services of third parties will prefer to work with suppliers who have a Business Continuity Plan in place.

A BCP requires careful preparation and planning. As a best practice, often followed, is appointing a person responsible for business continuity who will ensure that a Business Continuity Plan will be created, developed and maintained. The complexity of this plan must be synchronised with the risk exposure, size and value of the organisation's services, providing thus a practical and realistic ground.

3.3 Personnel health & safety

An organization's people are the most valuable asset. The unavailability of key people and injury to employees are risks that cannot be overlooked. **The fundamental factor towards** the success of any BCP is determined by the emergency framework established by the organization in order to protect and safeguard people's health and safety. It should be noted that due to the concentration on IT issues, the proposed BCM approach does not provide detailed guidelines or actions that an SME should carry out in order to protect personnel health and safety. However, due to the sensitive nature and importance of the topic some generic guidance is provided hereby.

Prior to developing a BCP the organization should have in place a set of emergency procedures describing the general measures that will be taken to protect employees, customers, visitors, etc. from the direct, indirect or potential effects of any incident or emergency (i.e. evacuation, shelter-in-place, area of refuge). Such precautions should eliminate or reduce further danger to personnel health and safety. In this respect, emergency procedures should as a minimum meet the following requirements:

- Employees understand the evacuation procedures;
- Employees know what to do if a fire breaks out;
- Employees know what to do if colleagues suffer an injury;

- Roles and responsibilities have been assigned for evacuation and first aid;
- All staff have been trained in their roles;
- Alternate sites / evacuation Points for the personnel have been determined if it is not considered safe to remain close to the building and
- An indoor emergency site has been identified, so staff can remain together safe, warm and dry while the next steps are decided.

The emergency procedures include protection of people in the first place, containment of the emergency comes second, and assessment of the situation comes next. Regardless of the type of the BCP the organization creates, the development of emergency procedures is the highest priority. Although it seems intuitive that people's health and safety is addressed first, it is not always the first thing that comes to mind when an emergency strikes.

In addition to the emergency procedures the organizations should prepare a set of **one-page emergency checklists** describing simple but life-saving tips and guidelines that employees should undertake **prior, during** and **after** a natural or man-made disaster. Indicatively, the following checklists should be developed and distributed to ALL personnel of the organization:

- Flood Safety Checklist
- Lighting Safety Checklist
- Extreme Heat Safety Checklist
- Fire Fighting Checklist
- Fire Safety Checklist
- Power Service Disruption Checklist
- Handling Suspicious Parcels and Letters Checklist
- Prevention and Response to Workplace Violence Checklist

In order to provide a guideline for the emergency checklists development, Annex E includes a sample of a Fire Fighting Checklist which describes engagement rules and safety methods for fighting a potential fire within the organization's premises.

Concluding, it has to be mentioned that EU legislation obliges organizations -operating within EU member states- to ensure employees' health and safety through a specific Legal Framework. Specifically, **OJ L 393, Council Directive 89/391/EEC (12/6/1989) includes the minimum requirements for the workplace, obliging employers to provide certain health and safety protection measures.** This includes first-aid and fire-fighting equipment, evacuation of workers training and information provisioning to workers. Annex E provides additional information regarding the aforementioned Directive since the latter has been further expanded to individual Directives in order cover certain issues regarding personnel health and safety.

4. A Simplified Approach: Overview

The present chapter presents the contents of a simplified **Business Continuity Management (BCM) approach** that can be used by SMEs for **self-assessment leading to the development of the organization's Business Continuity Plan (BCP). Both BCM and BCP form the strategy of the organisation towards Business Continuity.**

The BCP to be generated will address the following issues:

- Set the scope of the plan by identifying the critical business functions of the organization to be protected by the plan.
- Link to emergency management procedures and plans to ensure personnel safety.
- Identify critical ICT assets required to recover and sustain the minimum operating levels of the critical business functions in scope.
- Define the resource requirements (people, work area, IT, telecommunications) for the plan implementation
- Set the structure of the business continuity response with a focus on ICT.
  - Establish roles and responsibilities during an incident.
  - Disaster recovery plan: How to recover operations in a case of a disaster.
  - Per ICT asset contingency plan: How to recover a specific ICT asset.
- Define the controls used to safeguard the continuity of the functions in scope.
- Provide contact list(s) with business continuity responsible employees / teams / managers
- Provide contact details of vendors / suppliers committed to supporting the recovery efforts
- Provide contact list of Governmental authorities / bodies
- Define activities for Testing, Reassessing and Maintaining the organization's Business Continuity Plan

The **proposed approach is self-directed**, meaning that people from an organization assume responsibility for assessing the continuity requirements, selecting controls and thus setting the organization's continuity strategy. This technique combines predefined continuity risk profiles with a set of good practices and relevant continuity controls while leveraging people's knowledge of their organization to:

- Identify the continuity risk profile that matches their organization;
- Identify critical business functions that are necessary to sustain the viability of the organization;
- Identify the critical ICT assets to be protected;
- Capture the current state of business continuity practices within the organization;
- Decide on the priority of implementation for the proposed continuity controls and
- Develop a Business Continuity Plan setting the continuity strategy for the organization.

The main advantage of this SME BCM approach is that it can provide an acceptable (i.e. baseline) business continuity level with a low assessment and management effort. This is due to the following aspects that enhance practicability:

- The risk profile of the organization can be easily identified, through qualitative descriptions of profiles in four risk areas (Legal and Regulatory, Productivity, Financial stability, Reputation and Loss of Customer Confidence);
- Hints regarding the business functions which are likely to be critical are provided;
- The typical ICT assets for small organizations are given;
- Continuity requirements of the critical assets are automatically derived by the organization's risk profile and the recovery priority of the supported critical business function;
- Control options sufficient to meet the assets' continuity requirements are available through predefined control cards;

- The BCP is gradually developed while the phases of the proposed BCM approach are executed and
- Guidance for handling incidents and escalating up to the invocation point of BCP is provided.

These advantages can lead to a low cost self-assessment by teams with low expertise in the field of business continuity. If done carefully, an acceptable level of business contingency will result.

The proposed BCM approach could be further enhanced by integrating the aforementioned self-assessment business continuity management process within an automated tool. This will significantly simplify the necessary steps that an SME needs to undertake in order to initially run and establish a BCM.

4.2 Proposed BCM approach resourse requirements

The presented BCM approach is based on some elements from the OCTAVE ALLEGRO Risk Assessment Methodology and is modular to the ENISA deliverable "Information Package for SMEs" describing a simplified Risk Management approach. In this regard, the BCM approach is well-suited for SMEs who desire to follow a BCM model **without extensive organizational involvement, expertise, or input.**

However, in order to execute the proposed model an SME should be able to provide the required manpower for establishing an **Assessment Team**, responsible for utilizing the present BCM approach. Depending on the SME size, the Assessment Team is expected to engage three (3) to five (5) people with both business and IT skills.

Specifically, the presented BCM approach requires an Assessment Team incorporating a broad understanding of the organization, together with the following skills:

- Ability to understand the implemented business processes;
- Knowledge in IT Systems and Networks used by the organization for the provisioning of critical business functions;
- Knowledge on the dependencies between the business processes and IT;
- Problem-solving skills;
- Analytical skills;
- Ability to work in a team;
- Leadership / project management skills;
- Availability of few days for the necessary assessment and BCP development.

In case that an SME is not able to utilize an Assessment Team with the aforementioned skills, the involvement of a specialized third party / contractor should be considered instead. The contractor can provide the missing required expertise (i.e. BCP and IT expertise and project management skills) required for the execution of the proposed BCM approach.

The execution of the proposed BCM by the SME without the involvement of a third party offers many **advantages such as the development of internal organization know-how and competence in the field of BCM. Moreover, depending on consulting prices in the security market, this approach may result in reduced expenses.**

On the other hand, in case of an external third party involvement in the BCP creation, the organization must actively participate in the self-assessment process by using a third party as a facilitator/advisor. Moreover, the assessment must be based on a BCM approach that can be understood by the organization prior to its usage. On the long run, this is a necessary **precondition in order to achieve know-how transfer** between the third party and the organization that will allow the maintenance of the BCP and the sustainment of the entire BCM process.

4.3 Working assumptions

Lack of specialised personnel in several areas such as Risk Management, Business Impact Assessment, Business Continuity or Information Technology is one of the problems faced by SMEs. In addition, acquiring all the required skills through external contractors may not be possible or economically feasible. At the same time, most existing approaches to the assessment and management of continuity risks generally focus on the needs of large organizations. A simple approach designed for small

organizations does not exist today, at least not in the form of publicly available guidelines. Some consulting firms have developed good practices for that purpose, but they use them in the context of customer projects. Although claiming to be appropriate, other approaches for SMEs are often too complex for self assessments.

The ENISA deliverable "**Business and IT Continuity: Overview and Implementation Principles**" describes a six-step process to implementing Business Continuity Management. It focuses on the items to be considered for the delivery of the BCP and it is an overview of BCM derived by the contents of existing standards (i.e. **BS25999-1 and BS25999-2).** Furthermore, in that deliverable a graphical representation of the interfaces between BCM and Risk Management/Risks Assessment is provided. The present document **uses the ENISA six-step BCM approach as the basis** to produce a tailored, yet simplified approach to BCM implementation, so that it can be utilized by SMEs. It is worth mentioning, that parts of the presented material have also been influenced by OCTAVE[1] ALLEGRO principles.

Our intent is to provide those organizations with a simple, efficient and inexpensive approach to identifying and managing their continuity risks. Further, **the presented simplified approach provides small organizations with a means to perform self-assessments.**

In addition, some considerations/assumptions have been made for the development of this material:

- Due to limited resource availability SMEs are not in the position to implement a fully fledged BCM. Rather, a BCM has to be tailored in order to meet SMEs' capacities in terms of human and monetary resources;
- Even if an SME's staff have special knowledge of information systems, they might not possess special know-how on IT security and business continuity matters. Lack of specialized personnel in several areas such as Risk Management, Business Impact Assessment, Incident and Crisis Management is a typical problem faced by SMEs;
- Small sized companies are using standardized data-processing environments which are important for the business. They use off-the-shelf products and are connected for their business to the Internet and are thus exposed to numerous threats that might affect their business continuity;
- The establishment of BCM through SME trade bodies and associations will help promote understanding of continuity issues by those with little background in business continuity planning;
- SMEs are usually born out of entrepreneurial passion and limited funding, with business systems that are often 'patched together' and thus are heterogeneous and independent;
- Most SME business managers barely understand highly technical and complex terminology related to IT business continuity and
- In cases that SMEs are not even interested in business continuity planning they may benefit from access to awareness, training and guidance material.

4.4 A four-phased approach

In this chapter the contents of a simplified BCM approach that can be used by SMEs for the development and implementation of a BCP are presented. The proposed BCM approach uses four phases towards the development and delivery of a BCP for SMEs. An overview of the four phases is given in the following Figure.

[1] *OCTAVE Allegro is an assessment methodology to streamline and optimize the process of assessing information security risks so that an organization can obtain sufficient results with a small investment in time, people, and other limited resources. OCTAVE is a service mark of Carnegie Mellon University. OCTAVE was developed at the CERT Coordination Centre (CERT/CC).*

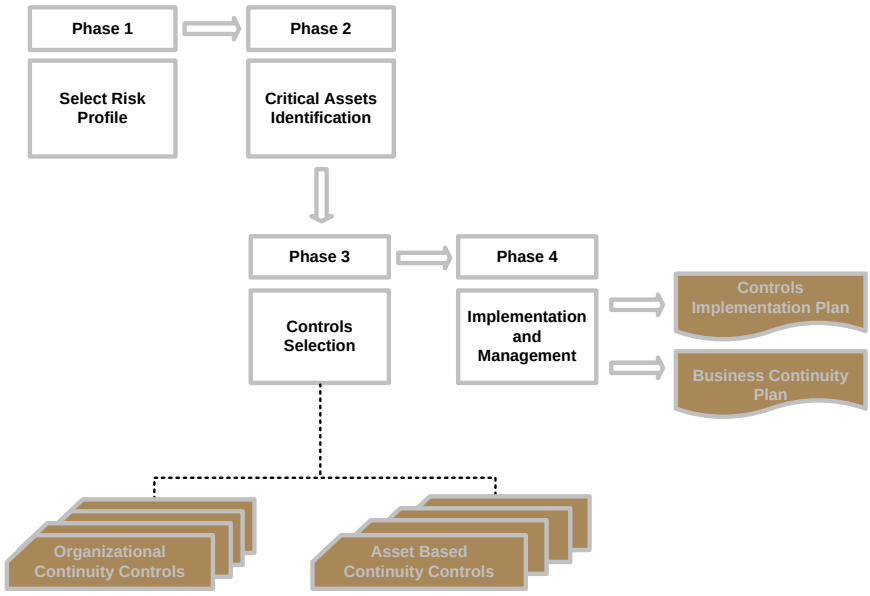

Figure 1: The four phases underlying the proposed BCM approach

In the rest of this chapter we deliver an overview of each phase, we describe the main elements processed and the generated outputs. This chapter is foreseen as an overview of the approach. More detailed information about the elements and the execution of each phase is given in chapter 5.

4.4.1 Phase 1 – Select Risk Profile

During this phase the Assessment Team evaluates their business risk profile by using a predefined set of qualitative criteria. By using **the risk profile evaluation table (see below)**, Assessment Teams are in a position to identify their risk context. The risk context is derived from the business, the internal and external environment of an organization and can be divided into four risk areas: **Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability**[2]**.**

Risk Areas	High	Medium	Low
Legal and Regulatory	The organization handles sensitive/personal customer information as defined by the EU Data Protection Law. 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. 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. Loss and / or destruction of the aforementioned data will lead to legal fines from Regulatory Bodies. 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. 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. 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. 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. 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. 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. 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.

[2] *The risk areas mentioned here are indicative. Additional risk areas might be introduced when applying the approach to particular sectors. The risk areas taken in this approach have (i.e. Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability) have been adopted from the OCTAVE ALLEGRO Risk Assessment Methodology.*

Financial Stability	Unavailability of products and services of less than one day lead to a major one time financial loss and cannot be tolerated. Yearly revenues are directly related to the continuous and uninterrupted provision of on-line services (i.e. sales are performed online). Unavailability of online presence will lead to direct financial loss as major services are provided by using e-business applications. Fines that may incur due to non-compliance with legal and regulatory requirements may lead to intolerable financial loss.	Unavailability of products and services of less than one day lead to a significant one time financial loss. Yearly revenues are indirectly related to the continuous and uninterrupted provision of online services (i.e. products and Services are supported with on-line services). 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.). Fines that may incur due to non-compliance with legal and regulatory requirements are possible but will not affect financial stability.	Unavailability of products and services of less than one day lead to no or marginal one time financial loss. Yearly revenues are not directly or indirectly related to the continuous and uninterrupted provision of on-line services. Unavailability of online presence 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.). 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

Each area is classified in three classes: High, Medium and Low. These classes express qualitative criteria for the organization in question with regard to the risk area and help identify a risk level. The team evaluates risks identified for every area in order to produce the **organization risk profile.**

As a rule of thumb the highest risk identified in any of the risk areas characterizes the overall business risk profile. A high risk carried in the financial risk area marks a high risk profile. Equally, a medium risk leads to a medium risk profile and low risks to low risk profiles. For example a low risk carried in the reputation and confidence, in legal and regulatory compliance and productivity but a high risk in financial stability risk class concludes to a high organization risk profile.

Risk profile selection should be considered as a very important decision **which subsequently leads to the risk-related selection of organizational continuity controls** (see Annex C and Annex D).

4.4.2 Phase 2 – Critical Asset Identification

During this phase, the Assessment Team selects **critical business functions** based on their relative importance to the organization. Critical business functions are these functions whose interruption will lead to an SME's suffering from serious financial, legal, and/or other damages or penalties**. It should be noted that the earliest possible recovery of such functions after a disruption is the main objective of a Business Continuity Plan.**

Typically, an organization's management knows what **its business key processes** are and how they can use their limited resources to protect them. The Assessment Team determines what is important to the organization and selects those key business processes as the most important to the organization, (also referred to as **critical business functions**)**. Together with the assessed Risk Profile, critical business functions** are the essential parameter for the BCP (i.e. complexity, required effort, recovery costs, etc.). The Assessment Team selects one or more of the following **business functions categories**[3] (here indicatively):

- **Production;**
- **Customer Relationship;**
- **Human Resource;**
- **Finance and**
- **New Product Acquisition / Development.**

Together with the selection of critical business functions the Assessment Team defines their recovery priority, referred to as **business function recovery priority.**

The business function recovery priority determines the absolute maximum time within which the function can be unavailable and the SME can remain viable, that is, it can avoid intolerable consequences. In other words it is the maximum period of time in which the function can be down before severe damage has been caused to the organization. In this regard, the organization should restore the business function within this timeframe in order to remain viable.

The recovery priority can be assigned with three distinct values; High, Medium and Low. Each value implies a different timeframe for the business function recovery; less than 1 day, 1 to 3 days and up to 5 days respectively[4]. The business function recovery priority will be later used to determine the asset based continuity controls selection (see Annex B and Annex D).

After identification of critical business functions the Assessment Team will associate the dependencies of the critical business functions with the supporting assets used for their provision. This activity reveals the dependencies between the various assets and the organization's business functions. **This will help the SME to focus its Business Continuity Plan on the assets that each business function relies on**. The assets supporting critical business functions are called **critical assets**. In security management, the **identification of critical assets** is a fundamental activity for the determination of the required protection level.

The following table depicts predefined categories of assets and types that can be considered by the Assessment Team during the critical asset identification. It should be noted that asset types may be composed of other asset types. For instance components of an application might be servers, workstations, routers, network segments etc. During this step seeking the contribution of people that have an understanding of the deployed IT systems is essential.

---

[3] *Business functions categories can be further expanded by the Assessment Teams with respect to the organization's operating environment and the critical business functions used to fulfil the organization's business goals and objectives.*

[4] *It is worth mentioning that these recovery priorities have been selected as indicative. According to the sector/requirements of an SME, these values may be adapted appropriately. For example a SME providing Value-Added Services (VAS) (i.e. call management services, mobile data services) may not be able to tolerate service unavailability more than few hours, as this could result in a major one-time financial loss affecting significantly business financial stability.*

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 those that are exposed to the outside world for business functions or services.	Server Laptop Workstation Storage 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 non trusted networks.	Routers Gateways Switches Wireless Access Points Network Segment (e.g. cabling and equipment between two computers) Other (SAT, Laser)
People	People in the organization, including business, administration, HR and IT. Critical people are those that play a key role for 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 Information Technology Manager Database Development & Administration (manager, analyst, architect, administrator etc.) Programming / Software Engineering (manager, engineer, programmer, tester etc.) Technical Support (Help Desk Operator, technician etc.) Systems Analysis & Integration (manager, analyst, integrator, specialist etc.) Technical Writing (manager, writer, publication specialist etc.) Network Design & Administration (manager, analyst, architect, administrator, technician etc.) 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 Customer Care Logistics ERP 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 2: Asset List

Finally, the Assessment Team will analyze the continuity requirements of the identified assets. The analysis is performed via **Asset Identification Cards**[5] which are distributed to organization's key personnel (asset owners). The cards will be used to select the appropriate controls in order to ensure their continuity in the case of an unlikely event.

[5] *Asset Identification Card is derived by OCTAVE ALLEGRO Risk Assessment Methodology.*

4.4.3 Phase 3 – Controls Selection

During Phase 3 the Assessment Team selects appropriate controls based on the risk profile selected for every risk category and the list of identified critical assets. Continuity Control Cards are predefined and can be selected by the Assessment Team. Controls are separated in **two categories, that is, organizational continuity controls and the asset-based continuity controls,** both are available as **control cards**:

- Organizational controls cards that contain controls applicable to the organization horizontally and are concerned with practices and management procedures and
- Asset control cards that are applicable to categories of critical assets. Control cards are essentially pre-selected and grouped according to risk profiles and asset recovery priority.

Table 3 lists the categories of controls, their structure and their name as they are considered in this approach.

Controls Category	Control No.	Name of the control
Organizational	**SP1**	Business Continuity Management Organization
	SP2	Business Continuity Policy, Plans and Procedures
	SP3	Test Business Continuity Plan
	SP4	Sustain Business Continuity Management
	SP5	Service Providers / Third Parties Business Continuity Management
Asset Based	**HN1.1**	Information System Resilience
	HN1.2	Information System Backup
	HN1.3	Information System Redundancy
	A1.1	Application resilience
	A1.2	Application Backup
	D1.1	Data Storage
	D2.2	Data Backup
	P1.1	Physical Security
	P1.2	Awareness and Training
	F1.1	IT Site
	F1.2	Environmental Security
	F1.3	Physical Security

Table 3: Continuity Controls used in the approach presented

Accordingly, phase 3 of the proposed assessment approach consists of two separate but equally important steps leading to the **selection of organizational continuity controls** and the **selection of asset-based continuity controls.**

The selection of the organizational control cards is performed in a fairly straightforward manner. The Assessment Team uses the **Risk Profile Evaluation Table and the Organizational Continuity Controls Table[6] (table 4)** to select organizational continuity control cards for the risk areas identified during phase 1 (select Risk Profile), thereby defining the direction for the organization's business continuity. **A detailed description of the controls is included in Annex C.**

[6] *Organizational controls assigned to risk areas vary according to their classification.*

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP2) SP3.4 (SP4) SP5.1	SP1.1 (SP2) SP3.4 (SP4)	SP1.1 SP2.3
Productivity	(SP1) (SP2) (SP3) (SP4) (SP5)	(SP2) SP3.4 (SP4)	SP2.1 SP2.2 SP5.2
Financial Stability	(SP1) (SP2) (SP4)	(SP2) (SP4)	SP2.1 SP5.2
Reputation and Loss of Customer Confidence	(SP1) (SP2) (SP4) SP3.4	SP2.2 SP2.3 (SP4)	SP2.7

Table 4: Organizational Continuity Controls

Based on the risk profile and the business function recovery priority the Assessment Team can use asset continuity control cards table (see Table 5) to identify the controls appropriate for the protection of critical assets.

Asset Continuity Control Cards			
Asset Category	**High Risk**	**Medium Risk**	**Low Risk**
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 5: Asset based Continuity Control Cards

Asset control cards are essentially grouped in two categories, **corresponding to asset category and risk profile.** It is worth mentioning that the recovery priority is also a factor that determines the necessary continuity control. Recovery priority is considered within each asset based control card, as can be seen in Table 6 below.

For the sake of this presentation, we add at this point the control card CCC-1HN. As indicated in Table 6, this card is appropriate for the protection of a hardware and / or a network component- in a high risk scenario (high risk profile). As shown below, different control assignments can be found for the various recovery priorities.

Asset Based Continuity Control Card ID		CCC-1HN		
Risk Profile		High		
Asset Category		Hardware and Network		
Continuity Controls Category		Resilience	Back up	Redundancy
Recovery Priority	High	HN.1.1.1 - HN.1.1.2 HN.1.1.3 - HN.1.1.4 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.3 - HN.1.2.4 HN.1.2.5	HN.1.3.1 - HN.1.3.2 HN.1.3.3
	Medium	HN.1.1.1 - HN.1.1.2 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.5	HN.1.3.1 - HN.1.3.3
	Low	HN.1.1.1 - HN.1.1.7	HN.1.2.1 HN.1.2.5	HN.1.3.3
Recovery Actions		RA.1.1.2 – RA.1.1.5	RA.1.2.1 - RA.1.2.4	RA.1.3.1 - RA.1.3.2 RA.1.3.3

Table 6: CCC-1HN Asset based control card

Finally, the Assessment Team will have the opportunity to document the selected controls (both organizational and asset-based ones) along with the rationale for selecting each control. The output of this activity will facilitate the next steps of the Assessment Team towards the definition of the actions plans.

4.4.4 Phase 4 – Implementation and Management

In Phase 4 the Assessment Team is occupied with the evaluation of the organization's current business continuity practices using the control cards as the “continuity requirements” and assessing the gaps between these and current business continuity practices both at an organizational and critical asset level. The output from this process forms the basis for the planning activity that follows next.

It might be the case that due to limited resources SMEs will not be able to implement all identified controls for all business functions and all the involved assets at once. Therefore, as an initial activity in the plan for implementation, prioritization has to take place.

The Assessment Team needs yet to plan the implementation of the selected controls and generate the corresponding BCP. SMEs will likely have limited funds and staff members available to implement the necessary controls. After the evaluation, the Assessment Team prioritizes the activities and then focuses on implementing the highest-priority activities

The prioritization of the asset based controls implementation is derived by the recovery priority of the critical asset -identified in phase 2- and the respective asset category. **As a rule of thumb the recovery priority of an asset characterizes the priority of the controls implementation.** An asset with a high recovery priority requires its controls to be implemented with a high priority. Equally, an asset with medium recovery priority leads to medium prioritization of the corresponding controls. However, **Facilities** asset category sets a high priority for the controls implementation irrespective to the assigned recovery priority. This is due to the fact that the corresponding continuity controls for this asset category (Annex B) involves the physical and environmental protection of an SME facilities (rooms, offices etc) which consequently protect personnel's health and safety. The table below presents an indicative assignment of the controls' implementation with respect to the recovery priority and the available asset categories:

Asset Based 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 7: Asset Based Controls Prioritization Matrix

The asset based controls prioritization can be assigned with three distinct values; **High, Medium** and **Low**. Each value implies a different timeframe for the control implementation; high priority controls should be implemented first, medium next and low last.

On the contrary, the implementation priority of organizational controls is performed in accordance with the risk level (high, medium, low) assigned to the predefined risk areas during phase 1. For example an organization with a **low** risk level in the legal and regulatory risk area will assign a **low** implementation priority for the controls dictated to this risk area. Likewise, the same organization may have a **high** risk level in the productivity risk area, selecting a **high** priority for the implementation of the organizational controls assigned to productivity risk area.

In addition, a set of criteria have been developed in order to assist the Assessment Team for prioritizing the implementation of the identified controls.

Following the output of all the previous phases, that is, risk profile definition, critical functions/assets identification and controls selection, **the Assessment Team ends up with the organization's Business Continuity Plan (BCP).**

Once the plan has been agreed it should be communicated to the organization's personnel. This will expose any flaws in the plan and will also ensure that all the roles and responsibilities are understood.

The Business Continuity Plan will address all requirements essential to keep the business running and includes processes to keep disruption to customers and employees to a minimum ensuring that a crisis is managed effectively before it escalates to a disaster.

The plan will focus on addressing the following business continuity aspects:

- Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permit the organization to recover its facility, data and assets.
- Identification of necessary resources to support Business Continuity Management on the long run, including personnel, information, equipment, financial allocations, infrastructure protection and accommodations.

5. Self Assessment Guidelines with one example

Most existing approaches to the assessment and management of continuity risks generally focus on the needs of large organizations. A simple approach designed for small organizations does not exist today, at least not in the form of publicly available guidelines.

The purpose of the present document is **to produce a tailored model to BCM implementation that can be utilized by SMEs,** including Micro-Enterprises.

The intent of the proposed BCM approach is to provide those organizations with a simple, efficient and inexpensive approach to identifying and managing their continuity risks. **The resulting simplified approach provides small organizations with a means to perform self-assessments.**

In this chapter, a more detailed breakdown of the four phases, described in section 4.4, of the proposed self-assessment BCM approach is presented in detail. Particularly the following phases along with the corresponding steps are described:

- **Phase 1: Select Risk Profile**
  - *Step 1: Identify Risk Areas*
  - *Step 2: Risk Profile Selection*
- **Phase 2: Critical Asset Identification**
  - *Step 1: Business Function Selection*
  - *Step 2: Select Asset Types*
  - *Step 3: Asset Continuity Requirements Analysis*
- **Phase 3: Controls Selection**
  - *Step 1: Select Organizational Control Cards*
  - *Step 2: Select Asset-Based Control Cards*
  - *Step 3: Document List of Selected Controls*
- **Phase 4: Implementation and Management**
  - *Step 1: Perform Gap Analysis*
  - *Step 2: Controls Implementation Plan*
  - *Step 3: Deliver Business Continuity Plan*

By performing the above phases and steps, an SME will:

- identify the risk profile of the organization with respect to the environment within which the company operates, (phase 1)
- identify the critical assets of the organization along with the dependant business functions, (phase 2)
- select continuity controls and solutions in order to achieve business continuity (phase 3) and finally,
- develop a BCP and a strategy for business continuity implementation and management (phase 4).

As mentioned above, the chapter is structured with phases and steps as the building blocks. One example is provided for every phase. The example uses the following company scenario:

Company Size: Micro Enterprise,

Number of Employees: 8 + 2 externals,

Type: Dental Equipment supplier,

Short Description: The company of the example is a dental equipment supplier based in north England. The company supplies both the equipment as well as their maintenance. Most of the customers have contracts of annual maintenance. In addition a significant percentage of the customers have special contracts for expedited repair in case of equipment breakdown. These special contracts guarantee a repair of the equipment within the next business day of filing the request when no spare parts replacement is required.

In the case where spare parts need to be replaced then the required maximum time to repair is four business days to allow for the shipment of spare parts from the manufacturer. In general no other special limitations and hard requirements exist for this company. The company employs 8 persons full time including the owner. Financial matters are handled by the owner with the support of the secretary and an external accountant. In addition the IT needs of the company are covered with external support from a local IT expert who is engaged on-demand to resolve problems that may arise or implement new solutions upon request.

Company Personnel		
	Employee	**Responsibilities**
1.	Company-Owner	Owns and runs the company, takes major decisions. Takes care of financial matters, customer relations, new products acquisition and dentist equipment technology updates
2.	Secretary	Supports the owner in financial matters. Receives orders for spare parts and equipment from other colleagues and sees to their fulfilment from the suppliers. In addition receives calls from new /prospective customers and assigns them to a salesman.
3.	Salesman1	Customer relationship agent that handles customer requests and sees to their fulfilment. His responsibilities also include the scheduling of expedited equipment repair under the special contract.
4.	Salesman2	Customer relationship agent that handles customer requests and sees to their fulfilment. His responsibilities also include the scheduling of expedited equipment repair under the special contract.
5.	Technician1	A senior technician responsible for new installations and training clients on equipment use, perform scheduled maintenance and repairs. He understands issues of technology and in many cases co-ordinates the executiom of IT related projects.
6.	Technician2	A junior technician supporting the senior for new installations and training clients on equipment use, perform scheduled maintenance and repairs. He is experienced enough to act independently in most situations and requires the support of the senior only in complex cases. Through his technical experience he can deal with some of the IT matters, but will always consult with the company's external IT expert.
7.	Van driver	Sees to the delivery of equipment and supplies to the customers
8.	Warehouseman	In charge of organising the company's supplies stock in the small ware house located on the basement of the office building. Occasionally may assist the van driver in delivering heavy or large equipment.
9.	Accountant (external)	Keeps financial records, handles taxation issues, and has responsibility for the issuing of financial reports. His is present at the premises a few times a month. Otherwise available on-call within business hours.
10.	IT expert (External)	On-call IT support within business hours, design and implementation of IT systems.

Table 8: Tabular information about involved roles in the example company

In the following discussion, figures (workflow diagrams) for every phase are also supplied; implementation hints for every step are provided in the dotted boxes for each of the forthcoming phase descriptions.

Phase 1 – Select Risk Profile

In phase 1, the Assessment Team considers a set of qualitative criteria from the business environment of the company to identify its risk context. The risk context is derived from the business, the internal and external environment of an organization and can be divided into four risk areas: **Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability**. The Assessment Team selects an appropriate risk level for each risk area using a predefined risk profile evaluation table. Finally the Assessment Team selects the organization's overall risk profile**.** As shown in figure 2, the phase involves two steps.

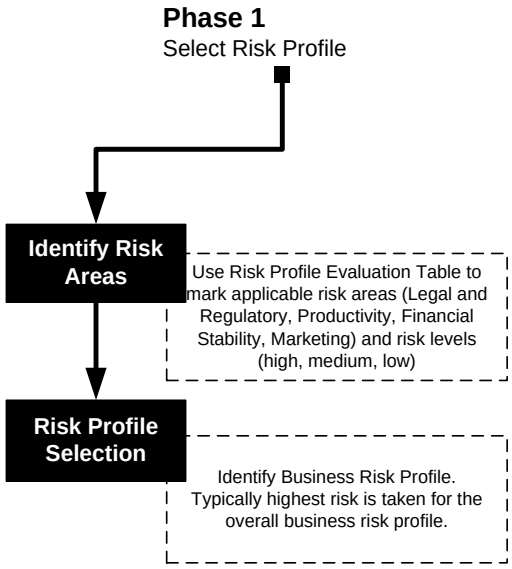

Figure 2: Phase 1 – Select Risk Profile Workflow

Step 1. Identify Risk Areas

During this step the Assessment Team determines the organization's business risk profile. This task is achieved through the Risk Profile Evaluation Table (Table 8) **by selecting risk areas** that can (a) directly or indirectly affect or damage reputation and customer confidence, (b) result in legal and regulatory non-compliance, (c) create financial loss and (d) decrease productivity. The team evaluates risks identified for every area in order to produce the **organization risk profile.** Each area is classified in three classes: High, Medium and Low. These classes represent qualitative criteria for the organization with respect to each risk area and help identify a risk level. In order to identify the current or potential risk level, Assessment Team members highlight the risk area and read the description in each column of the table. Risk areas that are closer to their business profile are chosen. The process is followed for every risk area. At the end there should be a Matrix highlighting the applicable risk level in each risk area.

Step 2. Risk Profile Selection

Based on the output of the previous step, the Assessment Team selects the organization's overall **risk profile**. The risk profile selection is performed via the highlighted Risk Profile Evaluation Table in a fairly straightforward manner: **The highest risk level identified in a risk area characterizes the overall business risk profile.** The identified risk levels in the predefined risk areas illustrate where the organization should focus its efforts to apply appropriate continuity controls and for setting implementation priorities.

Example (Micro Enterprise - Risk Profile: Low – Phase 1)

[Step 1] The Assessment Team uses the **Risk Profile Evaluation Table** to identify the risk context of the company. The Assessment Team proceeds by identifying:

- a low risk level in the legal and regulatory area since the company does not handle personal data other than those of the people employed by the organization,
- a low risk level in productivity since the business functions are not highly dependent on the information systems. Business workflows utilise information systems in a simple manner that is easy to perform manually
- a low risk level in financial stability since unavailability products will introduce no or marginal financial loss. This assessment is based on the average delivery time required by the customers and the low rate of occurrence of expedited service requests.
- a low risk level in reputation and loss of customer confidence is expected since currently information systems are not heavily used for customer interfaces.

The selected areas and level are shown in the following risk profile evaluation table.

Risk Areas	High	Medium	Low
Legal and Regulatory	The organization handles sensitive/personal customer information as defined by the EU Data Protection Law. 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. 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. Loss and / or destruction of the aforementioned data will lead to legal fines from Regulatory Bodies. 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. 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. 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. 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. 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. 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. 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. Yearly revenues are directly related to the continuous and uninterrupted provision of on-line services (i.e. sales are performed online). Unavailability of online presence will lead to direct financial loss as major services are provided by using e-business applications. Fines that may incur due to non-compliance with legal and regulatory requirements may lead to intolerable financial loss.	Unavailability of products and services of less than one day lead to a significant one time financial loss. Yearly revenues are indirectly related to the continuous and uninterrupted provision of online services (i.e. products and Services are supported with on-line services). 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.). Fines that may incur due to non-compliance with legal and regulatory requirements are possible but will not affect financial stability.	Unavailability of products and services of less than one day lead to no or marginal one time financial loss. Yearly revenues are not directly or indirectly related to the continuous and uninterrupted provision of on-line services. Unavailability of online presence 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.). 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 or service has direct impact on reputation, resulting thus in significant loss of customers using products and services though automated interfaces.	Unavailability or service has direct impact on reputation, resulting thus in considerable loss of customers using products and services though automated interfaces.	Unavailability or service cannot have impact on reputation, remaining thus unnoticed or marginally noticed by customers.

Table 9: Risk Profile Evaluation Table - Example

[Step 2] Next, the Business Risk Profile is calculated. Risk areas signify the overall business continuity risk context. **As a rule of thumb the highest risk identified in a risk class defines the overall business risk profile.**

Risk Areas	Risk Level	Risk Profile
Legal and Regulatory	**Low**	**Low**
Productivity	**Low**	
Financial Stability	**Low**	
Reputation and Loss of Customer Confidence	**Low**	

Table 10: Risk Profile Selection - Example

Phase 2 – Critical Asset Identification

During this phase, the Assessment Team selects critical business functions based on relative importance to the organization. Critical business functions are these functions whose interruption will lead to an SME's suffering from serious financial, legal, or other damages or penalties. **It should be noted that the earliest possible recovery of such functions after a disruption is the main objective of a Business Continuity Plan.**

Following the selection of the critical business functions, the organization will determine their dependencies in terms of the supporting assets used to provide each identified business function. Finally, based on the output of the previous steps the Assessment Team will analyze the continuity requirements of the identified critical assets.

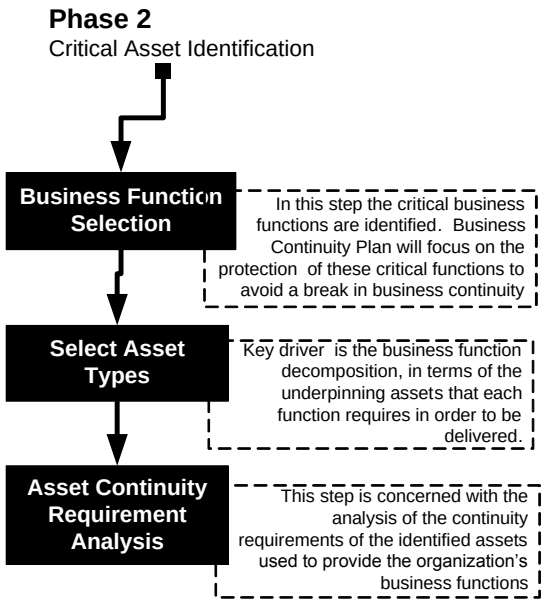

Figure 3: Phase 2 – Critical Assets Identification Workflow

Step 1. Business Function Selection

During the selection process of critical business functions, Assessment Team members should consider which functions will result in a large adverse impact on the organization in one of the following scenarios; (a) **Loss or destruction** of the business function or (b) **Interrupted access** to the function or to the information stored. The Assessment Team selects one or more of the following **business functions categories**[7] (here indicatively):

- **Production.**
- **Customer Relationship.**
- **Human Resource.**

[7] *Business functions categories can be further expanded or specialised by the Assessment Teams with respect to the organization's operating environment and the critical business functions used to fulfil the organization's business goals and objectives.*

- **Finance.**
- **New Product Acquisition / Development.**

In cases where the critical business functions are difficult to identify, teams should consider the assets inside the organization, as these are described in Table 2-Asset List.

Understanding why a function is critical can better enable the definition of the continuity requirements and **consequently the recovery priority of the function**. Capturing of this important information is facilitated by completing the critical business function profile card.

- **Critical business function Profile Card.** For each critical function, the following questions should be considered and answers recorded in the corresponding table:
  - Why is the business function critical to meeting the mission of the organization?
  - Who controls it?
  - Who is responsible for it?
  - Who uses it?
  - How is it used?

  These questions focus on how business functions are used and why they are important. If answers to all of these questions cannot be provided, people in the organization that can provide the answers must be located and included in the Assessment Team.

After defining the business functions that need to be secured the next step is to analyse and agree on the final list of critical business functions and the corresponding required recovery priorities. The outcome of this process will be documented using the "Critical Business Function List and Business Continuity Scope" form. With the completion of this step the scope of this business continuity assessment and of the resulting business continuity plan is set. The form requires filling the following information.

- **Rationale for selecting the business function.** While selecting critical business functions, a number of issues related to these functions are discussed. In this regard the rationale for selecting each critical function is documented for future reference during the decision making process.
- **The business function Recovery Priority[8] (High: less than 1 day, Medium: 1 to 3 days, Low: up to 5 days).** The business function recovery priority is the absolute maximum time that the function can be unavailable and the SME remain viable in order to avoid unacceptable consequences associated with a break in business continuity. In other words is the maximum period of time within which the function can be down before severe damage to the organization results. **In this regard the organization should restore the business function within this timeframe in order to remain viable.**

Step 2. Select Asset Types

Once the critical business functions are selected, the Assessment Team will identify their dependencies in terms of the assets used to provide and / or support the corporate business function. This activity reveals the dependencies between the various assets and the organization's business functions, identifying alternative methods for service delivery. **This will help the SME to focus its business continuity plan on the availability of the assets supporting critical business functions**. As an output, the Assessment Team should have a number of tables (one for each identified business function) listing all the assets used to provide / support the organization's business functions.

---

[8] *It is worth mentioning that these recovery priorities have been selected as indicative. According to the sector/requirements of an SME, these values may be adapted appropriately. For example a SME providing Value-Added Services (VAS) (i.e. call management services, mobile data services) may not be able to tolerate service unavailability more than few hours, as this could result in a major one-time financial loss affecting significantly business financial stability.*

Step 3. Asset Continuity Requirement Analysis

In Step 3 Assessment Teams are occupied with data gathering and analysis of the output produced in Steps 1 and 2 in order to define the continuity requirements of each identified asset. The data gathering and analysis is facilitated by the **Asset Identification Cards** which are distributed to organization's key personnel (asset owners). Answers to the following questions are required:

- What is the critical asset?
- Which critical business functions rely upon this asset?
- What is the agreed-upon description of this information asset?
- Who owns this asset[9]?
- What is the recovery priority of this asset[10]?

The Assessment Team will end up with an asset identification card for each identified asset. The cards will be used, later to **select the appropriate asset-based controls**.

Example (Micro Enterprise - Risk Profile: Low - Critical Business Function: Finance – Phase 2)

[Step 1] In our example the Assessment Team selects three functions: Finance - Medium priority, Customer Relationships - Medium priority and Expedited service contracts fulfilment – High priority. For this example we will follow closer the assessment process of the Finance function. As such detailed profiles and forms corresponding to the other functions will not be given, but the summary tables will include the output of the implied BCM processing.

The outcome of the discussion and selection of the recovery priorities is documented using the "Critical Business Function Identification and Business Continuity Scope" shown below. Now the team has a common understanding of what needs to be protected and what needs to be achieved in terms of recovery priorities. The agreed recovery priorities have to be updated in the corresponding critical business function profile cards.

Critical Business FunctionList – Business Continuity Scope		
Critical Business Function	Rationale for Selection	Recovery Priority (High, Medium, Low)
Production / Expedited service contracts fulfilment	Provides expedited equipment repair to customers that have purchased the expedited repair service. The repairs must be performed next business day when no spare parts are required. When spare parts need to be ordered then four business days is the defined maximum time to repair. The expedited repair service should be available for the customers in 1 day or less to maintain the agreed SLA.	High
Customer relationships	Receive communication and fulfil service requests of existing and new customers. The requests may range from new product information, equipment demonstrations, and requests for maintenance or repair at normal service level. Communication with our customers is important. Because of the many different means of communication we have (phone,	Medium

[9] *A business unit or individual being accountable and primary responsible for setting the requirements for the maintenance and physical and logical security of the asset as well assuring the requirements are met. Most often than not, the responsibility for the maintenance and security is delegated. Adapted from CMU/SEI-2005-TN-021*

[10] *It should be noted that assets inherit the recovery priority assigned to the critical business function during step 1.*

	email, fax, mobile phones) customers can be informed and postpone their service requiests for at least two days.	
Finance	This function is used to manage, store and process financial data generated by the commerce of medical equipment and services. The function is essential for the business as it represents the most important element of accounting information regarding purchase, invoicing and delivery of medical equipment. Most of the functions activities can be performed manually or delayed until information systems are available. Ordering spare parts required for the expedited service contracts fulfilment is the most time critical activity that must be recovered first.	Medium

Table 11: Critical Business Functions of example organisation

The assessment team completes the profiles of the identified functions and uses the information to finalise the selection and agree on the recovery priorities. The table below indicates the detail for the critical function "Finance".

Critical Business Function Profile Card			
Critical Business Function	Finance	Recovery Priority	Medium
Who controls the function	Company owner		
Who is responsible for delivering the function?	Company owner : funds management Secretary : orders & invoicing / scheduling of product deliveries Accountant : legal accounting obligations		
Who is the user? (Who benefits / needs this function? / why is it critical?)	This is a core function of the company used by almost every other function. The most demanding user is the **Expedited service contracts fulfilment** function that requires timely delivery of spare parts. **Customer Relationship Management** is also using the services of this function to fulfil customer orders. In addition prolonged unavailability of this function can starve the business from working capital.		
How is it used?	Orders are placed from customers through salesmen or technicians in the case of spare parts used for repairs. Currently internal emails are exchanged for placing orders. When prior arrangements (including credit) exist with suppliers the order is prepared and sent to the suppliers by the secretary without any further processing. The Orders depending on the supplier may need to be dispatched via FAX or Email and sometimes further details are worked out through phone calls. In other cases the company owner needs to secure a deal and supply adequate cash funds to support the order. The accountant updates/verifies the company records on a weekly basis and is available on call for urgent matters during business hours.		

Table 12: Detailsof the critical Business Function "Finance"

[Step 2] During step 2 the Assessment Team selects the dependant assets used to support / provide the selected critical business function. The team uses the Asset list hints provided here in combination with the business function profile created in the previous step. For each asset identified an asset identification card is created and populated with information in step 3. In this example the

team selects fifteen asset types from the respective Asset Categories: (a) Hardware, (b) Network, (c) Back-office Applications, (d) People and (e) Facilities.

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 services.	Server
		Laptop
		Workstation
		Storage
		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 non trusted networks.	Routers
		Gateways
		Switches
		Wireless Access Points
		Network Segment (e.g. cabling and equipment between two computers)
		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
		Information Technology Manager
		Database Development & Administration (manager, analyst, architect, administrator etc.)
		Programming / Software Engineering (manager, engineer, programmer, tester etc.)
		Technical Support (Help Desk Operator, technician etc.)
		Systems Analysis & Integration (manager, analyst, integrator, specialist etc.)
		Technical Writing (manager, writer, publication specialist etc.)
		Network Design & Administration (manager, analyst, architect, administrator, technician etc.)
		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	Financial Control
		Customer Care
		Logistics

	dependent business processes.	ERP
		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 13: Asset List - Example

As an output of this step the Assessment Team will fill the following form, identifying the supporting assets used to provide the organization's finance business function:

Critical Business Function Supporting IT Assets	
Critical Business Function	Finance
Supporting IT Assets	
Hardware	Secretary Desktop PC, Owner Laptop, Accountant Computer(in accountants office premises), Financial control application server
Network	Office Ethernet switch, Internet router
Back Office Application	Financial control, Email, office productivity applications,
Client Facing Applications	Internet Service provisioning, FAX, Company fixed-line phone
People /Contractors	Technician2, Company-Owner, Tecnician1, Secretary, warehouseman, External IT expert, Financial control software supplier
Data	Corporate Financial Data, supplier agreements and contact information, funding agreements, order progress tracking
Facilities	Company offices

Table 14: Business Function Supporting Assets – Example

Identifying Key Personnel and Contractors is one of the most important tasks if an effective response and recovery to an incident is to be prepared and executed. The owner of the critical business function has the overall responsibility to co-ordinate the restoration ans is in charge of key personnel. Personell involved in asset maintenance has also a role to play in when asset need to be recovered. For this reason even external contractors that have an operational responsibility (i.e. preferably a contractual obligation) for maintaining an asset must be included in this category. In the case of assets maintained by contractors, the asset owner is also important in the management of the recovery activities and has to be included in the list of critical people.

[Step 3] In Step 3 the Assessment Team continues with data gathering and analysis of the output produced in Steps 1 and 2. In our example the asset identification exercise revealed that the finance function depends on nineteen assets (Table 12). Thus, as an output of this step the Assessment Team will end up with nineteen asset identification cards, one for each asset. For this example only 7 cards will be presented.

Eventually no new assets will be discovered and the identification cards will contain all important information for the assets. The business function supporting IT assets card shown in table 12 needs to be amended accordingly to list any extra assets identified during this step.

Asset Identification Card	
Card Creation/Update Date	18/12/2009

Asset Category	Hardware
Asset Name	Financial control application server
Asset Description	This server holds the financial data and transactions. It hosts the financial control applications and allows the application's users to access /update the warehouse stock and issue invoices (If relevant include brand/model and vendor / supplier.)
Asset Owner	Company owner
Asset Location	Owner's office
Asset Maintainer	External IT Expert
Aggregated Recovery Priority	Medium
Supported Business Func#1	Finance
Assets role /usage in function	Provides the platform for the Financial control Application
Recovery Priority Requirement	Medium
Asset users	Company Owner, Accountant, Secretary. It is most of the time used remotely from their own computers.
Supported Business Func#2	-
Assets role /usage in function	
Recovery Priority Requirement	
Asset users	

Table 15: Financial control application server Asset Identification Card – Example

Asset Identification Card	
Card Creation/Update Date	18/12/2009
Asset Category	Application
Asset Name	Financial control application
Asset Description	The application that holds the financial data and transactions. Allows client to access /update the warehouse stock and issue invoices
Asset Owner	Company owner
Asset Location	Financial control application server
Asset Maintainer	Financial control software supplier
Aggregated Recovery Priority	Medium
Supported Business Func #1	Finance
Assets role /usage in function	Provides automation for the Finance function

Recovery Priority Requirement	Medium
Asset users	Company Owner, Accountant, Secretary. It is most of the time used remotely from their own computers.
Supported Business Func #2	-
Assets role /usage in function	
Recovery Priority Requirement	
Asset users	

Table 16: Financial Control Application Asset Identification Card – Example

Asset Identification Card	
Card Creation/Update Date	18/12/2009
Asset Category	Application
Asset Name	Email Service
Asset Description	Internet Email used for internal workflows and communication with customers, vendors, suppliers, Etc.
Asset Owner	Technician1
Asset Location	The Internet, Email Hosting Services LTD.
Asset Maintainer	Email Hosting Services LTD
Aggregated Recovery Priority	HIGH
Supported Business Func#1	Expedited Service Contract Fulfilment
Assets role /usage in function	Exchange documents, including spare part requests, service reports. Document exchanges are not time critical. When rapid action is required then phone communication is preceding the document exchange.
Recovery Priority Requirement	HIGH
Asset users	Technician1, Technician2
Supported Business Func#3	Finance
Assets role /usage in function	Supports internal workflow and external communication
Recovery Priority Requirement	Medium
Asset users	All function's users
Supported Business Func#3	Customer Relationship Management
Assets role /usage in function	Supports internal workflow and external communication
Recovery Priority Requirement	Medium
Asset users	All function's users

Table 17: Email Service Asset Identification Card – Example

Asset Identification Card	
Card Creation/Update Date	18/12/2009
Asset Category	Application
Asset Name	Company fixed-line phone numbers
Asset Description	Company fixed-line phones 0044 (0) 1223 234234 0044 (0) 1223 234235
Asset Owner	Secretary
Asset Location	The phone numbers are assigned to the Company-PBX
Asset Maintainer	The telephone company
Aggregated Recovery Priority	HIGH
Supported Business Func#1	Expedited Service Contract Fulfilment
Assets role /usage in function	Customers call to register their expedited support request
Recovery Priority Requirement	HIGH
Asset users	Customers, Salesman1, Salesman2
Supported Business Func#2	Finance
Assets role /usage in function	Same as office PBX
Recovery Priority Requirement	
Asset users	
Supported Business Func#3	Customer Relationship management
Assets role /usage in function	Same as office PBX
Recovery Priority Requirement	
Asset users	

Table 18: fixed-line phone numbers, Asset Identification Card – Example

Data Asset Identification Card	
Card Creation/Update Date	18/12/2009
Asset Category	Data
Asset Name	Order Progress Tracking
Asset Description	A spreadsheet for tracking the state of supplies and equipment requests placed by technicians and salesman.

Asset Owner	Company Owner
Asset Storage Location	Desktop-Secretary – C:\MyDocuments\
Asset Maintainer	Secretary
Aggregated Recovery Priority	Medium
Supported Business Func#1	Finance
Assets role /usage in function	Required for tracking order status for spare parts, supplies and equipment.
Recovery Priority Requirement	Medium
Asset users	Secretary

Table 19: Order Progress tracking, Asset Identification Card – Example

People / Suppliers Identification Card	
Card Creation/Update Date	18/12/2009
Name	External IT Expert
Organization and address (if not a company employee)	IT Valued Ltd.
Department	-
Title (Role)	-
Key BCM Responsibilities (If contractual obligations exist, put a reference to the contract)	
Office Telephone	+44 4556 445545
FAX	+44 4556 445546
Mobile	+44 4556 445547
Home Telephone	
E-mail	expert@itvalue.co.uk

Table 20: External IT Expert, Identification Card – Example

Facilities Identification Card	
Card Creation/Update Date	18/12/2009
Asset Category	Facilities
Asset Name	Company Offices
Asset Description	The operating location of the company. Includes offices, IT and warehouse

Asset Owner	Warehouse Man
Asset Location	12, Lisle st., Newcastle, UK
Asset Maintainer	Warehouse Man
Aggregated Recovery Priority	High (inherited by other critical functions)
Supported Business Func#1	Expedited Service Contract Fulfilment
Supported Business Func#2	Finance
Supported Business Func#3	Customer Relationship Management
Supported Business Func#4	
Supported Business Func#5	

Table 21: Offices Asset Identification Card – Example

When the Asset Identification cards are populated with information the Assessment Team can start analysing the recovery requirements for each asset based on how this is used by each critical function.

If there is evidence that a different recovery priority than the one inherited by the supported business function is needed, then the Assessment team may document the reasons and assign the new priority.

In addition, the Assessment Team might be willing to set more concrete recovery objectives, i.e. based on hours/days. This is a feasible option and will allow setting more clear requirements for the implementation of the controls that will be identified in the next phase. For example defining a recovery objective of 6 hours for an asset of High priority or 2 days for an asset of Medium priority will yield a more profound recovery order and more accurate implementation requirements.

The overview of the analysis results for the assets requirements for all critical business functions is summarized in the table given below. The Aggregated recovery priority will be used in the next phase to identify the appropriate control card for each asset.

IT Asset	**Function#1 Expedited Service Contract Fulfilment**	**Function#2 Finance**	**Function#3 Customer Relationship Management**	**Aggregated Recovery Priority**
Hardware				
Tech-Laptop1 (identical 2 tech-laptop2)	H			**H**
Tech-Laptop2 (identical 2 tech-laptop1)	H			**H**
Desktop-Sales1	H		M	H
Desktop-Sales2	H		M	H
Secretary Desktop PC		M		M
Owner Laptop,		M	M	M
Accountant Computer(in accountants office premises)		M		M
Financial control application server		M		M
Office Ethernet switch	H	M	M	H
Internet Router	H	M	M	H
Office-PBX	H	M	M	H

IT Asset	Function#1 Expedited Service Contract Fulfilment	Function#2 Finance	Function#3 Customer Relationship Management	Aggregated Recovery Priority
Back office Application				
Financial control App		M		**M**
Email	H	M	M	**H**
office productivity applications	H	M	M	**H**
Medical-Equipment-problem-diagnosis-application-vendor1	H			**H**
Medical-Equipment-problem-diagnosis-application-vendor2	H			**H**
Client Facing Application				
Company fixed-line phone	H	M	M	H
FAX		M		M
Technician Mobile phones	H			H
Salesmen mobile phones	H		M	H
Internet Service provisioning	H	M	M	H
web site			M	M
People / Suppliers				
External IT expert	H	M	M	H
Financial control software supplier		M		M
Technician2	H	M	M	H
PBX Supplier	H	M	M	H
Technician1	H	M	M	H
Secretary	H	M	M	H
Warehouseman	H	M	M	H
Company-Owner		M	M	M
Data				
Corporate Financial Data		M		M
supplier agreements and contact information		M		M
funding agreements		M		M
order progress tracking		M		M
Expedited Service Customer database	H			**H**
Technicians work Planning	H		M	**H**
Expedited Support/repair request reports	H			**H**
Medical equipment service manuals	H			**H**
Customer Request tracking database			M	**M**

IT Asset	Function#1 Expedited Service Contract Fulfilment	Function#2 Finance	Function#3 Customer Relationship Management	Aggregated Recovery Priority
Normal Support/repair request reports			M	**M**
Spare part requests	H		M	**H**
Medical equipment brochures and technical specifications			M	**M**
Facilities				
Company offices	H	M	M	**M**

Table 22: Asset Requirements Analysis Summary - Example

Phase 3 – Controls Selection

During Phase 3 the Assessment Team selects appropriate controls based on the risk profile selected for every risk category and the list of identified critical assets. Controls are separated in two Categories –(a) organizational continuity controls and (b) asset-based continuity controls.

Controls are further grouped in control cards. Two types of Continuity Control Cards are available for selection by the teams that carry the assessment of an SME:

- Controls cards that contain controls applicable to the organization horizontally and are concerned with practices and management procedures and
- Control cards that are applicable to critical assets and are asset-category-specific. Control cards are essentially pre-selected – grouped controls according to risk profiles and the asset recovery priority.

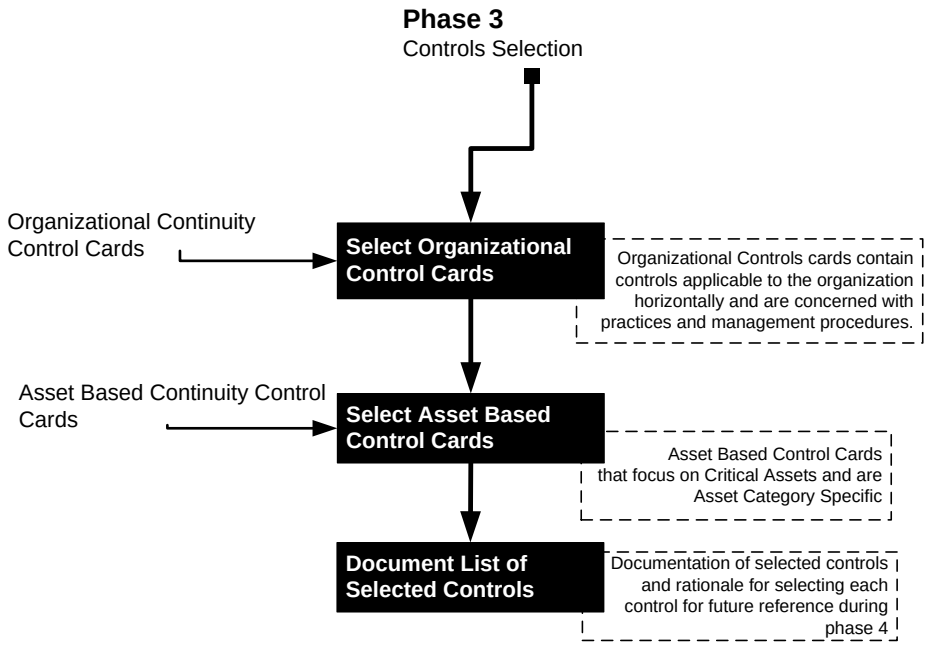

Figure 4: Phase 3 – Controls Selection Workflow

Step 1. Select Organization Continuity Controls

During this step, the Assessment Team selects organizational continuity control cards for the risk areas identified during phase 1 (Select Risk Profile) and thereby defines the direction for business continuity efforts in the organization. However, practical considerations will prevent SMEs from immediately implementing all of the initiatives after the evaluation. Organizations will likely have limited funds and staff members available to implement the protection strategy. After the evaluation, the Assessment Team prioritizes the activities in the protection strategy and then focuses on implementing the highest-priority activities (Phase 4: Implementation and Management). Organization Continuity Controls are available for every risk profile as defined in the Risk Profile Evaluation Matrix.

Step 2. Select Asset-Based Continuity Controls

Based on the organization's risk profile and the asset recovery priority (inherited by the respective critical business function) the Assessment Team shall use Asset Continuity Control Cards Table to identify the appropriate asset controls (see Annex B. Asset Based Continuity Control Cards). Asset control cards are essentially grouped in two categories, **corresponding to asset category and risk**

profile. For example Assessment Teams facing a high risk organization profile will have different business continuity requirements than medium or low risk profiles. Equally, controls cards will include more controls to address a higher range of risks and business continuity requirements.

Each asset-based control card involves a number of continuity controls to address the complete range of continuity risks for that asset, as needed for the particular risk profile. Furthermore, by taking into account the selected recovery priority, different control assignments are made. In addition, the asset control cards include the recovery actions that the organization should execute (after the disaster occurrence) in order to recover and resume critical business functions. The recovery actions selection is driven from the continuity control category and the respective continuity control.

Step 3. Document List of Selected Controls

While selecting control cards of critical assets in step 2, the Assessment Team will have to discuss issues related to these controls (e.g. rationale for selection, current implementation level, possible options for costs of control, etc.). In this step the team compiles a list including the selected controls and documents the rationale for selecting each control. By understanding controls, the team will be better able to define the appropriate action plans towards the development of the controls implementation plan during phase 4.

Example (Micro Enterprise - Risk Profile: Low - Critical Business Function: Finance – Phase 3)

[Step 1] In our example the organizational controls for a Low Legal and Regulatory risk level introduce continuity controls that are dictated by **SP1.1 and SP2.3** organizational controls. In the same way, a low risk in productivity risk class imposes a need for countermeasures and practices implied by **SP2.1, SP2.2 and SP5.2,** organizational controls. For low risk level in Financial Stability, **SP2.1 and SP5.2,** is dictated, and for Low risk level of Reputation and Loss Customer Confidence, **SP2.7.**

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP2) SP3.4 (SP4) SP5.1	SP1.1 (SP2) SP3.4 (SP4)	SP1.1 SP2.3
Productivity	(SP1) (SP2) (SP3) (SP4) (SP5)	(SP2) SP3.4 (SP4)	SP2.1 SP2.2 SP5.2
Financial Stability	(SP1) (SP2) (SP4)	(SP2) (SP4)	SP2.1 SP5.2
Reputation and Loss of Customer Confidence	(SP1) (SP2)	SP2.2 SP2.3	SP2.7

	(SP4)	(SP4)	
	SP3.4		

Table 23: Organizational Continuity Controls - Example

[Step 2] In step 2 the Assessment Team selects asset-based control card(s) using the asset-based continuity control cards table (table 22). In our example given the **low risk profile** of the organization identified in phase 1 and the critical asset types identified in Phase 2, step 2, they select card **CCC-3HN** for low profile hardware and network assets, **CCC-3A** card for low profile applications, and cards **CCC-3D and CCC-3F** for data and locations low profile assets respectively.

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 24: Asset Continuity Control Cards - Example

The cards selected (see Annex B) display the necessary controls for Hardware, Network, Application, Data and Facilities Assets operating at an organization **with a low risk profile**. The team identifies the controls that address the recovery priority identified in phase 2. In the example, Finance function has a **medium recovery priority**; thus the assets providing the function inherit the function's recovery priority. The following asset controls **HN.1.1.1 and HN.1.2.1** are selected for hardware and network assets addressing resilience and backup continuity requirements for these assets (Table 23). In accordance with the selected continuity controls the respective recovery action **RA.1.2.1** is selected, to achieve the recovery of the organization's assets. Equally, the Assessment Team selects the appropriate asset controls and recovery actions for Application, Data and Facilities assets as these are depicted into tables 24, 25 and 26.

Asset Based Continuity Control Card ID		**CCC-3HN**		
Risk Profile		**Low**		
Asset Category		**Hardware and Network**		
Continuity Controls Category		**Resilience**	**Back up**	**Redundancy**
Recovery Priority	**High**	**HN.1.1.1 - HN.1.1.7**	**HN.1.2.1 - HN.1.2.5**	**HN.1.3.3**
	Medium	**HN.1.1.1**	**HN.1.2.1**	-
	Low	**HN.1.1.1**	**HN.1.2.1**	-
Recovery Actions		-	**RA.1.2.1**	

Table 25: CCC-3HN Asset based control card - Example

Asset Based Continuity Control Card ID		CCC-3A	
Risk Profile		Low	
Asset Category		Application	
Continuity Controls Category		Application Resilience	Application Back up
Recovery Priority	High	A.1.1.1 - A.1.1.3 - A.1.1.4 A.1.1.6	A.1.2.1 - A.1.2.2
	Medium	A.1.1.1 - A.1.1.4	A.1.2.1 - A.1.2.2
	Low	A.1.1.1	A.1.2.1 - A.1.2.2
Recovery Actions		RA.1.1.3 - RA.1.1.6	RA.1.2.1

Table 26: CCC-3A Asset based control card - Example

Asset Based Continuity Control Card ID		CCC-3D	
Risk Profile		Low	
Asset Category		Data	
Continuity Controls Category		Data Storage	Data back up
Recovery Priority	High	D.1.1.1 - D.1.1.5	D.1.2.1 - D.1.2.3 - D.1.2.5
	Medium	D.1.1.5	D.1.2.1 - D.1.2.5
	Low	D.1.1.5	D.1.2.1
Recovery Actions		RA.1.1.1 - RA.1.1.5	RA.1.2.5

Table 27: CCC-3D Asset based control card - Example

Asset Based Continuity Control Card ID		CCC-3F		
Risk Profile		Low		
Asset Category		Facilities		
Continuity Controls Category	IT Site	Environmental Security	Physical Security	

Recovery Priority	High	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4	F.1.2.2 - F.1.2.3 F.1.2.4	F.1.3.4 - F.1.3.5 F.1.3.6
	Medium	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4	F.1.2.2 - F.1.2.3	F.1.3.5 - F.1.3.6
	Low	F.1.1.2 - F.1.1.3 F.1.1.4	F.1.2.2 - F.1.2.3	-
Recovery Actions		-	-	-

Table 28: CCC-3F Asset based control card – Example

The full listing of assets and the corresponding assect based control cards is summarisied in the following table.

IT Asset	Aggregated Recovery Priority	Selected Asset Based Control Cards
Hardware		
Tech-Laptop1 (identical 2 tech-laptop2)	H	CCC-3HN
Tech-Laptop2 (identical 2 tech-laptop2)	H	CCC-3HN
Desktop-Sales1	H	CCC-3HN
Desktop-Sales2	H	CCC-3HN
Secretary Desktop PC	M	CCC-3HN
Owner Laptop,	M	CCC-3HN
Accountant Computer(in accountants office premises)	M	CCC-3HN
Financial control application server	M	CCC-3HN
Office Ethernet switch	H	CCC-3HN
Internet Router	M	CCC-3HN
Office-PBX	H	CCC-3HN
Back office Application		
Financial control	**M**	CCC-3A
Email	**H**	CCC-3A
office productivity applications	**H**	CCC-3A
Medical-Equipment-problem-diagnosis-application-vendor1	**H**	CCC-3A

IT Asset	Aggregated Recovery Priority	Selected Asset Based Control Cards
Medical-Equipment-problem-diagnosis-application-vendor2	**H**	CCC-3A
Client Facing Application		
Company fixed-line phone	H	CCC-3A
FAX	M	CCC-3A
Technician Mobile phones	H	CCC-3A
Salesmen mobile phones	H	CCC-3A
Internet Service provisioning	M	CCC-3A
web site	M	CCC-3A
People / Suppliers		
External IT expert	H	CCC-3P
Financial control software supplier	M	CCC-3P
Technician2	H	CCC-3P
PBX Suppplier	H	CCC-3P
Technician1	H	CCC-3P
Secretary	H	CCC-3P
Warehouseman	H	CCC-3P
Company-Owner	M	CCC-3P
Data		
Corporate Financial Data	M	CCC-3D
supplier agreements and contact information	M	CCC-3D
funding agreements	M	CCC-3D
order progress tracking	M	CCC-3D
Expedited Service Customer database	**H**	CCC-3D
Technicians work Planning	**H**	CCC-3D
Expedited Support/repair request reports	**H**	CCC-3D
Spare part requests	**H**	CCC-3D
Medical equipment service manuals	**H**	CCC-3D
Customer Request tracking database	**M**	CCC-3D
Normal Support/repair request reports	**M**	CCC-3D

IT Asset	Aggregated Recovery Priority	Selected Asset Based Control Cards
Medical equipment brochures and technical specifications	**M**	CCC-3D
Facilities		
Company offices	**M**	CCC-3F

Table 29: Asset Based Control Card Summary

[Step 3] In this step Assessment Teams are occupied with data gathering and analysis of the output produced in Steps 1 and 2. Documenting the output of previous steps, both the selected asset-based controls and the organizational controls are then listed in the tables below.

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
HN.1.1.1	Tech-Laptop1	**H**	IT Infrastructure Documentation There is an up-to-date and detailed IT infrastructure diagram including network and hardware components.
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control application server	**M**	
HN.1.1.5	Tech-Laptop1	**H**	Disaster Recovery Cross Training No critical hardware or network component depends on an individual person for restoration in a disaster**.**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.1.7	Tech-Laptop1	**H**	Information Systems Hardening Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.2.1	Tech-Laptop1	**H**	Information Systems Backup Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control	**M**	

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
	application server		must be retained in good working condition.
HN.1.2.5	Tech-Laptop1	**H**	Staff Training Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.3.3	Tech-Laptop1	**H**	Vendors SLAs The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.
	Desktop-Sales1	**H**	
	Office PBX	**H**	

Table 30: List of Hardware Selected Controls – Example

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
A.1.1.1	Email Service	**H**	Application Documentation. The control requires the organization to document the required environment (OS version, external libraries, etc) for the execution of the application. This documentation has to be verified and updated at every maintenance cycle of the BCP.Furthermore, if the application is custom the application code should be documented. The criticality of the application will dictate the level of documentation required.
	Company fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
	Financial control	**M**	
	Internet Service provisioning	**M**	
A.1.1.3	Email Service	**H**	Application Configuration Management A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.
	Company fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
A.1.1.4	Email Service	**H**	Application Maintenance and Patching Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.
	Company fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
	Financial control	**M**	
	Internet Service provisioning	**M**	
A.1.1.6	Email Service	**H**	Application Vendors & SLAs. The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented agreement exists between the two parties for technical support provisioning when required.
	fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
A.1.2.1	Email Service	**H**	Application Backup

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
	fixed-line phone	**H**	Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules. When this control is applied to a service (such as email or internet provisioning) then establishing an alternate backup service is required in addition to backing up any relevant data. When considering backup of services that produce or store data the ability to have a usable local copy of the data or to transfer existing data to the backup service has to be considered and evaluated.
	Salesmen mobile phones	**H**	
	Financial control	**M**	
	Internet Service provisioning	**M**	

Table 31: List of Application Selected Controls – Example

Data - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
D.1.1.1	Spare part requests	**H**	Data Mirroring The control requires that all critical data are mirrored to additional storage media ensuring that data is written to two or more different disks (disk mirroring / raid array configuration) to ensure that two valid copies of the data are available.
D.1.1.5	Spare part requests	**H**	Store Backup Media Offsite Backup media should be labelled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.1	Spare part requests	**H**	Backup Rotation Schedules The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.3	Spare part requests	**H**	Backup System Flexibility The backup system should allow quick and flexible restoration of files, folders, partitions, mailboxes/messages and databases/tables. It should be possible to schedule restoration of data according to the pre-determined recovery priority. This is to be utilised when the time to restore the full datasets exceeds the target recovery times. Design your backup plan to meet the precise restoration time objectives. Order the backup sequence according to your recovery sequence to avoid time costly seeks on tapes. Create a precise map of the contents of each tape. If possible clone the backup sets to a hard disk storage to increase the speed of restoration.
D.1.2.4	Spare part requests	**H**	Internet Backup The control requires that workstation users (personnel) are allowed to back up data to a remote location over the Internet. Formal authorisation is required prior to the execution of this backup method.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	

Data - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
D.1.2.5	Spare part requests	**H**	Data Backup Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	

Table 32: List of Data Selected Controls – Example

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
P.1.1.2	External IT expert Technician2 PBX Suppplier Technician1 Secretary WarehouseMan	**H**	Physical Access Control Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.
P.1.1.3	External IT expert Technician2 PBX Suppplier Technician1 Secretary WarehouseMan	**H**	Clean Desk Policy A clean desk policy is in operation followed by all personnel, contactors and third parties
P.1.2.1	External IT expert Technician2 PBX Suppplier Technician1 Secretary WarehouseMan	**H**	Business Continuity Tool Set The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.
P.1.2.2	External IT expert Technician2 PBX Suppplier Technician1 Secretary WarehouseMan	**H**	Business Continuity Tests Staff, have been trained and involved in business continuity tests.
P.1.2.3	External IT expert Technician2 PBX Suppplier Technician1 Secretary	**H**	Key Personnel Deputies All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfil their duties / responsibilities.

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
	WarehouseMan		
P.1.2.4	External IT expert Technician2 PBX Suppplier Technician1 Secretary WarehouseMan	**H**	Key IT Personnel Training The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a "business as usual" basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures
	Financial control software supplier Company-Owner	**M**	

Table 33: List of People Selected Controls – Example

Facilities - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
F.1.1.1	Company offices	**H**	IT Site Physical Access Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or similar physical access control technologies.
F.1.1.2	Company offices	**H**	IT Site Power Supply The power supply of the site equipment is protected with UPS and / or generators.
F.1.1.3	Company offices	**H**	IT Site Air-Conditioning IT site humidity, ventilation and air-conditioning are controlled.
F.1.1.4	Company offices	**H**	IT Site Anti-fire Systems Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.
F.1.1.7	Company offices	**H**	IT Site Recovery Plan Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.
F.1.2.2	Company offices	**H**	Fire Fighting Equipment Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within corporate facilities
F.1.2.3	Company offices	**H**	Air-conditioning The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.
F.1.2.4	Company offices	**H**	Anti-flood Equipment There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.
F.1.3.4	Company offices	**H**	Rooms and Areas Secure Access Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to

Facilities - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Rationale for Selection**
			authorised personnel.

Table 34: List of Facilities Selected Controls – Example

Organizational Continuity Controls		
SP.1.1	**Dental Equipment Company**	A policy should be developed which will set a framework towards business continuity.
SP2.1	**Dental Equipment Company**	A business continuity plan should exist for the management of business continuity incidents.
SP2.2	**Dental Equipment Company**	An incident response procedure should exist for the proper handling of security incidents.
SP2.3	**Dental Equipment Company**	Emergency procedures will be developed for the health & safety of the organization's personnel.
SP2.7	**Dental Equipment Company**	The organisation has established diverse communication channels that clients and third parties can use to contact the organisation, request service or report a problem. These arrangements are part of the business as usual and no special actions are needed for their activation. Such communication channels may be land line phone numbers, mobile phone numbers, voice mailboxes, email and FAX from diverse providers to avoid single points of failure.
SP5.2	**Dental Equipment Company**	The organization has verified that outsourced security services, mechanisms, and technologies meet its business continuity needs and requirements. Business continuity requirements on providers are included in formal terms in the contract.

Table 35: List of Selected Organizational Controls – Example

Phase 4 – Implementation & Management

During Phase 4 the Assessment Team performs a gap analysis exercise in order to evaluate the organization's current state against the selected continuity controls, both organizational and asset grouped within the respective control cards. Following this, the Assessment Team develops the controls **Implementation Plan** which includes the controls that will be implemented, as well as the prioritization for their integration into the organization.

Finally the Assessment Team based on the information collected and assessed during the execution of the previous phases and steps, creates the Business Continuity Plan to address the continuity risks.

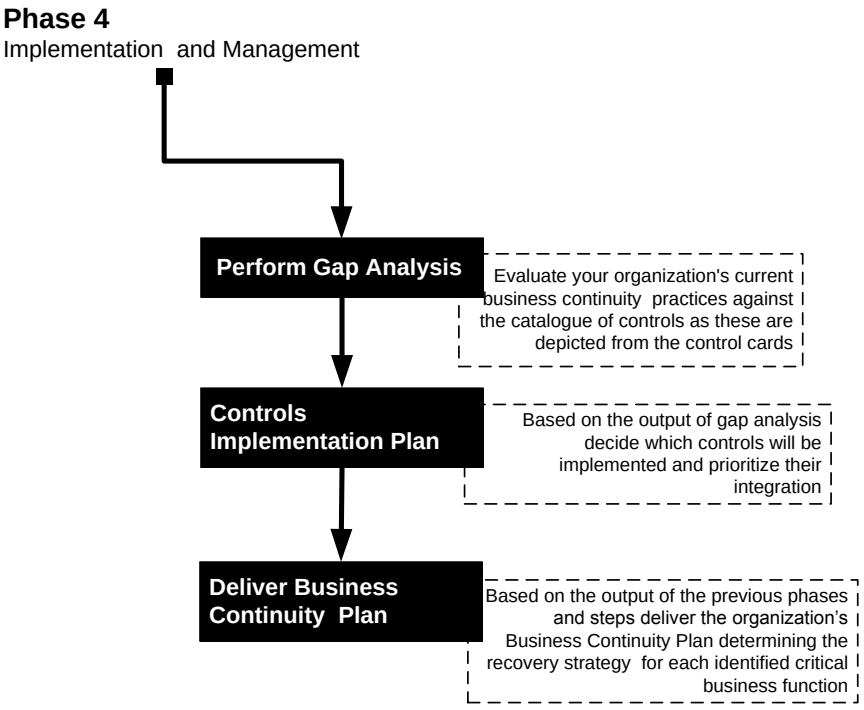

Figure 5: Phase 3 – Controls Selection Workflow

Step 1. Perform Gap Analysis

In this step Assessment Teams are occupied with the evaluation of the organization's current business continuity practices compared to controls described on the selected control cards. Assessment Teams carefully read controls that apply to their profile (as depicted from the selected control cards - Phase 3, Step 3) and elicit detailed information about the organization's current continuity policies, procedures, and practices, thus providing a starting point for improvement.

During the Gap Analysis process teams use the control cards as the "continuity requirements" and assess the gaps between these and current business continuity practices both at an organizational and critical asset level.

The output from this process can form the basis for the planning activity that follows next. It is separated into two categories: **(a) Organizational Continuity Controls**, where the Assessment Teams should identify the suggested practices that are already implemented and the ones not implemented. Then actions for improvement at an organizational level can be defined and **(b) Asset Based Continuity Controls** where Assessment Teams assess existing protection measures for the identified critical assets.

Step 2. Controls Implementation Plan

In this step the Assessment Team considers whether the organization will implement or not the continuity controls found missing during the gap analysis exercise. This task is achieved by the Assessment Team recording its answer to this question: What is required in terms of resources and changes in order to implement the selected controls? The team discusses the operational aspects of each control considering the following questions for each one.

- Who should implement it?
- Who should be responsible for it?
- Who should benefit from it?
- How should it be implemented?

These questions focus on how continuity controls should be used and why they are important. If the team can't answer all of these questions, it may need to ask people in the organization who can answer them. The information that will be identified by answering these questions will be useful later on when the implementation plan of the controls will be developed.

The output of this activity is the continuity controls **Action List** which **leads to a series of actions** that an organization should undertake to improve its existing level of business continuity.

Since specific actions / steps have been identified, the team develops the controls **Implementation Plan** assigning responsibility for completing them as well as a completion date and the **implementation priority**.

The following questions should be answered for each action item on the list and record the results:

- Who will be responsible for each action item?
- By what date does the action item need to be addressed?
- What can management do to facilitate the completion of this action item?
- How much will it cost?
- How long will it take?
- Can we do it ourselves?
- Do we need external assistance?

The actions prioritization for the implementation of organizational continuity controls is performed in accordance with the risk level (high, medium, low) assigned to the predefined risk areas during phase 1. For example an organization with a **low** risk level in the legal and regulatory risk area will assign a **low** implementation priority for the actions that should be executed towards the implementation of the controls dictated to this risk area. Likewise, the same organization may have a **high** risk level in the productivity risk area, assigning a **high** priority for the actions implementation.

On the contrary, the prioritization of the asset based controls implementation is derived by the recovery priority of the critical asset - identified in phase 2- and the respective asset category.

The asset based controls prioritization can be assigned with three distinct values: **High, Medium** and **Low**. Each value implies a different timeframe for the control implementation; high priority controls should be implemented first, medium next and low last.

It should be noted that **the SME should implement all the controls (both organizational and asset based) as soon as possible.** The aforementioned prioritization methods should be **followed in case that the SME is not able to implement all the controls at once due to limited resources** (manpower, budget etc).

It is worth mentioning that the implementation priority of the controls may be influenced by a number of key factors / criteria. These criteria should be counted in by the Assessment Team during the controls prioritization since they can significantly change the controls implementation priority derived by the method presented above. Bellow some additional criteria for prioritizing actions for implementing identified controls can be found:

- **Personnel life health and safety:** People are the most valuable assets within an organization. In this regard health and safety the personnel should be ensured assigning high priority to the implementation of controls referring to environmental and physical security issues.
- **Strategic alignment with organization goals:** Does this business function directly support documented organization and/or divisional work plan goals? What goals and/or work plan objectives will be supported and how?
- **Legal and Regulatory requirements:** If a business function is necessary to meet legal and regulatory requirements, this will be reflected in setting priorities. The organization should also consider Health and Safety legal requirements as these are established by the Legal and Regulatory Framework of the country in which the SME operates.
- **System-wide benefits:** System-wide benefits include improved customer service for several customer groups. A higher priority will be given to customer groups that are considered critical, but the larger the customer group affected the greater the benefit.
- **Cost/Time Savings:** Estimates of cost and/or time savings include staff time, customer time savings, revenue generation, and direct budget/cost reductions.
- **Continuity Risk Reduction:** As result of a project, information and/or services will prevent lost revenues and/or non-compliance with policies, legal, and audit requirements.

Step 3. Deliver Business Continuity Plan

As an output of the above phases and steps **the Assessment Team will derive with the organization's Business Continuity Plan (BCP).** The BCP will include the following sections: (1) BCP Governance, (2) The results of Self-Assessment Approach from all performed phases, (3) Plans, processes, measures, and arrangements for business continuity, (4) Quality assurance techniques (change management, exercises, maintenance and auditing). (5) Annexes with documentation and usage Instructions for the implemented controls. The Assessment Team fills in the template's sections based on the output of the previous phases and steps deriving with the organization's Business Continuity Plan.

The plan will form the organization's strategy regarding business continuity addressing the following business continuity requirements:

- Business continuity processes and plans (.i.e. Disaster Recovery Plan, Incident Management Procedure)
- Contact List(s) with business continuity responsible employees / teams / managers
- Business Continuity Team roles and responsibilities.
- List of Critical Business Functions
- The continuity controls that the organization uses in order to protect the continuity of the critical business functions / assets
- Activities for Testing Reassessing and Maintaining Business Continuity Plan
- Contact details of vendors / suppliers committed to supporting the recovery efforts
- Resource requirements (people, work area, IT, telecommunications)
- Contact List of Governmental authorities / bodies

Example (Micro Enterprise - Risk Profile: Low - Critical Business Function: Finance – Phase 4)

[Step 1] In this step Assessment Teams are occupied with the evaluation of the organization's current business continuity practices compared to controls described on control cards. Assessment Teams carefully read controls that apply to their profile (as depicted from the selected control cards - Phase 3, Step 3) and elicit detailed information about the organization's current continuity policies, procedures, and practices, thus providing a starting point for improvement.

The following Table refers to the Example:

Organizational Continuity Controls			
Control	**Asset**	**Control Description**	**Do we currently follow the controls included in the control cards?**
SP.1.1	**Dental Equipment Company**	A policy should be developed which will set a framework towards business continuity.	No
SP2.1	**Dental Equipment Company**	A business continuity plan should exist for the management of business continuity incidents.	No
SP2.2	**Dental Equipment Company**	An incident response procedure should exist for the proper handling of security incidents.	No
SP2.3	**Dental Equipment Company**	Emergency procedures will be developed for the health & safety of the organization's personnel.	Yes. We must align our plans with the upcoming business continuity plan
SP2.7	**Dental Equipment Company**	The organisation has established diverse communication channels that clients and third parties can use to contact the organisation, request service or report a problem. These arrangements are part of the business as usual and no special actions are needed for their activation. Such communication channels may be land line phone numbers, mobile phone numbers, voice mailboxes, email and FAX from diverse providers to avoid single points of failure.	Partially yes. We have diverse means of communication. Mobiles, land line, FAX, email. We are at present unsure about the diversity of suppliers for these services. It might be we are getting all the services from a single supplier or a subsidiary.
SP5.2	**Dental Equipment Company**	The organization has verified that outsourced security services, mechanisms, and technologies meet its business continuity needs and requirements. Business continuity requirements on providers are included in formal terms in the contract.	No

Table 36: Organizational Controls Gap Analysis List – Example

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
HN.1.1.1	Tech-Laptop1	**H**	No
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control application server	**M**	

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
HN.1.1.5	Tech-Laptop1	**H**	No
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.1.7	Tech-Laptop1	**H**	Partially. In some systems automatic updates are used.
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.2.1	Tech-Laptop1	**H**	No
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control application server	**M**	
HN.1.2.5	Tech-Laptop1	**H**	No
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.3.3	Tech-Laptop1	**H**	Partially. We have an SLA for next business day laptop repair. The office-PBX is under a three business days repair contract.
	Desktop-Sales1	**H**	
	Office PBX	**H**	

Table 37: Hardware Gap Analysis List – Example

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
A.1.1.1	Email Service	**H**	Partially, No custom application code is developed in the company. In general environment documentation for the applications is available in the vendor documents. But the information is not updated with new versions or patches of the software.
	Company fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
	Financial control	**M**	
	Internet Service provisioning	**M**	

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
A.1.1.3	Email Service	**H**	Not Applicable. The specs of the service availability are handled in the contract.
	Company fixed-line phone	**H**	Not Applicable. The specs of the service availability are handled in the contract.
	Salesmen mobile phones	**H**	No. Mobile phones are configured and applications can be installed by their users.
A.1.1.4	Email Service	**H**	Not Applicable. The specs of the service availability are handled in the contract.
	Company fixed-line phone	**H**	Not Applicable. The specs of the service availability are handled in the contract.
	Salesmen mobile phones	**H**	No. Mobile phones are configured and applications can be installed by their users.
	Financial control	**M**	Yes. Maintenance and patching is responsibility of the application vendor under the maintenance contract
	Internet Service provisioning	**M**	No.
A.1.1.6	Email Service	**H**	Yes
	fixed-line phone	**H**	Partially. We have the standard level support of the telephone company
	Salesmen mobile phones	**H**	No
A.1.2.1	Email Service	**H**	Yes backup of emails is part of the service
	fixed-line phone	**H**	No
	Salesmen mobile phones	**H**	No
	Financial control	**M**	Partially. Backups are performed by the vendor. We have not verified restoration though.
	Internet Service provisioning	**M**	No backup arrangements exist.

Table 38: Application Gap Analysis List – Example

Data - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
D.1.1.1	Spare part requests	**H**	No
D.1.1.5	Spare part requests	**H**	No.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.1	Spare part requests	**H**	Partially. Backups are responsibilities of employees. They are currently encouraged to backup a few times a week using their usb flash disks.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.3	Spare part requests	**H**	No.

Data - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
D.1.2.4	Spare part requests	**H**	No
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.5	Spare part requests	**H**	No
	Corporate Financial Data	**M**	
	order progress tracking	**M**	

Table 39: Data Gap Analysis List – Example

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
P.1.1.2	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHousaMan	**H**	No
P.1.1.3	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHousaMan	**H**	No
P.1.2.1	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHousaMan	**H**	No.
P.1.2.2	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHousaMan	**H**	No
P.1.2.3	External IT expert Technician2	**H**	No

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
	PBX Supplier Technician1 Secretary WareHousaMan		
P.1.2.4	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHousaMan	**H**	No
	Financial control software supplier Company Owner	**M**	

Table 40: People Gap Analysis List – Example

Facilities - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Do we currently follow the controls included in the control cards?**
F.1.1.1	Company offices	**H**	No. IT systems are dispersed in employee offices. Locking is not possible
F.1.1.2	Company offices	**H**	Partially. A UPS is installed for most of the IT equipment.
F.1.1.3	Company offices	**H**	Partially. Air-conditioning is controlled to human comfort levels.
F.1.1.4	Company offices	**H**	Fire detection is in-place.
F.1.1.7	Company offices	**H**	No.
F.1.2.2	Company offices	**H**	Partially. Fire fighting equipment is not selected to avoid damaging technology equipment.
F.1.2.3	Company offices	**H**	No. Auto shut off is not present.
F.1.2.4	Company offices	**H**	No. Our location is not prone to flooding.
F.1.3.4	Company offices	**H**	No. Only the warehouse is kept always locked.

Table 41: Facilities Gap Analysis List – Example

[Step 2] Following the gap analysis, Assessment Team reads the controls (Annex A, B) and decides whether the organization will implement or not the continuity controls. The Assessment Team documents the necessary actions towards the implementation of the continuity controls:

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

Organizational Continuity Controls			
Control	**Asset**	**Control Description**	**Activity needed, Outcome expected, Deliverable Documentation**
SP.1.1	**Dental Equipment Company**	A policy should be developed which will set a framework towards business continuity.	A policy shall be developed. The business continuity policy document will be made available to all employees. **Deliverable: Business Continuity Policy Document**
SP2.1	**Dental Equipment Company**	A business continuity plan should exist for the management of business continuity incidents.	A business continuity plan will be developed and documented. All the individuals with roles in the plan will receive their copy. Updates of the document will be distributed on every maintenance cycle of the BCP. **Deliverable: Business Continuity Plan Document**
SP2.2	**Dental Equipment Company**	An incident response procedure should exist for the proper handling of security incidents.	Incident response procedure will be drafted relevant to the know-how and expertise available for response within the company. **Deliverable: Incident Response Procedure – as a part of BCP document**
SP2.3	**Dental Equipment Company**	Emergency procedures will be developed for the health & safety of the organization's personnel.	Yes. We must align our plans with the upcoming business continuity plan. **Deliverable: Updated Emergency procedures document, attached to BCP**
SP2.7	**Dental Equipment Company**	The organisation has established diverse communication channels that clients and third parties can use to contact the organisation, request service or report a problem. These arrangements are part of the business as usual and no special actions are needed for their activation. Such communication channels may be land line phone numbers, mobile phone numbers, voice mailboxes, email and FAX from diverse providers to avoid single points of failure.	Establish a policy of communication channel diversity. The communication service used by the company will be documented including adequate supplier information. The following rules must be followed: 1) All customers and suppliers are aware of at least two points of contact with the company. These points of contact must be using different communication technologies. (e.g.: mobile phones and email) 2) At least one of the communication channels used as a point of contact must be supplied to the company through an independent supplier having no subsidiary relation to the dominant communications supplier of the company (if any). **Deliverable: Communication channel diversity policy (attached to the procurement policies)** **Deliverable: Communication channel map (attached to the BCP and to the procurement policies)**
SP5.2	**Dental Equipment Company**	The organization has verified that outsourced security services, mechanisms, and technologies meet its business continuity needs and requirements. Business continuity requirements on providers are included in formal terms in the contract.	The organisation will use the business continuity assessment results to identify the terms to be included when procuring relevant services. Where such terms are agreed a relevant business continuity testing capability must also be present. **Deliverable: Policy of business continuity requirements in contracts (attached to the procurement policies)**

Table 42: Organizational Controls Gap Analysis List – Example

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
HN.1.1.1	Tech-Laptop1	**H**	A detailed documentation of the IT Infrastructure in the form of diagrams will be created. The diagrams will be including the network and hardware components. **Deliverable: IT Infrastructure Diagrams (to be attached to the BCP)**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control application server	**M**	
HN.1.1.5	Tech-Laptop1	**H**	The company personnel is not adequate to provide for complete disaster recovery cross training. Where practical alternate external contractors will be identified. **Deliverable: Disaster Recovery Cross Training Matrix (To be attached to the BCP)**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.1.7	Tech-Laptop1	**H**	All devices that support automatic security updates will be configured to use this feature by default. A list of Systems exposed to the internet that don't have an automatic update feature will be created. Periodic hardening by our IT expert will be considered as an option, probably with the support of a government or commercial Computer Emergency Response Team. **Deliverable: Information Systems Hardening Report, once per BCP maintenance cycle**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.2.1	Tech-Laptop1	**H**	Information Systems Backup will be implemented. **Deliverable: Backup Plan (to be attached to the BCP)**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
	Secretary Desktop PC	**M**	
	Accountant Computer	**M**	
	Financial control application server	**M**	
HN.1.2.5	Tech-Laptop1	**H**	Training will be implemented. **Deliverable: Training Schedule and implementation records**
	Desktop-Sales1	**H**	
	Office PBX	**H**	
HN.1.3.3	Tech-Laptop1	**H**	In addition to the existing contracts the following action will be taken: 1) Maintain a list of suppliers for commodity hardware that can be easily obtained within 1 business day. 2) Sign an expedited provisioning agreement for hardware not widely available
	Desktop-Sales1	**H**	
	Office PBX	**H**	

Hardware Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
			or required to be available in less than a day. Existing Contracts: We have an SLA for next business day laptop repair. The office-PBX is under a three business days repair contract. **Deliverable: Vendor SLAs for expedited repair or provisioning (attached to the BCP)**

Table 43: Hardware Actions List – Example

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
A.1.1.1	Email Service	**H**	Relevant documentation will be identified collected and be available for reference. The documentation collected will have to be useful in restoring and using the application during a business continuity incident. **Deliverable: Critical Application reference documentation index (attached to the BCP)**
	Company fixed-line phone	**H**	
	Salesmen mobile phones	**H**	
	Financial control	**M**	
	Internet Service provisioning	**M**	
A.1.1.3	Email Service	**H**	No action
	Company fixed-line phone	**H**	No action
	Salesmen mobile phones	**H**	No action
A.1.1.4	Email Service	**H**	No action
	Company fixed-line phone	**H**	No action
	Salesmen mobile phones	**H**	No action
	Financial control	**M**	No action required.
	Internet Service provisioning	**M**	No action
A.1.1.6	Email Service	**H**	Yes. No action required
	fixed-line phone	**H**	Due to alternative communication channels no action required.
	Salesmen mobile phones	**H**	Due to alternative communication channels no action required.
A.1.2.1	Email Service	**H**	Yes backup of emails is part of the service
	fixed-line phone	**H**	No
	Salesmen mobile phones	**H**	No

Applications Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
	Financial control	**M**	The contractor will be requested to perform test restores according to the backup plan that will be developed. **Deliverable: Backup Plan (attached to the BCP)**
	Internet Service provisioning	**M**	Backup Internet service provisioning will be investigated as an option (e.g. Mobile Internet 3G/hsdpa, wireless providers, etc). The process for activating the backup service will be documented and be available with the BCP. **Deliverable: Telecommunications Disaster Recover documentation (attached to the BCP)**

Table 44: Application Actions List – Example

Data - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
D.1.1.1	Spare part requests	**H**	Installe a hard disk mirroring solution. **Documentation: Mirroring Solution Installation and user guide**.
D.1.1.5	Spare part requests	**H**	Backup media will be stored off-site and the process will be documented in the backup plan. **Documentation: Backup plan (attached to the BCP)**
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.1	Spare part requests	**H**	Backup sechedule will be formalised. Our IT expert will propose alternative plans to choose from. It is understood that procurement of media or hardware and software may be required for some options. **Deliverable: backup rotation schedules of the backup plan**
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.3	Spare part requests	**H**	Our IT expert will determine the amount of data to be backedup and restored. The time required for the activities with the proposed solution will be calculated. The backup system will be enhanced /replaced with functionality needed to meet the recovery objectives. The backup schedules may also be altered accordingly. **Deliverable: Backup system sizing and fine tuning (used for backup system procurement and backup plan fine tuning)**
D.1.2.4	Spare part requests	**H**	When the responsibility of data backup is staying with the individual data owners. They will use the Internet backup solution selected and procured by the company. **Deliverable: Internet Backup User Instructions (attached to the backup plan)** Corporate financial data are responsibility of the financial control application contractor and will not be backedup to the internet.
	Corporate Financial Data	**M**	
	order progress tracking	**M**	
D.1.2.5	Spare part requests	**H**	The Backup will be documented. Our IT expert will propose alternative plans to choose from. It is understood that procurement of media or hardware and software may be required for some options. **Deliverable: backup plan (attached to the BCP)** **Deliverable: Records of backup/restore tests and media content (attached to the backup plan)**
	Corporate Financial Data	**M**	
	order progress tracking	**M**	

Table 45: Data Actions List – Example

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
P.1.1.2	External IT expert	**H**	Due to the small size of our offices. No authorisation process is required. IT systems already require a username and password to be accessed.

People - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
	PBX Supplier Technician2 Technician1 Secretary WareHouseMan		No Action.
P.1.1.3	External IT expert PBX Supplier Technician2 Technician1 Secretary WareHouseMan	**H**	A clean desk policy will be applied.
P.1.2.1	External IT expert PBX Supplier Technician2 Technician1 Secretary WareHouseMan	**H**	A technology business continuity toolset will be developed and further enhanced with experience coming from exercises. An appropriate location for easy access will be identified and documented in the BCP. **Deliverable: technology business continuity toolset (software/hardware, documents, guidelines)** **Documentation: Toolset retrieval instructions attached to the BCP)**
P.1.2.2	External IT expert PBX Supplier Technician2 Technician1 Secretary WareHouseMan	**H**	Desktop business continuity exercises will be executed. Exercises will be simple and will only get more complex once employessunderstand their tasks. **Deliverable: Desktop exercises and exercise schedule**
P.1.2.3	External IT expert PBX Supplier Technician2 Technician1 Secretary WareHouseMan	**H**	Where possible deputies will be identified. **Deliverable: The BCP will include the identified deputies**
P.1.2.4	External IT expert Technician2 PBX Supplier Technician1 Secretary WareHouseMan	**H**	IT Personell is mostly outsourced. Training for disaster recovery will be part of the exercises. Technician2 will be trained to his responsibilities.
	Financial control software supplier Company Owner	**M**	

Table 46: People Actions List – Example

Facilities - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
F.1.1.1	Company offices	**H**	No action.
F.1.1.2	Company offices	**H**	All systems identified as critical assets will be powered through a UPS. **Deliverable: Asset profiles updated to reflect the existence of UPS.**
F.1.1.3	Company offices	**H**	Air-conditioning is controlled to human comfort levels. Employess will be advised to take not of malfunctions and if required equipment will be placed in a separate room. **Deliverable: Employee awareness**
F.1.1.4	Company offices	**H**	No further improvement is possible. No action
F.1.1.7	Company offices	**H**	Arrangements for transferring the telecommunication services, supplies and spare parts delivery to an alternate (disaster recovery) site will be documented. This will include redirection of internet based services to other providers. **Deliverable : IT site recovery plan(attached to the BCP)**
F.1.2.2	Company offices	**H**	No further improvement is possible. No action
F.1.2.3	Company offices	**H**	Auto shut off is not supported. The emergency procedures will be amended to instruct employess to poweroff airconditions in case of fire. **Deliverable: Amend emergency procedures**
F.1.2.4	Company offices	**H**	Our location is not prone to flooding. No action
F.1.3.4	Company offices	**H**	Only the warehouse is kept always locked. Personell will be instructed to challenge strangers accessing company premises and IT equipment. **Deliverable: Employee awareness**

Table 47: Facilities Actions List - Example

Since the necessary actions are determined, the Assessment Team prioritizes them and then focuses on implementing the highest-priority actions. The actions prioritization for the asset based controls implementation (table 46) is determined as **medium** since the recovery priority of the identified critical assets used to support the critical business function Finance is **medium**. The actions prioritization regarding the implementation of organizational controls is performed according to the Risk Profile Selection Table (table 9). In this regard, the Assessment Team assigns a **low** implementation priority.

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 48: Controls Prioritization Matrix - Example

The team decides high priority actions to be implemented within the next quarter, medium priority actions within the next six months and low priority actions until the end of the current year. The output of the implementation plan is summarized in the table below:

BC Controls Implementation Plan				
Control	**Responsible**	**External support required**	**Milestones Mm/Dd**	**Implementation Priority**
SP.1.1	Company Owner	No		Low
SP2.1	Technician1	External IT Expert and the Assessment team		Low
SP2.2	Technician1	External IT Expert		Low
SP2.3	WarehouseMan	No		Low
SP2.7	SalesMan1	External IT Expert		Medium
SP5.2	SalesMan1	External IT Expert		Medium
HN.1.1.1	Technician1	External IT Expert		
HN.1.1.5	Technician1	No		
HN.1.1.7	Technician1	External IT Expert		
HN.1.2.1	Technician1	External IT Expert		
HN.1.2.5	Technician1			
HN.1.3.3	SalesMan2			
A.1.1.1	Technician1	External IT Expert, Technician2		
A.1.2.1	Technician1	External IT Expert		
D.1.1.1	Technician2	External IT Expert		Medium
D.1.1.5	WarehouseMan	External IT Expert		High
D.1.2.1	Technician1	External IT Expert		Medium
D.1.2.3	Technician1	External IT Expert		Medium
D.1.2.4	Technician2			Medium
D.1.2.5	Technician1	External IT Expert		High
P.1.1.3	Company Owner			Low
P.1.2.1	Technician2	External IT Expert		
P.1.2.2	Company Owner			
P.1.2.3	Company Owner	External IT Expert		
P.1.2.4	Technician1	External IT Expert		Medium
F.1.1.2	Technician2			High

F.1.1.3	Company Owner			High
F.1.1.7	Technician1	External IT Expert		
F.1.2.3	WarehouseMan			High
F.1.3.4	WarehouseMan			High

Table 49: Implementation plan – Example

[Step 3] As an output of the above phases and steps the Assessment Team will derive the organization's Business Continuity Plan (BCP). **The following tasks will be required to complete the BCP Document:**

- The Business Continuity Team members must be appointed.
- A primary and a secondary emergency command centre have to be selected for the BC Team to meet and organize their actions.
- The Business Continuity Team Responsibility matrix has to be reviewed and tasks/responsibilities should be added or modified as needed for the specific BCP.
- Create an Annex with Contact List of Governmental authorities / bodies that may help in a Business Continuity incident
- When the Business Continuity Controls are implemented their documentation and usage instructions have to be added as an annex to the plan.
- The full set of Critical Business Function Profile Cards and Asset Identification Cards have to be included in an annex of the BCP.
- Implementation of the recovery controls for each individual critical business function have to be clearly indicated
- A date for the first walkthrough/desktop exercise of the plan must be set.
- A date for the first review of the BC Assessement and BCP must be set.
- The BCP must be approved and signed of by a manager with appropriate authority (i.e. the owner of the company),
- The BCP must be distributed among the involved personnel.

The BCP for the example company is a separate document is being made available together with the present BCM approach documentation.

Annex A– Organizational Continuity Control Card

The organisational based controls cards are selected in Phase 3: Controls Selection. The selection of the organizational control cards is performed in a fairly straightforward manner. The Assessment Team marks with a circle the organisational controls applicable for the risk profile of each individual risk area by consulting the Risk Profile Selection Table that was generated in Phase 1. **A detailed description of the controls is included in Annex C.**

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

Annex B– Asset Based Continuity Control Cards

The asset based controls cards[11] are selected in Phase 3: Controls Selection. The control cards, except for the proactive continuity controls (prior to the disaster occurrence), also include the immediate recovery actions[12] (after the disaster occurrence) in order to achieve business recovery. The recovery actions selection is driven from the continuity control category and the respective continuity control, where the latter implies / requires an action for its implementation.

It should be noted that the recovery actions are indicative; specific recovery actions for business recovery should be designed and documented within the relative recovery plans (i.e. Business Continuity Plan).

The objective of the recovery actions is to eliminate the impact of the continuity threats after their occurrence. The controls will be categorized according to their nature continuing on the ground and reflecting the aforementioned Organizational Continuity Controls.

High Risk Cards

Asset Based Continuity Control Card ID		CCC-1HN		
Risk Profile		High		
Asset Category		Hardware and Network		
Continuity Controls Category		Resilience	Back up	Redundancy
Recovery Priority	High	HN.1.1.1 - HN.1.1.2 HN.1.1.3 - HN.1.1.4 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.3 - HN.1.2.4 HN.1.2.5	HN.1.3.1 - HN.1.3.2 HN.1.3.3
	Medium	HN.1.1.1 - HN.1.1.2 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.5	HN.1.3.1 - HN.1.3.3
	Low	HN.1.1.1 - HN.1.1.7	HN.1.2.1 HN.1.2.5	HN.1.3.3
Recovery Actions		RA.1.1.2 – RA.1.1.5	RA.1.2.1 - RA.1.2.4	RA.1.3.1 - RA.1.3.2 RA.1.3.3

[11] The assignment of controls to the asset control cards throughout this annex has been performed in a way that a good degree of protection can be achieved. In case of assets with very high security requirements, additional controls might be considered. Nevertheless, by using these assets control cards a good average protection can be achieved which seems to be appropriate for the majority of SMEs. In the middle term, ENISA plans to validate the assumptions made herein by means of pilot projects.

[12] The recovery actions presented into this section are indicative revealing an integrated approach towards business continuity management within SME environments. An SME could expand the recovery actions in order to indicate specifically the steps required for the implementation of the selected continuity controls

A high risk profile implies threats that occur in hardware and network components unavailability leading to interruption of critical business functions. Systems are unable to host business back office and client facing applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

Essential Controls for the safeguard of availability in critical assets are the following:

HN.1.1.1: IT Infrastructure Documentation. There is an up-to-date and detailed IT infrastructure diagram including network and hardware components.

HN.1.1.2: IT Equipment Documentation. The organization maintains detailed records of hardware and network components configuration / parameterization.

HN.1.1.3: Information Systems Monitoring. Network and system availability figures are monitored for trends as well as threshold exception basis and the information is used to identify points of throughput weakness (bottlenecks).

HN.1.1.4: Information Systems Resilience. The control requires the implementation of technologies such as clustering and load balancing for the resilience of hardware and network components.

HN.1.1.5: Disaster Recovery Cross Training. No critical hardware or network component depends on an individual person for restoration in a disaster.

HN.1.1.6: Information Systems Distribution. Critical IT hardware / network components are spread across diverse locations within the organization's premises.

HN.1.1.7: Information Systems Hardening. Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

HN.1.2.1: Information Systems Backup. Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and must be retained in good working condition.

HN.1.2.2: Backup Restoration. Appropriate procedures are present to assure the ability to restore from backup media under the following conditions: (a) changes of backup software version (b) changes of backup device hardware/firmware (including mechanical maintenance/service) (c) changes in the hardware configuration of the backed up system.

HN.1.2.3: Backup Media Redundancy. Backup clones are available to safeguard against damage of the original backup media. The cloned backup set is stored in a different location than the original.

HN.1.2.4: Backup Fail-Over. Where redundant systems are used, backup devices and software are in place to manage backups from a single, secondary system when the primary has failed. Care is taken to maintain compatibility of hardware, media types, software versions between the primary and the secondary system.

HN.1.2.5: Staff Training. Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

HN.1.3.1: Information Systems Redundancy. Network equipment and hardware modules are designed to be fully redundant with no single points of failure.

HN.1.3.2: Information Systems Replication. Alternative, stand-by equipment is in place to mirror the production systems in the case of a disaster. The equipment should be capable of replacing the primary equipment after loading the necessary data from the backup media.

HN.1.3.3: Vendors SLAs. The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.

RA.1.1.2: Consult the configuration records to restore hardware / network component.

RA.1.1.5: Establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components

RA.1.2.1: Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules

RA.1.2.4: Use the secondary backup system to manage backups, if the primary has failed.

RA.1.3.1: Switch to manual procedures and restore hardware / software failure

RA.1.3.2: Use alternative, mirrored equipment to replicate the production system

RA.1.3.3: Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment

Asset Based Continuity Control Card ID		CCC-1A	
Risk Profile		High	
Asset Category		Application	
Continuity Controls Category		Application Resilience	Application Back up
Recovery Priority	High	A.1.1.1 - A.1.1.2 - A.1.1.3 A.1.1.4 - A.1.1.5 - A.1.1.6 A.1.1.7 - A.1.1.8	A.1.2.1 - A.1.2.2
	Medium	A.1.1.1 - A.1.1.2 - A.1.1.3 A.1.1.4 - A.1.1.5 - A.1.1.6	A.1.2.1 - A.1.2.2
	Low	A.1.1.1 - A.1.1.3 - A.1.1.4 A.1.1.6	A.1.2.1 - A.1.2.2
Recovery Actions		RA.1.1.3 - RA.1.1.6	RA.1.2.1

Application-based availability controls for a high risk organizational profile typically address high availability requirements on an application level to safeguard application's accessibility by internal and external authorized users. Controls are selected to protect information assets from unavailability to authorized entities whether external or internal to the organization's environment.

Essential Controls for the protection of availability in critical assets are the following:

A.1.1.1: Application Documentation. The control requires the organization to identify and collect documents required to install and operate the application. This includes information on the environment (OS version, external libraries, etc) for the execution of the application. This documentation has to be verified and updated at least at every maintenance cycle of the BCP.Furthermore, if the application is custom the application code should be documented. The criticality of the application will dictate the level of documentation required.

A.1.1.2: Application Staging. The control requires that the application should undergo thorough testing on test servers before allowing it for production usage.

A.1.1.3: Application Configuration Management. A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.

A.1.1.4: Application Maintenance and Patching. Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.

A.1.1.5: Application Hardening. Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

A.1.1.6: Application Vendors & SLAs.. The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented agreement exists between the two parties for technical support provisioning when required.

A.1.1.7: Application Clustering.. The control requires the implementation of clustering technologies for the resilience of the application. The application is scaled out across multiple compute nodes to provide application's high availability and performance

A.1.1.8: Application Monitoring. Application availability figures are monitored for trends as well as threshold exception basis and the information is used to identify points of throughput weakness (bottlenecks).

A.1.2.1: Application Backup. Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules. When this control is applied to a service (such as email or internet provisioning) then establishing an alternate backup service is required in addition to backing up any relevant data.When considering backup of services that produce or store data the ability to have a usable local copy of the data or to transfer existing data to the backup service has to be considered and evaluated.

A.1.2.2: Staff Training. Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

RA.1.1.3: Consult the application's configuration records to repair / reinstall the application

RA.1.1.6: Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.

RA.1.2.1: Initiate backup procedure to restore the application software modules or Initiate the processof switching to the backup service provider.

Asset Based Continuity Control Card ID		CCC-1D	
Risk Profile		High	
Asset Category		Data	
Continuity Controls Category		Data Storage	Data back up
Recovery Priority	High	D.1.1.1 - D.1.1.2 -D.1.1.3 D.1.1.4 - D.1.1.5	D.1.2.1 - D.1.2.2 - D.1.2.3 - D.1.2.5
	Medium	D.1.1.1 - D.1.1.2 - D.1.1.5	D.1.2.1 - D.1.2.3 - D.1.2.5
	Low	D.1.1.1 - D.1.1.5	D.1.2.1 - D.1.2.3 - D.1.2.5
Recovery Actions		RA.1.1.1 - RA.1.1.2 - RA.1.1.3 – RA.1.1.4 - RA.1.1.5	RA.1.2.1 - RA.1.2.2 - RA.1.2.3 - RA.1.2.4 - RA.1.2.5

A high risk profile implies storage and backup of internal proprietary or external information that would typically incur a generic threat profile involving external malicious entities intending to violate information availability. Data-based continuity controls for a high risk organizational profile define the level of accuracy of information while availability refers to the level of accessibility.

Essential Controls for the protection of data availability are the following:

D.1.1.1: Data Mirroring. The control requires that all critical data are mirrored to additional storage media ensuring that data is written to two or more different disks (disk mirroring / raid array configuration) to ensure that two valid copies of the data are available. Ensure adequate monitoring is in place (prefferably with a persistent sound notification too) to avoid a failure of one of the storage media goes unnoticed until all copies have failed.

D.1.1.2: Network Storage. Data stored on end user devices (Laptops, workstations, etc) must be periodically synced to a networked disk (a single server with data storage capacity) or a networked storage device (network-attached storage (NAS) or storage area network (SAN)). In addition, the most recent backup of critical data or systems can be kept on the network storage for high speed restoration.

D.1.1.3: Secure Remote Storage. The control requires that on a daily basis, after imaging the servers to which it is attached, the Network Attached Storage (NAS) device creates an independent encrypted tunnel and transmits the imaged data to a secure offsite location where it resides in an encrypted, compressed format, creating a total of two copies of the data in two geographically distinct regions.

D.1.1.4: Data Replication. The control requires that all critical data are replicated to additional storage locations to ensure that two valid copies of the data are available. The second location can be a different branch office of the organization or a remote data center. Depending on the amount of data loss that can be tolerated and the cost of the technical solution a zero data loss or point in time implementation should be selected.

D.1.1.5: Store Backup Media Offsite. Backup media should be labelled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.

D.1.2.1: Backup Rotation Schedules. The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.

D.1.2.2: Near Real-Time Backups. The control requires an incremental methodology which captures all changes to the initial image in increments within minutes. The Incremental methodology not only backs up recent datasets but also allows end users to reconstruct the state of their data as it stood at the end of various minute-based restoration points.

D.1.2.3: Backup System Flexibility. The backup system should allow quick and flexible restoration of files, folders, partitions, mailboxes/messages and databases/tables. It should be possible to schedule restoration of data according to the pre-determined recovery priority. This is to be utilised when the time to restore the full datasets exceeds the target recovery times. Design your backup plan to meet the precise restoration time objectives. Order the backup sequence according to your recovery sequence to avoid time costly seeks on tapes. Create a precise map of the contents of each tape. If possible clone the backup sets to a hard disk storage to increase the speed of restoration.

D.1.2.5: Data Backup. Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.

RA.1.1.1: If the mirrored set failes and cannot recover automatically revert to backup restration on new storage media. If data call a recovery expert. In any case make sure data salavage operation is performed on a copy and not on the original media, if possible.

RA.1.1.2: Restore data to the required information systems via the NAS / SAN

RA.1.1.3: Load backup data to the required information systems via the NAS / SAN. If the data are corrupted or irretrievable obtain data from the secondary site.

RA.1.1.4: Select one of the recovery strategies: a) Transfer IT operations to the location of the data. B) transport the replicated data to the designated recovery site c) Arrange for sufficient network BW and Q.o.S. (latency and delay) for the remote access of the data.

RA.1.1.5: Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.

RA.1.2.1: Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.

RA.1.2.2: Assess your ability to salavage near real-time backups if they are located at the incident site.

RA.1.2.3: If time limits are tight schedule the restoration of data according to the pre-determined recovery priority. Use a pre-compiled restoration sequence.

RA.1.2.5: Initiate the backup plan to restore the damaged / lost data

Asset Based Continuity Control Card ID			CCC-1P
Risk Profile			High
Asset Category			People
Continuity Controls Category		Physical Security	Awareness & Training
Recovery Priority	High	P.1.1.1- P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.2 – P.1.2.3 – P.1.2.4
	Medium	P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.2 - P.1.2.3 – P.1.2.4
	Low	P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.4
Recovery Actions			RA.1.2.3

A high risk profile implies threats that occur in people health / safety and in human resources in general. The level of staff commitment on using the appropriate continuity controls determines level of protection that can be achieved.

Awareness and training of staff on emergency and incident management procedures ensures the protection of human resources and the availability of information.

Essential Controls for securing and protecting people from continuity threats that could put in human life into danger are the following:

P.1.1.1: Actions Accountability. Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for

P.1.1.2: Physical Access Control. Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

P.1.1.3: Clean Desk Policy. A clean desk policy is in operation followed by all personnel, contactors and third parties

P.1.2.1: Business Continuity Tool Set. The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.

P.1.2.2: Business Continuity Tests. Staff, have been trained and involved in business continuity tests.

P.1.2.3: Key Personnel Deputies. All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfil their duties / responsibilities.

P.1.2.4: Key IT Personnel Training. The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a "business as usual" basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures

RA.1.2.3: Business Continuity Deputies take over the duties of the staff responsible with business continuity responsibilities.

Asset Based Continuity Control Card ID		CCC-1F		
Risk Profile		High		
Asset Category		Facilities		
Continuity Controls Category		IT Site	Environmental Security	Physical Security
Recovery Priority	High	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4 F.1.1.5 - F.1.1.6 F.1.1.7 - F.1.1.8	F.1.2.1 - F.1.2.2 F.1.2.3 - F.1.2.4 F.1.2.5	F.1.3.1 - F.1.3.2 F.1.3.3 - F.1.3.4 F.1.3.5 - F.1.3.6
	Medium	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.5 F.1.1.5 - F.1.1.6 F.1.1.7	F.1.2.2 - F.1.2.3 F.1.2.4 - F.1.2.5	F.1.3.2 - F.1.3.3 F.1.3.4 - F.1.3.5 F.1.3.6
	Low	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4 F.1.1.7	F.1.2.2 - F.1.2.3 F.1.2.4	F.1.3.4 - F.1.3.5 F.1.3.6
Recovery Actions		RA.1.1.1 – RA.1.1.2 - RA.1.1.3 – RA.1.1.4 - RA.1.1.5 – RA.1.1.6 - RA.1.1.7 – RA.1.1.8	RA.1.2.1	RA.1.3.2 – RA.1.3.3

A High risk profile implies high environmental and physical continuity controls to safeguard the organization's facilities from natural and man-made disasters. Furthermore, these controls will also protect the corporate people and information as well as the IT equipment which operate within the organization's facilities.

Essential Controls for securing and protecting corporate facilities from continuity threats are the following:

F.1.1.1: IT Site Physical Access. Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or similarphysical access control technologies.

F.1.1.2: IT Site Power Supply. The power supply of the site equipment is protected with UPS and / or generators.

F.1.1.3: IT Site Air-Conditioning. IT site humidity, ventilation and air-conditioning are controlled.

F.1.1.4: IT Site Anti-fire Systems. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.

F.1.1.5: IT Site Anti-flood Systems. IT Site is equipped with water detection systems and anti-flood mechanisms (raised floors, drop ceilings)

F.1.1.6: IT Disaster Recovery Site. There is an alternate dedicated site where IT is restored following a disaster.

F.1.1.7: IT Site Recovery Plan. Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.

F.1.1.8: Secondary Disaster Recovery Site. There is an additional secondary site with certain mechanisms in place for invoking it if the primary recovery site is not available.

F.1.2.1: Electrical Power Mechanisms. All critical business functions are protected by uninterruptible power supply (UPS) or similar battery backup. In addition all areas and systems of the corporate facilities have their power supply backed up by generators. Power can be provided by generato

F.1.2.2: Fire Fighting Equipment. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within corporate facilities

F.1.2.3: Air-conditioning. The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.

F.1.2.4: Anti-flood Equipment. There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.

F.1.2.5: Electrical Power Protection. Corporate facilities are protected against electrical spikes and surges (e.g. lightning strikes). In addition the control requires the proper grounding and shielding of the cables used to supply electrical power.

F.1.3.1: Battle Boxes. Sites use 'battle boxes' containing a variety of equipment selected to assist with the management and control of a business continuity incident. Alternatively, the organization keeps and maintains the materials required to help the recovery of business op

F.1.3.2: Secure Delivery and Loading Area. The control requires a documented policy for controlling introduction of packages or items within a dedicated post room which systematically inspects for threatening objects received by couriers and visitors.

F.1.3.3: Facilities Access Control. All critical sites have security guards (24 hours a day, 7 days a week), and / or internal / external CCTVs, access control systems and a standard access management security procedure.

F.1.3.4: Rooms and Areas Secure Access. Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to authorised personnel.

F.1.3.5: Visitors Escort. Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.

F.1.3.6: ID Badges. Permanent and temporary staff, contract staff and visitors required to wear visible id badges.

RA.1.1.1: Once the emergency/incident is contained provide arrangements for the physical security of the incident site.

RA.1.1.2: Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and

RA.1.1.3: Verify air-conditioning operates normally. Make sure you can contact qualified technicians in case of failure.

RA.1.1.4: If the anti-fire systems were engaged, make sure the site is safe for personell(engage the fire department) before attempting to salvage any equipment.C23

RA.1.1.5: Be aware of the risk of electrical shock due to exposed wires to the water. Refresh the operating procedures and operate any anti-flood systems you might have in place or seek support from the emergency services. Monitor closely the condition as you might

RA.1.1.6: Evaluate the need to activate the disaster recovery site. Check site availability and announce the DR site location to be activated. Follow the activation plan

RA.1.1.7: On DR site activation implement the site recovery plan.

RA.1.1.8: Evaluate the need to activate the disaster recovery site. Check site availability and announce the DR site location to be activated. Follow the activation plan

RA.1.2.1: Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and

RA.1.3.2: Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.

RA.1.3.3: Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.

Medium Risk Cards

Asset Based Continuity Control Card ID		CCC-2HN		
Risk Profile		Medium		
Asset Category		Hardware and Network		
Continuity Controls Category		Resilience	Back up	Redundancy
Recovery Priority	High	HN.1.1.1 - HN.1.1.2 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.5	HN.1.3.1 - HN.1.3.3
	Medium	HN.1.1.1 - HN.1.1.2 HN.1.1.7	HN.1.2.1 - HN.1.2.5	HN.1.3.3
	Low	HN.1.1.1 - HN.1.1.2	HN.1.2.1	HN.1.3.3
Recovery Actions		RA.1.1.2	RA.1.2.1 - RA.1.2.2	RA.1.3.1 - RA.1.3.2 RA.1.3.3

A medium risk profile implies moderate level threats that occur in system or network equipment instabilities leading to unavailability of business service for a short period of time. Systems and / or network components are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system and network components to ensure their availability.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

HN.1.1.1: IT Infrastructure Documentation. There is an up-to-date and detailed IT infrastructure diagram including network andhardware components.

HN.1.1.2: IT Equipment Documentation. The organization maintains detailed records of hardware and network components configuration / parameterization.

HN.1.1.5: Disaster Recovery Cross Training. No critical hardware or network component depends on an individual person for restoration in a disaster.

HN.1.1.6: Information Systems Distribution. Critical IT hardware / network components are spread across diverse locations within the organization's premises.

HN.1.1.7: Information Systems Hardening. Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

HN.1.2.1: Information Systems Backup. Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and must be retained in good working condition.

HN.1.2.2: Backup Restoration. Appropriate procedures are present to assure the ability to restore from backup media under the following conditions: (a) changes of backup software version (b) changes of backup device hardware/firmware (including mechanical maintenance/service) (c) changes in the hardware configuration of the backed up system.

HN.1.2.5: Staff Training. Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

HN.1.3.1: Information Systems Redundancy. Network equipment and hardware modules are designed to be fully redundant with no single points of failure.

HN.1.3.3: Vendors SLAs. The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.

RA.1.1.2: Consult the configuration records to restore hardware / network component.

RA.1.1.5: Establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components

RA.1.2.1: Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules

RA.1.3.1: Switch to manual procedures and restore hardware / software failure

RA.1.3.3: Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment

Asset Based Continuity Control Card ID		CCC-2A	
Risk Profile		Medium	
Asset Category		Application	
Continuity Controls Category		Application Resilience	Application Back up
Recovery Priority	High	A.1.1.1 - A.1.1.2 - A.1.1.3 A.1.1.4 - A.1.1.5 - A.1.1.6	A.1.2.1 - A.1.2.2
	Medium	A.1.1.1 - A.1.1.3 - A.1.1.4 A.1.1.6	A.1.2.1 - A.1.2.2
	Low	A.1.1.1 - A.1.1.4 - A.1.1.6	A.1.2.1 - A.1.2.2
Recovery Actions		RA.1.1.3 - RA.1.1.6	RA.1.2.1

A medium risk profile implies storage and backup activities of moderate-value applications that would typically incur a generic threat profile involving external malicious entities intending to violate moderate-value application availability.

Essential Controls for the protection of availability in applications are the following:

A.1.1.1: Application Documentation. The control requires the organization to document the application code (if the application is custom) and the required environment (OS version, external libraries, etc) for the execution of the application.

A.1.1.2: Application Staging. The control requires that the application should undergo thorough testing on test servers before allowing it for production usage

A.1.1.3: Application Configuration Management. A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.

A.1.1.4: Application Maintenance and Patching. Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.

A.1.1.5: Application Hardening. Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

A.1.1.6: Application Vendors & SLAs. The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented agreement exists between the two parties for technical support provisioning when required.

A.1.2.1: Application Backup. Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules.

A.1.2.2: Staff Training. Control requires that all staff understand and are able to carry out their responsibilities under the backup plans**.**

The recovery actions that the organization with medium risk profile should undertake in order to achieve critical assets recovery are the following:

RA.1.1.3: Consult the application's configuration records to restore the application

RA.1.1.6: Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.

RA.1.2.1: Initiate backup procedure to restore the application software modules

Asset Based Continuity Control Card ID			CCC-2D
Risk Profile			Medium
Asset Category			Data
Continuity Controls Category		Data Storage	Data back up
Recovery Priority	High	D.1.1.1 - D.1.1.2 - D.1.1.5	D.1.2.1 - D.1.2.3 - D.1.2.5
	Medium	D.1.1.1 - D.1.1.5	D.1.2.1 - D.1.2.5
	Low	D.1.1.1 - D.1.1.5	D.1.2.1 – D.1.2.5
Recovery Actions		RA.1.1.1 - RA.1.1.2 - RA.1.1.5	RA.1.2.5

A medium risk profile implies storage and backup of internal proprietary or external information that would typically incur a generic threat profile involving external malicious entities intending to violate or information availability. Data-based continuity controls for a medium risk organizational profile define the level of accuracy of information while availability refers to the level of accessibility.

Essential Controls for the protection of data availability are the following:

D.1.1.1: Data Mirroring. The control requires that all critical data are mirrored to additional storage media ensuring that data is written to two or more different disks (disk mirroring / raid array configuration) to ensure that two valid copies of the data are available. Ensure adequate monitoring is in place (prefferably with a persistent sound notification too) to avoid a failure of one of the storage media goes unnoticed until all copies have failed.

D.1.1.2: Network Storage. Data stored on end user devices (Laptops, workstations, etc) must be periodically synced to a networked disk (a single server with data storage capacity) or a networked storage device (network-attached storage (NAS) or storage area network (SAN)). In addition, the most recent backup of critical data or systems can be kept on the network storage for high speed restoration.

D.1.1.5: Store Backup Media Offsite. Backup media should be labelled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.

D.1.2.1: Backup Rotation Schedules. The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.

D.1.2.3: Backup System Flexibility. The backup system should allow quick and flexible restoration of files, folders, partitions, mailboxes/messages and databases/tables. It should be possible to schedule restoration of data according to the pre-determined recovery priority. This is to be utilised when the time to restore the full datasets exceeds the target recovery times. Design your backup plan to meet the precise restoration time objectives. Order the backup sequence according to your recovery sequence to avoid time costly seeks on tapes. Create a precise map of the contents of each tape. If possible clone the backup sets to a hard disk storage to increase the speed of restoration.

D.1.2.5: Data Backup. Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.

RA.1.1.1: If the mirrored set failes and cannot recover automatically revert to backup restration on new storage media. If data call a recovery expert. In any case make sure data salavage operation is performed on a copy and not on the original media, if possible.

RA.1.1.2: Restore data to the required information systems via the NAS / SAN

RA.1.1.5: Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.

RA.1.2.1: Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.

RA.1.2.3: If time limits are tight schedule the restoration of data according to the pre-determined recovery priority. Use a pre-compiled restoration sequence.

RA.1.2.5: Initiate the backup plan to restore the damaged / lost data

Asset Based Continuity Control Card ID		CCC-2P	
Risk Profile		Medium	
Asset Category		People	
Continuity Controls Category		Physical Security	Awareness & Training
Recovery Priority	High	P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.2 – P.1.2.3 – P.1.2.4
	Medium	P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.2 - P.1.2.4
	Low	P.1.1.3	P.1.2.4
Recovery Actions		-	-

A high risk profile implies threats that occur in people health / safety and in human resources in general. The level of staff commitment on using the appropriate continuity controls determines level of protection that can be achieved.

Awareness and training of staff on emergency and incident management procedures ensures the protection of human resources and the availability of information.

Essential Controls for securing and protecting people from continuity threats that could put in human life into danger are the following:

P.1.1.2: Physical Access Control. Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

P.1.1.3: Clean Desk Policy. A clean desk policy is in operation followed by all personnel, contactors and third parties

P.1.2.1: Business Continuity Tool Set. The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.

P.1.2.2: Business Continuity Tests. Staff, have been trained and involved in business continuity tests.

P.1.2.3: Key Personnel Deputies. All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfil their duties / responsibilities.

P.1.2.4: Key IT Personnel Training. The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a “business as usual” basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures

RA.1.2.3: Business Continuity Deputies take over the duties of the staff responsible with business continuity responsibilities.

Asset Based Continuity Control Card ID		CCC-2F		
Risk Profile		Medium		
Asset Category		Facilities		
Continuity Controls Category		IT Site	Environmental Security	Physical Security
Recovery Priority	High	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.5 F.1.1.4 - F.1.1.6 F.1.1.7	F.1.2.2 - F.1.2.3 F.1.2.4 - F.1.2.5	F.1.3.2 - F.1.3.3 F.1.3.4 - F.1.3.6
	Medium	F.1.1.1 - F.1.1.2 F.1.1.3 – F.1.1.4 F.1.1.7	F.1.2.2 - F.1.2.3 F.1.2.4	F.1.3.3 - F.1.3.4
	Low	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4 F.1.1.7	F.1.2.2 - F.1.2.3	F.1.3.4
Recovery Actions		-	-	-

A medium risk profile implies medium-level environmental and physical continuity controls to safeguard the organization's facilities from natural and man-made disasters. Furthermore, these controls will also protect the corporate people and information as well as the IT equipment which operate within the organization's facilities.

Essential Controls for securing and protecting corporate facilities from continuity threats are the following:

F.1.1.1: IT Site Physical Access. Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or similar physical access control technologies.

F.1.1.2: IT Site Power Supply. The power supply of the site equipment is protected with UPS and / or generators.

F.1.1.3: IT Site Air-Conditioning. IT site humidity, ventilation and air-conditioning are controlled.

F.1.1.4: IT Site Anti-fire Systems. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.

F.1.1.5: IT Site Anti-flood Systems. IT Site is equipped with water detection systems and anti-flood mechanisms (raised floors, drop ceilings)

F.1.1.6: IT Disaster Recovery Site. There is an alternate dedicated site where IT is restored following a disaster.

F.1.1.7: IT Site Recovery Plan. Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.

F.1.2.2: Fire Fighting Equipment. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within corporate facilities

F.1.2.3: Air-conditioning. The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.

F.1.2.4: Anti-flood Equipment. There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.

F.1.3.2: Secure Delivery and Loading Area. The control requires a documented policy for controlling introduction of packages or items within a dedicated post room which systematically inspects for threatening objects received by couriers and visitors.

F.1.3.3: Facilities Access Control. All critical sites have security guards (24 hours a day, 7 days a week), and / or internal / external CCTVs, access control systems and a standard access management security procedure.

F.1.3.4: Rooms and Areas Secure Access. Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to authorised personnel.

F.1.3.6: ID Badges. Permanent and temporary staff, contract staff and visitors required to wear visible id badges.

RA.1.1.1: Once the emergency/incident is contained provide arrangements for the physical security of the incident site.

RA.1.1.2: Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and

RA.1.1.3: Verify air-conditioning operates normally. Make sure you can contact qualified technicians in case of failure.

RA.1.1.4: If the anti-fire systems were engaged, make sure the site is safe for personell(engage the fire department) before attempting to salvage any equipment.C23

RA.1.1.5: Be aware of the risk of electrical shock due to exposed wires to the water. Refresh the operating procedures and operate any anti-flood systems you might have in place or seek support from the emergency services. Monitor closely the condition as you might

RA.1.1.6: Evaluate the need to activate the disaster recovery site. Check site availability and announce the DR site location to be activated. Follow the activation plan

RA.1.1.7: On DR site activation implement the site recovery plan.

RA.1.3.2: Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.

RA.1.3.3: Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.

Low Risk Cards

Asset Based Continuity Control Card ID		CCC-3HN		
Risk Profile		Low		
Asset Category		Hardware and Network		
Continuity Controls Category		Resilience	Back up	Redundancy
Recovery Priority	High	HN.1.1.1 – HN.1.1.5 HN.1.1.7	HN.1.2.1 - HN.1.2.5	HN.1.3.3
	Medium	HN.1.1.1	HN.1.2.1	-
	Low	HN.1.1.1	HN.1.2.1	-
Recovery Actions		-	RA.1.2.1	-

A low risk profile implies minimum level threats that entail potential system or network components instabilities leading to unavailability of business service for a short period of time.

System and network based controls for minimum risk organizational profiles involve methods that ensure proper configuration and functionality of the system and network component to ensure their availability.

Impact of system and / or network component unavailability does not affect organization reputation as information is neither private nor critical to the organization.

Unavailability of system and / or network component does not affect quality of service or product.

Essential Control for the protection of availability in systems and network components are the following:

HN.1.1.1: IT Infrastructure Documentation. There is an up-to-date and detailed IT infrastructure diagram including network and hardware components.

HN.1.1.5: Disaster Recovery Cross Training. No critical hardware or network component depends on an individual person for restoration in a disaster.

HN.1.1.7: Information Systems Hardening. Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

HN.1.2.1: Information Systems Backup. Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and must be retained in good working condition.

HN.1.2.5: Staff Training. Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

HN.1.3.3: Vendors SLAs. The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.

RA.1.1.5: Establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components

RA.1.2.1: Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules

RA.1.3.3: Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment

Asset Based Continuity Control Card ID		CCC-3A	
Risk Profile		Low	
Asset Category		Application	
Continuity Controls Category		Application Resilience	Application Back up
Recovery Priority	High	A.1.1.1 - A.1.1.3 - A.1.1.4 A.1.1.6	A.1.2.1 - A.1.2.2
	Medium	A.1.1.1 - A.1.1.4	A.1.2.1 - A.1.2.2
	Low	A.1.1.1	A.1.2.1 - A.1.2.2
Recovery Actions		RA.1.1.3 - RA.1.1.6	RA.1.2.1

A low risk profile implies storage and backup of applications but with no critical level of importance that would entail minimal finance loss. Organization reputation is not at stake. However, controls that would prevent even that kind of application unavailability and that can secure the application accessibility should be applied.

Furthermore, even if there is no high unavailability impact, application availability to every authorized user must be secured.

Essential controls for availability of the application asset are the following:

A.1.1.1: Application Documentation.. The control requires the organization to identify and collect documents required to install and operate the application. This includes information on the environment (OS version, external libraries, etc) for the execution of the application. This documentation has to be verified and updated at least at every maintenance cycle of the BCP.Furthermore, if the application is custom the application code should be documented. The criticality of the application will dictate the level of documentation required.

A.1.1.3: Application Configuration Management. A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.

A.1.1.4: Application Maintenance and Patching. Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.

A.1.1.6: Application Vendors & SLAs.. The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented agreement exists between the two parties for technical support provisioning when required.

A.1.2.1: Application Backup. Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules. When this control is applied to a service (such as email or internet provisioning) then establishing an alternate backup service is required in addition to backing up any relevant data.When considering backup of services that produce or store data the ability to have a usable local copy of the data or to transfer existing data to the backup service has to be considered and evaluated.

A.1.2.2: Staff Training. Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

RA.1.1.3: Consult the application's configuration records to repair / reinstall the application

RA.1.1.6: Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.

RA.1.2.1: Initiate backup procedure to restore the application software modules or Initiate the processof switching to the backup service provider.

Asset Based Continuity Control Card ID			CCC-3D
Risk Profile			Low
Asset Category			Data
Continuity Controls Category		Data Storage	Data back up
Recovery Priority	High	D.1.1.1 - D.1.1.5	D.1.2.1 - D.1.2.3 - D.1.2.4 - D.1.2.5
	Medium	D.1.1.5	D.1.2.1 - D.1.2.4 - D.1.2.5
	Low	D.1.1.5	D.1.2.1 - D.1.2.4 - D.1.2.5
Recovery Actions		RA.1.1.1 - RA.1.1.5	RA.1.2.5

A low risk profile implies storage and processing of public or internal information but with no critical level of importance that would entail more than a minimal loss of money. Organization reputation is not at stake. However, controls that would prevent even that kind of information unavailability and that can secure the information life-cycle should be applied.

Furthermore, even if there is no major unavailability impact, information accessibility to every authorized user must be secured.

Essential controls for information availability are the following:

D.1.1.1: Data Mirroring. The control requires that all critical data are mirrored to additional storage media ensuring that data is written to two or more different disks (disk mirroring / raid array configuration) to ensure that two valid copies of the data are available. Ensure adequate monitoring is in place (prefferably with a persistent sound notification too) to avoid a failure of one of the storage media goes unnoticed until all copies have failed.

D.1.1.2: Network Storage. Data stored on end user devices (Laptops, workstations, etc) must be periodically synced to a networked disk (a single server with data storage capacity) or a networked storage device (network-attached storage (NAS) or storage area network (SAN)). In addition, the most recent backup of critical data or systems can be kept on the network storage for high speed restoration.

D.1.1.5: Store Backup Media Offsite. Backup media should be labelled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.

D.1.2.1: Backup Rotation Schedules. The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.

D.1.2.3: Backup System Flexibility. The backup system should allow quick and flexible restoration of files, folders, partitions, mailboxes/messages and databases/tables. It should be possible to schedule restoration of data according to the pre-determined recovery priority. This is to be utilised when the time to restore the full datasets exceeds the target recovery times. Design your backup plan to meet the precise restoration time objectives. Order the backup sequence according to your recovery sequence to avoid time costly seeks on tapes. Create a precise map of the contents of each tape. If possible clone the backup sets to a hard disk storage to increase the speed of restoration.

D.1.2.4: Internet Backup. The control requires that workstation users (personnel) are allowed to back up data to a remote location over the Internet. Formal authorisation is required prior to the execution of this backup method.

D.1.2.5: Data Backup. Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.

RA.1.1.1: . If the mirrored set failes and cannot recover automatically revert to backup restration on new storage media. If data call a recovery expert. In any case make sure data salavage operation is performed on a copy and not on the original media, if possible.

RA.1.1.2: Restore data to the required information systems via the NAS / SAN

RA.1.1.5: Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.

RA.1.2.1: Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.

RA.1.2.3: If time limits are tight schedule the restoration of data according to the pre-determined recovery priority. Use a pre-compiled restoration sequence.

RA.1.2.4: Start retrieving Internet backups as soon as possible from a location providing good bandwidth and stable internet connection. Keep in mind internet speeds vary and BW bottlenecks may impose a critical delay to the download. Prioritise your downloads according to your needs.

RA.1.2.5: Initiate the backup plan to restore the damaged / lost data

Asset Based Continuity Control Card ID			CCC-3P
Risk Profile			Low
Asset Category			People
Continuity Controls Category		Physical Security	Awareness & Training
Recovery Priority	High	P.1.1.2 – P.1.1.3	P.1.2.1- P.1.2.2 - P.1.2.3 - P.1.2.4
	Medium	P.1.1.3	P.1.2.4
	Low	P.1.1.3	-
Recovery Actions		-	-

A high risk profile implies threats that occur in people health / safety and in human resources in general. The level of staff commitment on using the appropriate continuity controls determines level of protection that can be achieved.

Awareness and training of staff on emergency and incident management procedures ensures the protection of human resources and the availability of information.

Essential Controls for securing and protecting people from continuity threats that could put in human life into danger are the following:

P.1.1.2: Physical Access Control. Control requires that there are documented procedures for authorizing and overseeing thosewho work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

P.1.1.3: Clean Desk Policy. A clean desk policy is in operation followed by all personnel, contactors and third parties

P.1.2.1: Business Continuity Tool Set. The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.

P.1.2.2: Business Continuity Tests. Staff, have been trained and involved in business continuity tests.

P.1.2.3: Key Personnel Deputies. All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfil their duties / responsibilities.

P.1.2.4: Key IT Personnel Training. The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a “business as usual” basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures

RA.1.2.3: Business Continuity Deputies take over the duties of the staff responsible with business continuity responsibilities.

Asset Based Continuity Control Card ID		CCC-3F		
Risk Profile		Low		
Asset Category		Facilities		
Continuity Controls Category		IT Site	Environmental Security	Physical Security
Recovery Priority	High	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4 F1.1.7	F.1.2.2 - F.1.2.3 F.1.2.4	F.1.3.4
	Medium	F.1.1.1 - F.1.1.2 F.1.1.3 - F.1.1.4	F.1.2.2 - F.1.2.3	F.1.3.4
	Low	F.1.1.2 - F.1.1.3 F.1.1.4	F.1.2.2 - F.1.2.3	-
Recovery Actions		-	-	-

A low risk profile implies low-level environmental and physical continuity controls to safeguard the organization's facilities from natural and man-made disasters. Furthermore, these controls will also protect the corporate people and information as well as the IT equipment which operate within the organization's facilities.

Essential Controls for securing and protecting corporate facilities from continuity threats are the following:

F.1.1.1: IT Site Physical Access. Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or similar physical access control technologies.

F.1.1.2: IT Site Power Supply. The power supply of the site equipment is protected with UPS and / or generators.

F.1.1.3: IT Site Air-Conditioning. IT site humidity, ventilation and air-conditioning are controlled.

F.1.1.4: IT Site Anti-fire Systems. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.

F.1.1.7: IT Site Recovery Plan. Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.

F.1.2.2: Fire Fighting Equipment. Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within corporate facilities

F.1.2.3: Air-conditioning. The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.

F.1.2.4: Anti-flood Equipment. There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.

F.1.3.4: Rooms and Areas Secure Access. Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to authorised personnel.

RA.1.1.1: Once the emergency/incident is contained provide arrangements for the physical security of the incident site.

RA.1.1.2: Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and

RA.1.1.3: Verify air-conditioning operates normally. Make sure you can contact qualified technicians in case of failure.

RA.1.1.4: If the anti-fire systems were engaged, make sure the site is safe for personell(engage the fire department) before attempting to salvage any equipment.C23

RA.1.1.7: On DR site activation implement the site recovery plan.

Annex C – Organizational Continuity Controls

Business Continuity Management Organization (SP1)	
SP1	Business Continuity Management Organization Control Card includes controls that require the organization's business strategies to routinely incorporate business continuity considerations. Equally, business continuity strategies and policies must take into consideration the organization's business strategies and goals.
Business Continuity Policy, Plans and Procedures (SP2)	
SP2	The Control Card requires an organization to have a comprehensive set of documented, current Business Continuity Policies, Plans and Procedures that are periodically reviewed and updated.
Test Business Continuity Plan (SP3)	
SP3	Continuity Planning/Disaster Recovery Control Card incorporates security controls in order to complete a test simulation of the continuity plan to ensure its smooth running if the time comes to implement it.
Sustain Business Continuity Management (SP4)	
SP4	Security Awareness and Training Control Card includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified. Business Continuity Framework should be routinely reviewed, updated, and communicated to the organization.
Service Providers / Third Parties Business Continuity Management (SP5)	
SP5	Service Providers / Third Parties Business Continuity Management Control Cards include security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations (e.g. third parties, collaborators, subcontractors, or partners).

Business Continuity Management Organization (SP1)	
SP1.1	The organization has a documented business continuity policy outlining the fundamental / driving factors that the business continuity framework is designed and built on. The policy should address, but not limited to, the following issues:
	- Business Continuity Goals and Objectives
	- Business Continuity teams, roles and responsibilities
	- Management Responsibilities & Commitment regarding organizational efforts for Business Continuity
	- The requirement of periodic Business Impact Assessments horizontally to the organization
	- Business Continuity Threats with respect to the organization's operating environment
	- Service agreements with third parties ensuring the continuity of the outsourced IT services
SP1.2	The organization's business strategies routinely incorporate business continuity considerations.
SP1.3	Business continuity strategies and policies take into consideration the organization's structure, business strategies and goals.
SP1.4	Business continuity strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.
SP1.5	Business continuity policy, plans and procedures reflect consultation of local emergency services' response plans and include reference materials.
SP1.6	The organization ensures that staff are fully aware and stay vigilant with respect to business continuity. Staff realises that business continuity is not a choice, but a legal, ethical and operational requirement that could mean the difference between business continuance and failure.
SP1.7	Business continuity is included in induction programmes for new employees. The induction pack should include the organization's business continuity strategy and of the roles, responsibilities and organization of the business continuity teams.
SP1.8	The organization has assigned business continuity roles and incident responsibilities, including the following business continuity and incident teams:
	- Business Continuity Steering Committee. The team is consisted of upper management personnel and is responsible for the critical decision making during a business continuity incident.
	- Business Continuity Team. The team is concerned with the handling of business continuity incidents through the organization's Business Continuity Plan
	- Security Incident Response Team. The team is responsible for handling undesirable security events undertaking the required actions to minimize the damage to organization's critical business functions and consequently restore them to the desired operational mode. Another critical responsibility of the team is to trigger the organization's Business Continuity Plan in the case that the "security incident" escalates to a "business continuity incident"
	- Emergency Response Team. The team is responsible for executing the organization's emergency procedures in the case of a natural or manmade physical disaster (fire, earthquake, flood etc)
SP1.9	A fully detailed impact analysis on loss of IT is performed on an annual basis to identify which of the organisation's IT systems, data and infrastructure are the most business critical. The business impact assessment includes the following steps:

	- Gathering information;
	- Performing a vulnerability assessment;
	- Analyzing the information;
	- Documenting the results and presenting the recommendations.
	- Firewalls are deployed at external network entry points
	- Anti-virus products are deployed on mail servers and on all desktops and laptops. Anti-virus products are automatically updated when released by vendor.
SP.1.10	Management allocates sufficient funds and resources to establish a Business Continuity Programme.

Business Continuity Policy, Plans and Procedures (SP2)	
SP2.1	The organization has a comprehensive business continuity plan which is periodically reviewed and updated. The plan address key business continuity topic areas, including:
	- Critical Business Functions Priority List
	- Critical Business Functions IT infrastructure dependencies
	- Contact List(s) with business continuity manager / team
	- Critical Business Functions protection & recovery strategy
	- Business continuity relative procedures (incident response, emergency etc)
	- Testing Reassessing and Maintaining Business Continuity Plan
	- Critical Suppliers List & Contact Details
SP2.2	There is a documented procedure for incident response covering in detail the following topics:
	- Incident Detection. The topic should provide the necessary steps for detecting and reporting an incident to the responsible parties.
	- Incident Containment & Eradication. Activities required by the security incident response team for the effective containment and eradication of the security event.
	- Incident Follow up. The steps that the involved parties should carry out for evaluating the effectiveness of the incident response procedure
SP2.3	The organization has a set of documented emergency procedures for ensuring staff health when a physical disaster (fire, flood, earthquake) occurs. These procedures should address the following health & safety issues :
	A designated trained senior manager or its deputy is assigned to take responsibility for managing evacuation of the organizations premises in the case of a natural disaster (fire, flood, earthquake etc).
	Evacuation points are identified and clearly marked for all staff. In addition there is a clear demonstrable way of ensuring the building is clear (e.g. electronic records, roll call).
	- Emergency team contact details (name/surname, phone number, email etc)
	- Maintenance of emergency toolkits including water, food, first aid kit, torches, radio and batteries, pay-as-you go mobile phone and charger tarpaulins, cleaning supplies, gloves, plastic bags, duct tapes and blankets. All staff should be aware of the location that the emergency kits are stored.
	Emergency drills -without staff awareness- in order to test the emergency procedures efficiency and staff training.
SP2.4	There is a clearly defined procedure for dealing with the media (media communication procedure) and public relations during a crisis.
SP2.5	The organization makes use of security products in order to protect its critical assets from undesirable security events that may lead to a break into business continuity. The following products are in place: - Firewalls are deployed at external network entry points - All computers are using personal firewalls and antivirus software. Daily automatic updates are activated, especially for laptops.
SP2.6	All executives, managers and designated critical staff have trained deputies who can fulfil their duties.
SP2.7	The organisation has established diverse communication channels that clients and third parties can use to contact

	the organisation, request service or report a problem. These arrangements are part of the business as usual and no special actions are needed for their activation. Such communication channels may be land line phone numbers, mobile phone numbers, voice mailboxes, email and FAX from diverse providers to avoid single points of failure.
SP2.8	There is a well known point of contact and designated backups to report incidents and alternate means of communication.

Test Business Continuity Plan (SP3)	
SP3.1	IT recovery tests are performed to realistically reflect the worst case scenario where all critical systems must be restored concurrently. These tests include, but not limited to, the following:
	- Critical business functions recovery is tested every six months.
	- Where a test environment is used, it is very similar to the live environment.
	- Where some IT functions are outsourced, critical IT outsource companies participate individually in tests.
SP3.2	If certain IT aspects are outsourced, a policy to test outsourcers' IT disaster recovery capability exists.
SP3.3	The organization follows a business continuity test plan in order to assess the effectiveness of its Business Continuity Programme. The following elements are tested:
	- Identified critical application or hardware and/or software
	- Rebuilding of client or desktop environment.
	- Remote home working recovery capability to the alternate (disaster recovery) site and adequate capability is evidenced.
	- Restoration of critical business functions
	- If mirrored systems are used, the operation of each secondary system with the primary switched off is tested.
	- If critical backups are needed, they are restore-tested every month.
	- Individual restoration tests suggest that all critical business functions can be recovered in the required timeframes.
	- Power generators and UPS are full-load tested.
SP3.4	Full fire and earthquake evacuation tests are required annually.

Sustain Business Continuity Management (SP4)	
SP4.1	Staff members understand their security business continuity roles and responsibilities. This is documented and verified. Staff understanding is documented and conformance is periodically verified.
SP4.2	Security awareness, training, and periodic reminders are provided for all personnel. Training includes these topics:
	- Business continuity strategies, goals, and objectives
	- Business continuity , polices, plans and procedures
	- Business continuity policies and procedures for working with third parties
	- Emergency procedures
	- Health and safety issues
	- Physical security requirements
	- Incident management
	- General staff practices
	- Enforcement, sanctions, and disciplinary actions for environmental and safety violations of health and safety controls
SP4.3	Business continuity is included in induction programmes for new employees.
SP4.4	Staff members are trained to recognize report and respond to incidents events (manmade or natural) that may impact the organization causing a break to business continuity.
SP4.5	Staff is aware of the organization's business continuity strategy and of the roles, responsibilities and organization of the business continuity team.
SP4.6	All changes to Business Continuity Framework go through an agreed and signed-off procedure.
SP4.7	The organization has a documented change management procedure ensuring that any changes (internal or external) which impact the organisation are reviewed in relation to Business Continuity Documents. The changes triggering an adjustment to the business continuity plan include but not limited to the following:
	- Regulatory changes
	- Resources or organizational structures change
	- Funding or budget level changes
	- When changes to the threat environment occur;
	- When substantive changes to the organization's IT infrastructure take place
	- After an exercise to incorporate findings.
SP4.8	The organization uniformly enforces its business continuity policy, plans and procedures.
SP4.9	Business Continuity Plans and Procedures are subject to internal audit.
SP4.10	Business Continuity Plans and Procedures are subject to external audit.

Service Providers / Third Parties Business Continuity Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for ensuring the availability and recovery of outsourced services to external organizations (e.g., third parties, collaborators, subcontractors, or partners)
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies meet its business continuity needs and requirements. Business continuity requirements on providers are included in formal terms in the contract.
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or is used by its own personnel.
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' business continuity policies and procedures for personnel who are involved with those external organizations.
SP5.5	Procedures as to how the disaster recovery providers will manage a multiple invocation of their sites is known, documented and agreed;
SP5.6	The organization uses more than one telecom providers for voice and data. The following interactions take place with providers:
	- Planned formal meetings take place to plan resilience of the communications network;
	- Planned verification takes place to check the resilience of telecoms providers' network architecture and of the connectivity and routing within it;
	- Verification of IT third party suppliers' disaster recovery capability.
SP5.7	Where outsourcing is used, critical IT outsourcing companies' business continuity management capabilities are audited.

Annex D – Asset Based Continuity Controls

Hardware and Network (HN)	
Resilience (HN.1.1)	
HN.1.1.1	**IT Infrastructure Documentation.** There is an up-to-date and detailed IT infrastructure diagram including network and hardware components.
HN.1.1.2	**IT Equipment Documentation.** The organization maintains detailed records of hardware and network components configuration / parameterization.
HN.1.1.3	**Information Systems Monitoring.** Network and system availability figures are monitored for trends as well as threshold exception basis and the information is used to identify points of throughput weakness (bottlenecks).
HN.1.1.4	**Information Systems Resilience.** The control requires the implementation of technologies such as clustering and load balancing for the resilience of hardware and network components.
HN.1.1.5	**Disaster Recovery Cross Training.** No critical hardware or network component depends on an individual person for restoration in a disaster.
HN.1.1.6	**Information Systems Distribution.** Critical IT hardware / network components are spread across diverse locations within the organization's premises.
HN.1.1.7	**Information Systems Hardening.** Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.
Back up (HN.1.2)	
HN.1.2.1	**Information Systems Backup.** Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and must be retained in good working condition.
HN.1.2.2	**Backup Restoration.** Appropriate procedures are present to assure the ability to restore from backup media under the following conditions: (a) changes of backup software version (b) changes of backup device hardware/firmware (including mechanical maintenance/service) (c) changes in the hardware configuration of the backed up system.
HN.1.2.3	**Backup Media Redundancy.** Backup clones are available to safeguard against damage of the original backup media. The cloned backup set is stored in a different location than the original.
HN.1.2.4	**Backup Fail-Over.** Where redundant systems are used, backup devices and software are in place to manage backups from a single, secondary system when the primary has failed. Care is taken to maintain compatibility of hardware, media types, software versions between the primary and the secondary system.
HN.1.2.5	**Staff Training.** Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.
Redundancy (HN.1.3)	

HN.1.3.1	**Information Systems Redundancy.** Network equipment and hardware modules are designed to be fully redundant with no single points of failure.
HN.1.3.2	**Information Systems Replication.** Alternative, stand-by equipment is in place to mirror the production systems in the case of a disaster. The equipment should be capable of replacing the primary equipment after loading the necessary data from the backup media.
HN.1.3.3	**Vendors SLAs.** The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.
Recovery Actions	
RA.1.1.2	Consult the configuration records to restore hardware / network component.
RA.1.1.5	Establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components
RA.1.2.1	Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules
RA.1.2.4	Use the secondary backup system to manage backups, if the primary has failed.
RA.1.3.1	Switch to manual procedures and restore hardware / software failure
RA.1.3.2	Use alternative, mirrored equipment to replicate the production system
RA.1.3.3	Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment

Application (A)	
Application Resilience (A.1.1)	
A.1.1.1	**Application Documentation..** The control requires the organization to identify and collect documents required to install and operate the application. This includes information on the environment (OS version, external libraries, etc) for the execution of the application. This documentation has to be verified and updated at least at every maintenance cycle of the BCP.Furthermore, if the application is custom the application code should be documented. The criticality of the application will dictate the level of documentation required.
A.1.1.2	**Application Staging.** The control requires that the application should undergo thorough testing on test servers before allowing it for production usage.
A.1.1.3	**Application Configuration Management.** A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.
A.1.1.4	**Application Maintenance and Patching.** Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.
A.1.1.5	**Application Hardening.** Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

A.1.1.6	**Application Vendors & SLAs..** The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented agreement exists between the two parties for technical support provisioning when required.
A.1.1.7	**Application Clustering..** The control requires the implementation of clustering technologies for the resilience of the application. The application is scaled out across multiple compute nodes to provide application's high availability and performance
A.1.1.8	**Application Monitoring.** Application availability figures are monitored for trends as well as threshold exception basis and the information is used to identify points of throughput weakness (bottlenecks).
Application Back up (A.1.2)	
A.1.2.1	**Application Backup.** Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules. When this control is applied to a service (such as email or internet provisioning) then establishing an alternate backup service is required in addition to backing up any relevant data.When considering backup of services that produce or store data the ability to have a usable local copy of the data or to transfer existing data to the backup service has to be considered and evaluated.
A.1.2.2	**Staff Training.** Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.
Recovery Actions	
RA.1.1.3	Consult the application's configuration records to repair / reinstall the application
RA.1.1.6	Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.
RA.1.2.1	Initiate backup procedure to restore the application software modules or Initiate the processof switching to the backup service provider.

Data (D)	
Data Storage (D.1.1)	
D.1.1.1	**Data Mirroring.** The control requires that all critical data are mirrored to additional storage media ensuring that data is written to two or more different disks (disk mirroring / raid array configuration) to ensure that two valid copies of the data are available. Ensure adequate monitoring is in place (prefferably with a persistent sound notification too) to avoid a failure of one of the storage media goes unnoticed until all copies have failed.
D.1.1.2	**Network Storage.** Data stored on end user devices (Laptops, workstations, etc) must be periodically synced to a networked disk (a single server with data storage capacity) or a networked storage device (network-attached storage (NAS) or storage area network (SAN)). In addition, the most recent backup of critical data or systems can be kept on the network storage for high speed restoration.
D.1.1.3	**Secure Remote Storage.** The control requires that on a daily basis, after imaging the servers to which it is attached, the Network Attached Storage (NAS) device creates an independent encrypted tunnel and transmits the imaged data to a secure offsite location where it resides in an encrypted, compressed format, creating a total of two copies of the data in two geographically distinct regions.

D.1.1.4	**Data Replication.** The control requires that all critical data are replicated to additional storage locations to ensure that two valid copies of the data are available. The second location can be a different branch office of the organization or a remote data center. Depending on the amount of data loss that can be tolerated and the cost of the technical solution a zero data loss or point in time implementation should be selected.
D.1.1.5	**Store Backup Media Offsite.** Backup media should be labelled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.
Data Backup (D.1.2)	
D.1.2.1	**Backup Rotation Schedules.** The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.
D.1.2.2	**Near Real-Time Backups.** The control requires an incremental methodology which captures all changes to the initial image in increments within minutes. The Incremental methodology not only backs up recent datasets but also allows end users to reconstruct the state of their data as it stood at the end of various minute-based restoration points.
D.1.2.3	**Backup System Flexibility.** The backup system should allow quick and flexible restoration of files, folders, partitions, mailboxes/messages and databases/tables. It should be possible to schedule restoration of data according to the pre-determined recovery priority. This is to be utilised when the time to restore the full datasets exceeds the target recovery times. Design your backup plan to meet the precise restoration time objectives. Order the backup sequence according to your recovery sequence to avoid time costly seeks on tapes. Create a precise map of the contents of each tape. If possible clone the backup sets to a hard disk storage to increase the speed of restoration.
D.1.2.4	**Internet Backup.** The control requires that workstation users (personnel) are allowed to back up data to a remote location over the Internet. Formal authorisation is required prior to the execution of this backup method.
D.1.2.5	**Data Backup.** Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.
Recovery Actions	
RA.1.1.1	If the mirrored set failes and cannot recover automatically revert to backup restration on new storage media. If data call a recovery expert. In any case make sure data salavage operation is performed on a copy and not on the original media, if possible.
RA.1.1.2	Restore data to the required information systems via the NAS / SAN
RA.1.1.3	Load backup data to the required information systems via the NAS / SAN. If the data are corrupted or irretrievable obtain data from the secondary site.
RA.1.1.4	Select one of the recovery strategies: a) Transfer IT operations to the location of the data. B) transport the replicated data to the designated recovery site c) Arrange for sufficient network BW and Q.o.S. (latency and delay) for the remote access of the data.
RA.1.1.5	Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.

RA.1.2.1	Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.
RA.1.2.2	Assess your ability to salavage near real-time backups if they are located at the incident site.
RA.1.2.3	If time limits are tight schedule the restoration of data according to the pre-determined recovery priority. Use a pre-compiled restoration sequence.
RA.1.2.4	Start retrieving Internet backups as soon as possible from a location providing good bandwidth and stable internet connection. Keep in mind internet speeds vary and BW bottlenecks may impose a critical delay to the download. Prioritise your downloads according to your needs.
RA.1.2.5	Initiate the backup plan to restore the damaged / lost data

People (P)	
Physical Security (P.1.1)	
P.1.1.1	**Actions Accountability.** Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for
P.1.1.2	**Physical Access Control.** Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.
P.1.1.3	**Clean Desk Policy.** A clean desk policy is in operation followed by all personnel, contactors and third parties
Awareness & Training (P.1.2)	
P.1.2.1	**Business Continuity Tool Set.** The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.
P.1.2.2	**Business Continuity Tests.** Staff, have been trained and involved in business continuity tests.
P.1.2.3	**Key Personnel Deputies.** All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfil their duties / responsibilities.
P.1.2.4	**Key IT Personnel Training.** The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a "business as usual" basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures
Recovery Actions	
RA.1.2.3	Business Continuity Deputies take over the duties of the staff responsible with business continuity responsibilities.

Facilities (F)	
IT Site (F.1.1)	
F.1.1.1	**IT Site Physical Access.** Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or

	similar physical access control technologies.
F.1.1.2	**IT Site Power Supply.** The power supply of the site equipment is protected with UPS and / or generators.
F.1.1.3	**IT Site Air-Conditioning.** IT site humidity, ventilation and air-conditioning are controlled.
F.1.1.4	**IT Site Anti-fire Systems.** Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.
F.1.1.5	**IT Site Anti-flood Systems.** IT Site is equipped with water detection systems and anti-flood mechanisms (raised floors, drop ceilings)
F.1.1.6	**IT Disaster Recovery Site.** There is an alternate dedicated site where IT is restored following a disaster.
F.1.1.7	**IT Site Recovery Plan.** Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.
F.1.1.8	**Secondary Disaster Recovery Site.** There is an additional secondary site with certain mechanisms in place for invoking it if the primary recovery site is not available.
Environmental Security (F.1.2)	
F.1.2.1	**Electrical Power Mechanisms.** All critical business functions are protected by uninterruptible power supply (UPS) or similar battery backup. In addition all areas and systems of the corporate facilities have their power supply backed up by generators. Power can be provided by generato
F.1.2.2	**Fire Fighting Equipment.** Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within corporate facilities
F.1.2.3	**Air-conditioning.** The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.
F.1.2.4	**Anti-flood Equipment.** There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.
F.1.2.5	**Electrical Power Protection.** Corporate facilities are protected against electrical spikes and surges (e.g. lightning strikes). In addition the control requires the proper grounding and shielding of the cables used to supply electrical power.
Physical Security (F.1.3)	
F.1.3.1	**Battle Boxes.** Sites use 'battle boxes' containing a variety of equipment selected to assist with the management and control of a business continuity incident. Alternatively, the organization keeps and maintains the materials required to help the recovery of business op
F.1.3.2	**Secure Delivery and Loading Area.** The control requires a documented policy for controlling introduction of packages or items within a dedicated post room which systematically inspects for threatening objects received by couriers and visitors.
F.1.3.3	**Facilities Access Control.** All critical sites have security guards (24 hours a day, 7 days a week), and / or internal / external CCTVs, access control systems and a standard access management security procedure.
F.1.3.4	**Rooms and Areas Secure Access.** Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to authorised personnel.
F.1.3.5	**Visitors Escort.** Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.
F.1.3.6	**ID Badges.** Permanent and temporary staff, contract staff and visitors required to wear visible id badges.

Recovery Actions	
RA.1.1.1	Once the emergency/incident is contained provide arrangements for the physical security of the incident site.
RA.1.1.2	Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and
RA.1.1.3	Verify air-conditioning operates normally. Make sure you can contact qualified technicians in case of failure.
RA.1.1.4	If the anti-fire systems were engaged, make sure the site is safe for personell(engage the fire department) before attempting to salvage any equipment.C23
RA.1.1.5	Be aware of the risk of electrical shock due to exposed wires to the water. Refresh the operating procedures and operate any anti-flood systems you might have in place or seek support from the emergency services. Monitor closely the condition as you might
RA.1.1.6	Evaluate the need to activate the disaster recovery site. Check site availability and announce the DR site location to be activated. Follow the activation plan
RA.1.1.7	On DR site activation implement the site recovery plan.
RA.1.1.8	Evaluate the need to activate the disaster recovery site. Check site availability and announce the DR site location to be activated. Follow the activation plan
RA.1.2.1	Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish the nature of the problem, coordinated course of action and
RA.1.3.2	Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.
RA.1.3.3	Once the emergency/incident is contained arrange for maintenace of a secure physical perimeter.

Annex E – Business Continuity Awareness

Why Business Continuity Management

Business Continuity should become part of the way business is performed. Organizations that have a business continuity capability are far more likely to survive the effects of a major incident than those that don't. It is better to plan for incidents, which may affect business-as-usual activities, rather than having to "cope with" when a problem occurs.

Business Continuity Management (BCM) ensures that the organization is able to respond to major disruptions that threaten its survival. BCM develops organization-wide resilience allowing an organization to survive the loss of part or all of its operational capability, providing an effective response **that safeguards the interests of its key stakeholders and customers, reputation, brand and value creating activities.** Because an organization's BCM resilience depends on its management and operational staff as well as technology and geographical diversity, this resilience must be developed throughout the organization from **senior management** across **all sites and the supply chain.**

Business Continuity Threats

Unplanned events can have catastrophic effects and the disruptive incidents can come from accidents, criminal activity or natural disasters. This section of the report provides an indicative list of continuity threats which could lead to an undesirable event, causing a negative impact to an asset in terms of asset interruption or loss/destruction. The nature of the potential threats has been categorized into three distinct types with respect to the source that triggers the actual threat. Specifically:

- Natural Disasters
- System Problems / Cyber Attacks
- Man Made Disasters

Natural Disasters

- **Accidental Fire.** Catching fire through an external event or internal accident e.g. lightning, waste-paper bin fire, short circuit.

  Output: Interruption, Loss/Destruction

- **Climatic Phenomenon.** Destruction or temporary shutdown of equipment, located in a geographical area prone to extreme heat, cold, humidity, wind or drought.

  Output: Interruption, Loss/Destruction

- **Meteorological Phenomenon.** Isolated atmospheric disturbance causing extreme climatic conditions such as storms, hail, lightning, avalanche etc

  Output: Interruption, Loss/Destruction

- **Seismic Phenomenon.** Earth tremor or earthquake causing extreme vibration or triggering a disaster (tidal wave) leading to temporal unavailability or permanent destruction of equipment.

  Output: Interruption, Loss/Destruction

- **Accidental Flood**. Flood due to pipe leakage from air-conditioning equipment, leakage from a water room on the floor above, fire nozzle open.

  Output: Interruption, Loss/Destruction

- **Accidental Failure of Air-Conditioning.** Failure, shutdown or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction or fail completely

Output: Interruption, Loss/Destruction

- **Electromagnetic Radiation**. Accidental: Electromagnetic interference from an internal or external device such as radar, radio antenna, electricity generating station etc. Deliberate: Person using stray radiation to jam or saturate communications or disturb the operation of an appliance

  Output: Interruption

- **Loss of Power Supply.** Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier's service or from the internal distribution system

  Output: Interruption, Loss/Destruction

System Problems / Cyber Attacks

- **Software Malfunction.** Design error, installation error or operating error committed during modification causing incorrect execution

  Output: Interruption, Loss/Destruction

- **Equipment Malfunction / Failure.** A logical or physical event causing an equipment item to malfunction and / or failure due to failure to follow equipment qualification procedures after updates/upgrades or use of equipment under conditions outside its operating limits (temperature, humidity).

  Output: Interruption, Loss/Destruction

- **Breach of Information System Maintainability.** Lack of expertise in the system making retrofitting and upgrading impossible; for example, inability to correct an operating problem on respond to new needs; failure of external software and hardware maintenance companies, termination of support contract leaving a lack of competency or resources for system upgrading.

  Output: Interruption

- **Saturation of the System (Denial of Service).** Accidental: Hardware, software or network resource inadequate for meeting users' needs due to overworking the machine (too many requests processed simultaneously). Deliberate: An attacker simulates an intense demand on resources by setting up continuous bombardment.

  Output: Interruption

Man-Made Disasters

- **Theft of Equipment.** Someone inside or outside the organization accessing equipment located on the premises or transported outside.

  Output: Interruption, Loss/Destruction

- **Deliberate Fire.** An impostor gaining access to property in order to set light to flammable or explosive materials directly or indirectly (incendiary bombs, tampering with ventilation devices, etc.)

  Output: Interruption, Loss/Destruction

- **Deliberate Flood.** An Impostor gaining access to the property to cause flooding in the rooms. Deliberate breakage of pipes, triggering of extinguishing systems or simply spraying the equipment

  Output: Interruption, Loss/Destruction

- **Deliberate Loss Of Power Supply**. Sabotage or disturbance of the electrical installation by someone gaining access to the equipment (head-end, low voltage transform inverter, etc.)

Output: Interruption, Loss/Destruction

- **Deliberate Failure Of Air-Conditioning.** A person can sabotage the equipment used to operate the air-conditioning system (cut off the water or power supply, destroy the system).

  Output: Interruption, Loss/Destruction

- **Destruction of Equipment or Media.** Accidental Cause: Negligence or accidental event causing destruction of equipment or media. Deliberate Cause: Person gaining access to equipment and causing its destruction.

  Output: Interruption, Loss/Destruction

- **Unauthorized Use of Equipment.** A person inside or outside the organization accesses the information system and uses one of its services to penetrate it, run operations or steal information.

  Output: Interruption, Loss/Destruction

Event –Incident Detection & First actions

A security incident is a suspected or possible security breach to one or more information resources. It is any adverse event whereby some aspect of information availability could be threatened, for example, by loss / destruction of data, denial of an information system's service and / or disruption of a business function. Incidents can be divided into two distinct categories:

- **Life threatening incident** - It affects personnel health and safety:
  - Fire
  - Earthquake
  - A colleague is injured
  - Other life threatening situation
- **Non-life threatening incident** – It affects the continuity of the business.
  - Saturation of system resources
  - Denial of Service
  - Loss / Destruction of information
  - Inability of suppliers to provide the agreed upon / required service level

An organization should develop a set of checklists which will include simple instructions / guidelines for the personnel that should be followed when a life or non-life threatening incident occurs. As a starting point the section provides two checklists; a life-threaten checklist namely **Fire Fighting Checklist;** and a checklist for the detection of and response to a business continuity incident, namely **Incident Detection and Action Checklist.**

Fire Fighting Checklist

All fires can be very dangerous and life-threatening. Personnel safety should always be the primary concern when attempting to fight a fire.

- **Before deciding to fight a fire, be certain that:**
  - The fire is small and not spreading. A fire can double in size within two or three minutes.
  - You have the proper fire extinguisher for what is burning.
  - The fire won't block your exit if you can't control it. A good way to ensure this is to keep the exit at your back.
  - You know your fire extinguisher works. Assure the pressure is at the recommended level. On extinguishers equipped with a gauge, the needle should be in the green zone - not too high and not too low.

- You know how to use your fire extinguisher. There's not enough time to read instructions when a fire occurs.

- **How to Fight a Fire Safely:**
  - Always stand with an exit at your back.
  - Stand several feet away from the fire, moving closer once the fire starts to diminish.
  - Use a sweeping motion and aim at the base of the fire.
  - If possible, use a "buddy system" to have someone back you up or call for help if something goes wrong.
  - Be sure to watch the area for awhile to ensure it doesn't re-ignite.

- **Never Fight A Fire If:**
  - **The fire is spreading rapidly**. Only use a fire extinguisher when the fire is in its early stages. If the fire is already spreading quickly, evacuate and call the fire department.
  - **You don't know what is burning.** Unless you know what is burning, you won't know what type of fire fighting equipment to use; there could be something that will explode or produce highly toxic smoke.
  - **You don't have the proper fire fighting equipment**. The wrong type of fire-fighting equipment can be dangerous or life-threatening.
  - **There is too much smoke or you are at risk of inhaling smoke**. Seven out of ten fire-related deaths occur from breathing poisonous gases produced by the fire.

- **In case that you are not able to evacuate the building / office due to blocked exits:**
  - Seal all gaps under doorways and windows with dry towels and duct tape.
  - Turn off heating, cooling or ventilation systems.
  - Protect your breathing, cover your nose and mouth with a dry handkerchief or other cloth folded over several times.
  - Use any fire-fighting equipment available or any other manual technique in case that you must constrain fire dispersion towards your temporal shelter.

- **Note:** Any sort of fire will produce some amount of carbon monoxide, the most deadly gas produced by a fire. Materials such as wool, silk, nylon and some plastics can produce other highly toxic gases such as carbon dioxide, hydrogen cyanide, or hydrogen chloride. Beware - all of these can be fatal.

Incident Detection and Action Checklist

A sample checklist which defines a business continuity incident instructing personnel to carry out specific actions in the case of a non-life threatening incident is the following:

- **Do we have an incident?**
  - Is there an indication or evidence that :
    - Access to facilities / offices will be impossible?
    - Equipment has or is about to fail?
    - Telecommunications services have or about to be unavailable for an unacceptable amount of time?
    - Data could or are lost / destroyed?
    - IT equipment or applications have a severely degraded performance or totally unavailable?
    - Evidence of computer hacking or cyber attack?
    - Absence of an unusually high number of colleagues.
    - Complaints from clients or third parties for the quality of the offered service or product.

- **If you answered yes to any of the above questions then:**
  - Contact the leader of the incident response team or his deputy; keep trying to contact the first available person in the communications tree.
  - Provide all the known information and support to assist the Incident Response Team to control the incident.
  - Prepare to take up your pre-defined role in the BCP and / or any other plan / procedure that you may be involved.

Personnel Health and Safety EU Legislation

EU legislation obliges organizations -operating within EU member states- to ensure employees health and safety. Specifically, **OJ L 393, Council Directive 89/391/EEC (12/6/1989) includes the minimum requirements for the workplace, obliging employers to provide certain health and safety protection measures.** OJ L 393, Council Directive 89/391/EEC (12/6/1989) has been further expanded to individual Directives in order cover certain health and safety issues within the following topics:

- **Work places** (OJ L 393, Council Directive 89/654/EEC concerning the minimum safety and health requirements for the workplace - first individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Work equipment** (OJ L 393, Council Directive 89/655/EEC concerning the minimum safety and health requirements for the use of work equipment by workers at work - second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Personal protective equipment** (OJ L 393, Council Directive 89/656/EEC minimum health and safety requirements for the use by workers of personal protective equipment at the workplace - third individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Work with visual display units** (OJ L 156, Council Directive 90/269/EEC on the minimum health and safety requirements for the manual handling of loads where there is a risk particularly of back injury to workers - fourth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Handling of heavy loads involving risk of back injury** (OJ L 156, Council Directive 90/270/EEC on the minimum safety and health requirements for work with display screen equipment - fifth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Temporary or mobile work sites** (OJ L 196, Council Directive 90/394/EEC on the protection of workers from the risks related to exposure to carcinogens at work - sixth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- **Fisheries and agriculture** (OJ L 391, Council Directive 90/679/EEC on the protection of workers from risks related to exposure to biological agents at work - sixth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)

Annex F – Business Continuity Plan Template

The annex presents the Business Continuity Plan Template produced by the execution of the proposed BCM approach described in the current document. The Plan is created gradually as the Assessment Team executes the various steps. The BCP template exists as a separate document for the company used within the example of chapter *5. Self Assessment Guidelines with one example*.

Available as a separate document: BCM_for_SME_Example_BCP-Template

Annex G – Useful Templates

Available as a separate document BCM_for_SMEs_Annexes_G-H_Assessment_Templates

Annex H – Asset Types List

Available as a separate document BCM_for_SMEs_Annexes_G-H_Assessment_Templates

Annex I – List of Figures and Tables