University of Piraeus
Department of Digital Systems
MSc Security of Digital Systems

BUSINESS CONTINUITY

Name: Stamatopoulou Syrmoula

Supervisor: Prof. K. Lambrinoudakis

Executive Summary

Companies, organizations and institutes which provide critical services and are connected with vulnerable processes, is crucial to ensure the availability of these. According to the report released by the AXA Company, and which was published in 2007, “80% of businesses affected by a major incident either never re-opened or closed within 18 months”. To prevent such catastrophic consequences, companies should establish mechanisms and procedures to ensure the business continuity after a disastrous event. This is provided by the development and implementation of a Business Continuity Plan (BCP).

The main objective of the current study is the examination and presentation of the Business Continuity Management (BCM) and Business Continuity Plan (BCP) processes. Targeted standards, guidelines and methodologies of BCP, are examined and presented in order to cover different areas of business operations. Specifically, these are the BS 25999 (covers the entire range of a business operation), the NIST SP 800-34 (contingency planning guide for Information Technology Systems for government institutions), the ENISA (an approach for Small Medium Sized Organizations focus on IT Systems), the FFIEC (Business Continuity Planning for financial institutes) and the Bank Of Greece Governor’s Acts 2577 9.3.2006 - Annex 2 (for Systemically Important Payment Systems – SIPSs).

Finally, a case study which is based on the guidelines given by the Bank Of Greece will be presented at the end of this document. The case study concerns the BCP creation by a hypothetical medium financial institute (bank) that provides services only via telecommunication networks (internet and telephone) and services through Automated Teller Machine (ATM) and Point Of Sale (POS).

Περίληψη εργασίας Επιχειρησιακής Συνέχειας

Την τελευταία δεκαετία έχει διαπιστωθεί ότι οι εταιρείες και οι οργανισμοί που παρέχουν κρίσιμες υπηρεσίες, οι οποίες συνδέονται με ευάλωτες διαδικασίες, πρέπει να εξασφαλίσουν την διαθεσιμότητα αυτών. Σύμφωνα με μία αναφορά της εταιρίας AXA που δημοσιοποιήθηκε το 2007, «το 80% των εταιριών που πλήγονται από ένα καταστροφικό γεγονός είτε δεν ξαναλειτουργούν είτε κλείνουν μετά από 18 μήνες». Για να αποφευχθούν τέτοιου είδους καταστροφικές συνέπειες, οι εταιρείες θα πρέπει να θεσπίσουν μηχανισμούς και διαδικασίες ώστε να εξασφαλίζεται η συνέχεια της επιχειρηματικής δραστηριότητας μετά από ένα καταστροφικό συμβάν. Αυτό μπορεί να επιτευχθεί σχεδιάζοντας και εφαρμόζοντας ένα Σχεδίου Επιχειρησιακής Συνέχειας (ΣΕΣ).

Ο σκοπός αυτής της εργασίας είναι η μελέτη και η παρουσίαση των διαδικασιών της Διαχείρισης και του Σχεδίου Επιχειρησιακής Συνέχειας. Για την επίτευξη αυτού του στόχου μελετήθηκαν κάποια από τα ποίο διαδεδομένα πρότυπα/οδηγίες και αποτυπώθηκαν πέντε από αυτά. Τα πρότυπα αυτά επιλέχτηκαν έτσι ώστε να καλυφτούν διάφορα πεδία εφαρμογής της Επιχειρησιακής Συνέχειας σε σχέση με τις επιχειρησιακές δραστηριότητες μίας εταιρίας. Ποίο συγκεκριμένα, το πρότυπο BS25999 στο οποίο καλύπτεται όλο το φάσμα της λειτουργίας μιας επιχείρησης, οι οδηγίες του NIST (SP800-34) για δημιουργία Σχεδίου Συνέχειας των πληροφορικών συστημάτων των κυβερνητικών ιδρυμάτων, μια προσέγγιση του ENISA για τις μικρομεσαίες επιχειρήσεις με επίκεντρο τα πληροφοριακά συστήματα, το ΣΕΣ για τα οικονομικά ιδρύματα από τον FFIEC και οι οδηγίες της Τράπεζας της Ελλάδος (Π.Δ. 2577 9.3.2006 – Παράρτημα 2) για τα τραπεζικά συστήματα πληρωμών.

Στην συνέχεια πραγματοποιείται η σύγκρισή των πέντε προτύπων/οδηγιών, καταλήγοντας στο συμπέρασμα ότι παρόλο που προσεγγίζουν το θέμα από διαφορετικές οπτικές γωνίες, ακολουθούν πολλές κοινές διαδικασίες. Μέσα από αυτήν την σύγκριση είναι εμφανές ότι δεν μπορεί να χαρακτηριστεί κάποιο από αυτά ως η καλύτερη λύση και ουσιαστικά οποιαδήποτε από αυτά μπορεί να υλοποιηθεί σε έναν οργανισμό/εταιρία.

Τέλος, προσκομίζεται μια μελέτη περίπτωσης για την δημιουργία ενός ΣΕΣ, το οποίο εναρμονίζεται με τις μοναδικές Ελληνικές οδηγίες που μελετήθηκαν σε αυτήν την εργασία (Π.Δ. 2577 9.3.2006). Ποίο αναλυτικά, αποτυπώνονται τα βήματα που πρέπει να ακολουθηθούν για την δημιουργία, υλοποίηση και συντήρηση του σχεδίου χρησιμοποιώντας τις ανάγκες μίας υποθετικής μεσαίας Ελληνικής τράπεζας, η οποία παρέχει υπηρεσίες μόνο μέσω τηλεπικοινωνιακού δικτύου (τηλέφωνο και internet), αυτομάτων μηχανών ανάληψης μετρητών (ATM) και σημείων πωλήσεων (POS). Για αυτήν την περίπτωση επιλέχτηκε ως αφετηρία οι ανάγκες μια υποθετικής τράπεζας διότι το πληροφοριακό σύστημα των οικονομικών ιδρυμάτων παρουσιάζει ενδιαφέρον περεταίρω μελέτης λόγο της πολυπλοκότητας του.

Contents

CONTENTS **4**

1. INTRODUCTION **5**

1.1 AIM 6
1.2 OBJECTIVES 6

2. BUSINESS CONTINUITY MANAGEMENT AND PLAN **7**

2.1 OVERVIEW 7
2.2 BC STANDARDS, GUIDELINES AND METHODOLOGIES 9

3. BS 25999 - BUSINESS CONTINUITY MANAGEMENT **11**

3.1 OVERVIEW 11
3.2 PART 1: CODE OF PRACTICE 11
3.3 PART 2: SPECIFICATION 16
3.4 CONCLUSION 18

4. NIST SPECIAL PUBLICATION 800-34 ..... **19**

4.1 OVERVIEW 19
4.2 IT CONTINGENCY PLANNING PROCESS 19
4.3 CONCLUSION 24

5. ENISA - BUSINESS CONTINUITY FOR SMES **25**

5.1 OVERVIEW 25
5.2 IT CONTINGENCY PLANNING PROCESS 25
5.3 CONCLUSION 32

6. FFIEC - BUSINESS CONTINUITY PLANNING **33**

6.1 OVERVIEW 33
6.2 BUSINESS CONTINUITY PLANNING PROCESS 33
6.3 CONCLUSION 37

7. BANK OF GREECE G.A. 2577 9.3.2006 - ANNEX 2 ..... **38**

7.1 OVERVIEW 38
7.2 IT CONTINGENCY PLANNING PROCESS 38
7.3 CONCLUSION 40

8. COMPARISON OF BC STANDARDS/GUIDELINES **41**

9. CASE STUDY **44**

9.1 OVERVIEW 44
9.2 BUSINESS IMPACT ANALYSIS (BIA) 44
9.3 DEVELOPING BCP AND DRP 54

10. CONCLUSIONS **57**

BIBLIOGRAPHY / REFERENCE **58**

1. Introduction

Nowadays, most of companies and organizations in order to achieve their proper function have to establish general principles and objectives (policies) that define a broader framework of obligations and rules in order to attain their objectives.

The policies that are related to the organization's strategy plan are called security policies and define how to protect a company's critical information, physical infrastructure and Information Technology (IT) assets. Through the security policy, a company defines its objectives, commitments, roles/responsibilities and policy statements. This policy is created based on the results of Risk Management, the legislation of the country and policy relative's standards/guidelines. A security policy should include:

- General Policies

This covers a specific business area without details. This can be a modular security policy, a single document with appendices that describe the individual policies (it can be a form of hypertext).

- Specific Policies

Policies relate to specific areas of security and can be computer (implemented technically) or human oriented (applied by users) or individual security policies (per system or application). For example:

    - User Responsibilities Security Policies (human-oriented).
    - Remote Access Security Policies (computer-oriented).
    - Internet Acceptable Use Security Policies (individual security policies - human-oriented).
    - Email Acceptable Use Security Policies (individual security policies - human-oriented).
    - Passwords Security Policies (individual security policies).
    - Security Policy for Operating Systems (computer-oriented).
    - Business Continuity Policy (individual security policies).

- Security Procedures

  These are guidelines which provide detailing procedures for specific operations. For example:

    - Account creation procedure.
    - Backup – Restore procedure.
    - Update Operation System procedure.

- Technical Manuals and Instructions

  Through the technical manual the security procedures can be applied based on step-by-step technical instructions.

All security procedures and instructions are implemented based on the appliance of security measures and security controls.

1.1 Aim

The aim of this assignment is to present the creation process of the Business Continuity Management and Plan, which is a part of a security policy. Firstly, the purpose and necessity of BCM and BCP is going to be analysed. Secondly, some standards, guidelines and methodologies will be presented in this document that can be applied from a company/organization in order to ensure the effectiveness of the BCP. Finally, a case study will be presented for BCP of a medium financial institute.

1.2 Objectives

The main objectives are:

- The importance of the Business Continuity Management and Plan;
- Examination and presentation of the targeted standards, guidelines and methodologies of BC;
- Comparison of Business Continuity standards/guidelines;
- Present a case study for BCP of a medium financial institute; and
- Conclusions for BC.

2. Business Continuity Management and Plan

2.1 Overview

The Business Continuity Management (BCM) is a vital part of one organizations' global strategy and policy. Through this management process the organization can identify the threats and the business impact of these. A treat is an action that can interrupt the normal business operation and can be caused by different events. For example:

- Natural disasters and accidents such as floods, storms, fires;
- Failure of utilities and corruption of Information Technologies (IT) systems (e.g. electricity, telecommunications etc);
- Human threat (malicious actions or accidents);
- Loss, corruption or theft of data/documents/critical information;
- Breach of confidentiality.

According the type of event and the business area that effect, the organization will undergo the proportional business impact, such as:

- Financial loss;
- Loss of reputation or public confidence;
- Failure to deliver a service;
- Impact on stakeholders.

When the organization realizes the threats and the impact then has to proceed to the next step which is to apply policies and processes so as to minimize the time of the interruption of business operations and reduce the impact of disaster. All these processes address not only the restoration of IT infrastructure, but also focus on the rapid recovery and resumption of critical business functions for the fulfilment of business obligations.

The organization can formalize and adopt a BCM framework by creating documented continuity plans (table 2.1). There are various plans that are being related to each other (figure 2.1), companies (usually the small and medium) often create and implement a Business Continuity Plan (BCP) which may include various continuity plan components according to their needs.

The scope of a BCP is to gather documents and implement all the procedures which will be enabled during an interruption of critical business services so the organization can return to "business as usual" and minimise the effects of any disruption. The primary aim of this plan is not to prevent the disruption but to minimize its effects.

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

Table 2.1 Contingency Plans Components [1]

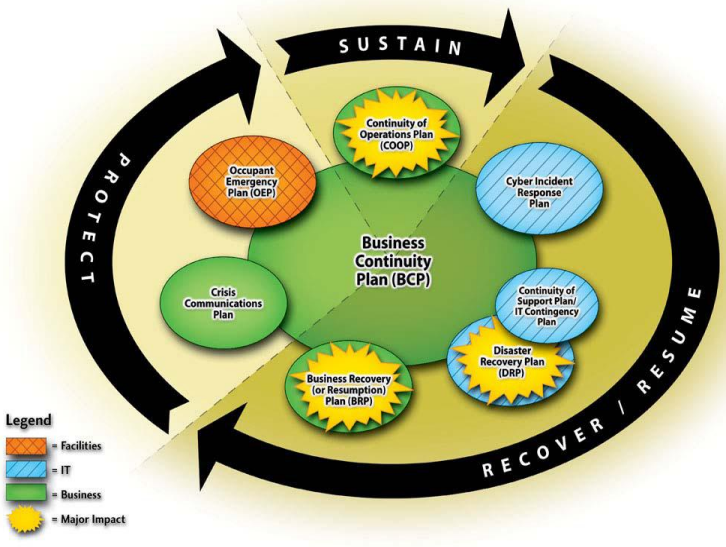

Figure 2.1 Interrelationships of Emergency Preparedness Plans [1]

The company/organization that adopts BCP gains some commercial benefits. This improves the overall efficiency of a business, by eliminating the downtime of the critical services. Also, when a company applies the BCP it becomes more attractive to costumers and thus it a competitive advantage.

As time consuming and tedious is the process of BCP creation, more difficult is the regularly reviewing and testing of the plan. Nevertheless, this is the only way for organization to ensure the effectiveness of the BCP.

2.2 BC standards, guidelines and methodologies

There are a lot of standards, guidelines and methodologies which address the issue of Business Continuity Plan, Business Continuity Management and Disaster Recovery Plan. Some of them are included in the table 2.2. Five of them will be presented in this assignment in order to cover different areas of business operations (global BCP, IT BCP, IT BCP for Small and Medium Enterprise, BCP for financial institutes, and BCP for Systemically Important Payment Systems).

Standard/Methodology/Guideline	Vendor	Country	Description
APS 232 Business Continuity Management [13]	Australian Prudential Regulation Authority (APRA)	AU	Brief documents which describe the required BC standards for authorised deposit-taking institutions to increase their resilience to business disruption.
ASIS SPC. 1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use [14]	American National Standard (ANS)	USA	Provides a framework for action planning and decision making for respond, recognise and recover from a disruptive incident (emergency, crisis, disaster).
GA.BG 2577 9.3.2006 - Annex 2 [12]	Bank of Greece	GR	Instruction for financial institution about BCP and DRS.
BS 25999-1 - Business Continuity Management Code of Practice [2]	British Standards Institute (BSI)	UK	Establishes the process, principles and terminology of BCM.
BS ISO/IEC 24762:2008 Information Security Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services [15]	British Standards Institute (BSI) and International Standards Organization (ISO)	UK	Provides guidelines on the provision of ICT DR services as part of BCM.
ENISA - IT Business Continuity Management. An approach for Small Medium Sized Organizations [10]	European Network and Information Security Agency (ENISA)	EU	A simplified and comprehensive view of IT Continuity/BCM for use within small and medium sized enterprises.
HB 292-2006 A Practitioners Guide to Business Continuity Management [16]	Standards Australia	AU	A very detailed Handbook describing all the elements required to develop, implement and maintain a BC programme.

HB 221:2004 Business Continuity Management [17]	Standards Australia and Standards New Zealand	AU and NZ	Covers all of the main elements of BCP and provides some useful examples, templates and checklists.
ISO/PAS 22399:2007 Societal Security – Guideline for Incident Preparedness and Operational Continuity Management [18]	International Standards Organization (ISO)	CH	Based upon the BS 25999-1, HB 221:2004 and NFPA 1600:2004 standards and as such contains the familiar elements of BCM.
FEMA 141 Emergency Management Guide for Business and Industry [19]	Federal Emergency Management Agency (FEMA)	USA	Predominantly aimed at the development of an incident response or management plan, but does not cover the continuity arrangements for the critical activities within the organisation
FFIEC - Business Continuity Planning [11]	Federal Financial Institutions Examination Council (FFIEC)	USA	Guidance for evaluating the financial institution and service provider risk management process to ensure the availability of critical financial services.
FSA BC Management Practice Guide [20]	Financial Services Authority (FSA)	UK	Aimed at financial organisations and is more of a guide to inform organisations about what should be included in their plans rather than a guide to tell them how to plan
CObIT [21]	Information Systems Audit and Control Association (ISACA), and IT Governance Institute (ITGI)	USA	A set of best practices (framework) for information technology (IT) management.
NFPA 1600:2004 Standard on Disaster/Emergency Management and Business Continuity Programmes [22]	National Fire Protection Association (NFPA)	USA	Address the elements of BCP, focused on emergency management and multi agency collaboration
NIST 800-34 Contingency Planning Guide for Information Technology Systems [1]	National Institute of Standards and Technology (NIST)	USA	A fairly comprehensive guide for the development of a BCP, focused on IT Service Continuity
Pas 77: 2006 IT Service Continuity Management [23]	British Standards Institute (BSI)	UK	Introduces IT Service Continuity Management which contains elements of BCP.
ITIL V3 [24]	The Stationery Office (TSO)	UK	Based on ISO/IEC 20000 and the ISO 9000 to provide continual service improvement.

Table 2.2 BC Standard/Methodology/Guideline

3. BS 25999 - Business Continuity Management

3.1 Overview

The British Standards Institution (BSI) has produced a standard about Business Continuity Management (BCM), named BS 25999. This standard consists of two parts:

- "BS 25999-1:2006 Business Continuity Management. Part 1: Code of Practice", which was released on November of 2006 and provides general guidelines, recommendations and processes of Business Continuity Management. In addition, it supplies a comprehensive set of controls based on BCM best practice and covers the whole BCM life-cycle.

- "BS 25999-2:2007 Business Continuity Management. Part 2: Specification", which was released on November of 2007 and describes only relevant requirements of a documented Business Continuity Management System (BCMS) within the context of managing an organization's overall business risks.

3.2 Part 1: Code of Practice

This method specifies six steps of the BCM life-cycle (as illustrated by Figure3.1).

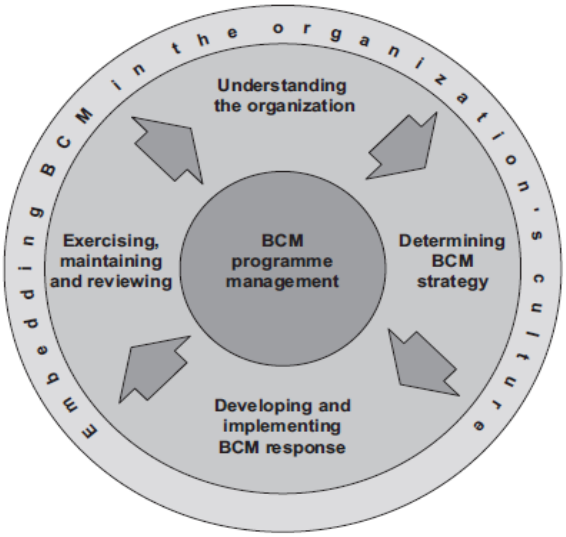

Figure 3.1: BCM life-cycle [2]

1) BCM programme management

The core of the BCM process is the programme management. This function facilitates the establishment of the Business Continuity capability and its maintenance in a manner appropriate to the size and complexity of the organisation. The objectives of the Business Continuity policy can be carried out with the use of the BCM programme.

BCM programme management involves three elements:

- Assigning responsibilities.

  The business management should designate an employee who will be in charge of BCM policy and effectuation. This employee is supposed to have the overall responsibility for BCM and he will be directly accountable for ensuring the continuous success of this capability. Additionally, the management should assign to one or more people the responsibilities regarding the implementation and maintenance of the BCM programme. Finally, it essential the new roles and

responsibilities of the BCM to be integrated into job descriptions and skill sets. Simultaneously, the organization's audit process should review the responsibilities of these new roles.

- Implementing business continuity in the organization.

  The implementation of Business Continuity programme must first pass through the stages of designation and build-up and then to the implementation of the programme. The company should notify the programme to all the parties who are interested and also provide appropriate training to employees in order to be able to exercise the Business Continuity capability. It would be necessary that a project management method will ensure that the implementation is effectively managed.

- The ongoing management of Business Continuity.

  Ongoing management activities should assure that Business Continuity is an integral part of the company. In order to achieve this, it is necessary for all the elements of the Business Continuity to be adapted to the organization's evolutions and needs. This means that the policy and plans of the Business Continuity should be updated whenever there is a significant change in the organization's operating environment (personnel, processes or technology).

  Furthermore, documentation must be created about Business Continuity, which may include the Business Continuity policy and plan; the Business Impact Analysis (BIA), the risk-threat assessment, the awareness-training programme and Business Recovery Plans (BRP).

2) Understanding the organization

The activities associated with "Understanding the organization" help to prioritize the organization's key products and services as well as the critical activities and resources that are associated with them. Through this step of BCM life-cycle, the organization can select an appropriate BCM strategy based on the organization's main objectives.

The key steps in this phase are:

- The scope of BCMS.

  Determine the organization's objectives, activities, assets and resources.

- Business Impact Analysis.

  Through this process the organization should determine and document the impact of a disruption to the activities that are associated with the critical products and services.

- Identification of critical activities.

  The activities of an organization are being categorized according to their significance and their priority for recovery.

- Determining continuity requirements.

The organization should take into consideration all the resources such as: people, premises, technology, information, supplies and stakeholders that each activity will require upon resumption.

- Evaluating threats to critical activities (undertaking a risk assessment).

  The threats to the resources of critical activities should be identified and recorded. Also, it is important to define the vulnerabilities of these resources, as well as the impact that would arise in case that a threat will cause an incident and therefore a business disruption.

- Determining choices.

  The final step is that the organization should identify measures (that are known as loss mitigation and risk treatment) that reduce the probability of interruption, minimize the period of disruption and mitigate the disruption of critical products and services.

  The strategies that are going to be used for the reduction of loss should be formulated in combination with other approaches, because not all risks can be prevented or reduced to an acceptable level. A strategy may be the acceptable of risk without any further action being taken. In some circumstances the impact of a risk might be outside the organization's normal risk appetite, but due to the low likelihood of the risk occurring and/or the uneconomic cost of control, top management may accept the risk. In other case for some risks the best response may be to transfer them using insurance or arrangements. This option is particularly good for mitigating financial risks or risks to assets. Additionally, in some circumstances it might be appropriate to change, suspend or terminate the service, product, activity, function or process if this has a limited lifespan.

3) Determining Business Continuity strategy

As soon as an organization or company has clarified the prioritization of its own products and services, it will be in a position of choosing the appropriate continuity strategies to enable them to meet the objectives.

The aim of this phase is to enable the organisation to demonstrate the extent to which its strategies and plans are complete, current and accurate, and to identify opportunities for improvement.

The strategy should include the organizations' critical activities and resources (people, technology, information, premises etc.) that each activity will require on its resumption.

4) Developing and implementing a BCM response

At this BCM life-cycle stage the organization should develop and implement plans (Incident Management Plan and Business Continuity Plan or Business Recovery Plan)

to ensure the continuity of critical activities. The response plans must cover all the phases of an incident (figure 3.2).

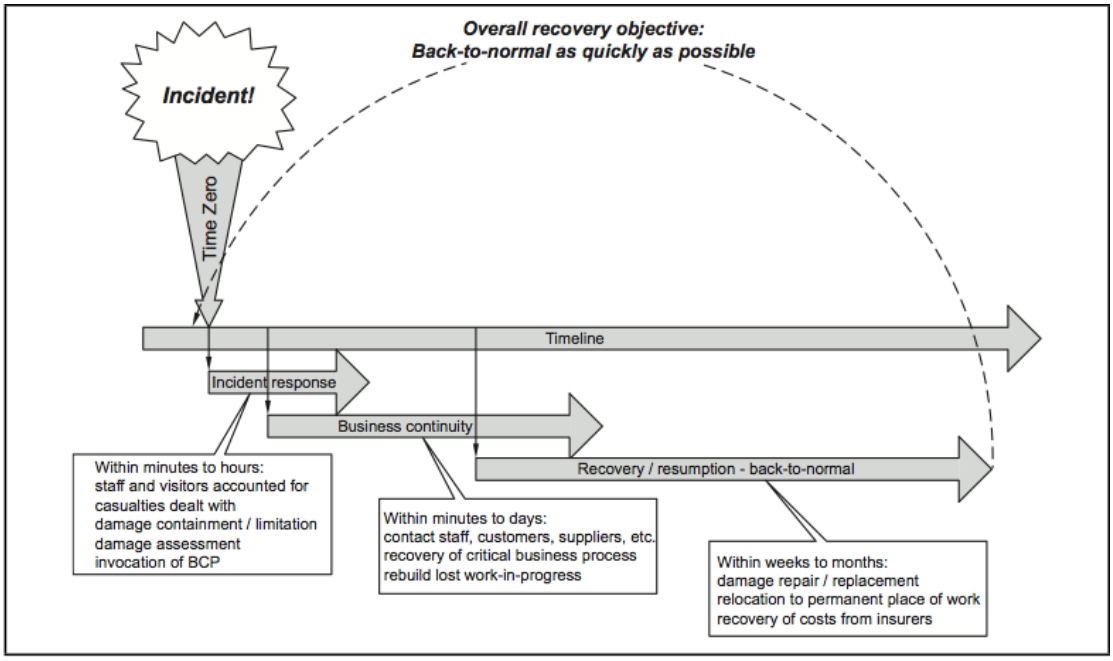

Figure 3.2: BCM response plan [2]

Based on the Incident Management Plan (IMP) the organization can manage the initial phase of an incident. The contents of the IMP can be:

- Purpose and scope;
- Roles and responsibilities;
- Plan invocation;
- Document owner and maintainer;
- Contact details;
- Task and action lists;
- Emergency contacts;
- People activities;
- Media response; and
- Stakeholder management.

The scope of Business Continuity Plan (BCP) is to secure the fastest and smoothest recovery of critical activities in the case of a disruption event to normal business operations. The contents of the BCP can be:

- Purpose and scope;

- Roles and responsibilities;
- Plan invocation;
- Document owner and maintainer;
- Contact details;
- Action plans/ task lists;
- Resource requirements;
- Responsible person(s); and
- Forms and annexes.

5) BCM exercising, maintaining and reviewing BCM arrangements

This phase provides that the BCM is updated through exercise, maintenance and review. The organization through these arrangements will be aware of the effectiveness of the plan and strategy.

6) Embedding BCM in the organization's culture

The final step of the BCM life-cycle is to embed BCM in the organization's culture and through this BCM becomes a part of the organization's core values. Incorporating the BCM in the organization's culture can offer the following advantages:

- *Develop a BCM programme more efficiently;*
- *Instil confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions;*
- *Increase its resilience over time by ensuring BCM implications are considered in decisions at all levels;*
- *Minimize the likelihood and impact of disruptions. [2]*

According to the British Standards Institution [2] in order for the development to be successful, the BCM culture must be supported by:

- *Leadership from senior personnel in the organization;*
- *Assignment of responsibilities;*
- *Awareness raising;*
- *Skills training; and*
- *Exercising plans.*

3.3 Part 2: Specification

The second part of the BS 25999 (BS 25999-2:2007 Business Continuity Management. Part 2: Specification) defines the requirements for implementing a documented Business Continuity Management System (BCMS).

This emphasizes the importance of:

- *Understanding business continuity needs and the necessity for establishing policy and objectives for business continuity;*
- *Implementing and operating controls and measures for managing an organization's overall business continuity risks;*
- *Monitoring and reviewing the performance and effectiveness of the BCMS; and*
- *Continual improvement based on objective measurement. [3]*

BS 25999-2 has adopted the PDCA[1] (Plan-Do-Check-Act) cycle for developing, implementing and improving the effectiveness of an organization's BCMS (figure 3.3). This ensures compatibility with other management systems standards such as "BS ISO/IEC 27001:2005 - Information Security Management Systems" and "BS ISO/IEC 20000:2005 - IT Service Management".

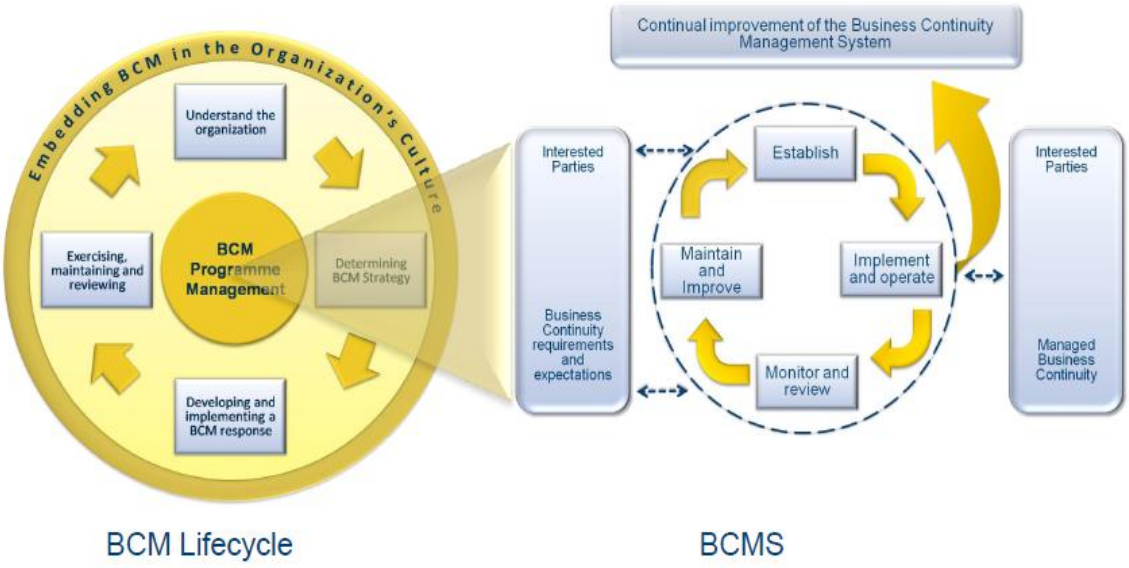

Figure 3.3: BCM and BCMS lifecycle [4]

[1] The Plan-Do-Check-Act methodology is based on the work of Walter Stewhart who developed statistical process control in the US during the 1930s. It was taken up and promoted very effectively from the 1950s and onwards by the famous quality management authority, W. Edwards Deming, and is used extensively to achieve continuous improvement in management systems.

1) Establishing and Managing the BCMS (PLAN)

The organization defines the scope and policy of BCMSs. Additionally it establishes the processes of managing risk and improving Business Continuity based on the general organization's policies. Also, this should incorporate the Business Continuity Management into the normal operations and management processes of the organization.

The documentation is a part of the BCMS, which should be controlled and protected by document release and authorisation processes. As a minimum the BCMS should include the following topics to documentation:

- The BCMS policy and objectives;
- The scope of the BCMS;
- Procedures and controls in support of the BCMS;
- A description of the risk assessment methodology;
- The risk assessment report;
- The risk treatment plan;
- Resource provision;
- Role and responsibilities of the participants;
- Incident response structure and plan; and
- Business continuity plan.

2) Implementing and Operating the BCMS (DO)

In this phase, the implementation and operation of the Business Continuity policy, controls, processes and procedures will take place. During this a number of operations will take place:

- Understanding the Organization.
    - Business Impact Analysis;
    - Risk Assessment; and
    - Determining Choices.
- Determining BC strategy.
- Developing and implementing a BCM response.
    - Incident response structure;
    - Incident management plan; and

    - Business continuity plan.

- Exercising, maintaining and reviewing BCM arrangements.

3) Monitoring and Reviewing the BCMS (CHECK)

The responsible employees monitor and review the effectiveness and efficiency of Business Continuity policy, objectives and scope, and after that they should report the results to management for review. Additionally, during this phase they should determine and authorize actions for maintenance and improvement.

Also, the organization should conduct internal audits at regular intervals to determine whether the objectives, controls, processes and procedures of its BCMS are being effectively implemented and maintained.

4) Maintaining and Improving the BCMS (ACT)

The organization in order to ensure effectiveness and efficiency of BCMS, has to maintain and improve it by taking corrective and preventive actions, based on the results of management review (in the previous phase). A range of activities such as audits, event analysis, identifies corrective and preventive actions or management reviews is involved. The management review will determine a range of actions that need to be taken.

3.4 Conclusion

The British standard BS25999 provides an integrated approach for Business Continuity Management process for an organization, by adopting the PDCA methodology for the documented BCMS. According to BS 25999 part 1, BCM is: *"A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities."*

A range of steps should be completed for the effectiveness of the BCP. First of all, the organization should define the scope of BCMS and after that to implement BIA and Risk Assessments so as to determine the continuity requirements and BCM strategy. Moreover, the BCP should be exercised, maintained and reviewed at regular periods of time (at least once a year). Finally, is important the organization to incorporate BCM in the organization's culture.

What is important to be mentioned finally, is that this standard has been used as the basis for many methodologies related to Business Continuity.

4. NIST Special Publication 800-34

4.1 Overview

The Information Technology (IT) system is one of the critical components of business processes. The needs of availability and effectiveness of IT system is crucial because the success of the organization is depended on the services that are being provided by the IT system. Based on this point of view, the National Institute of Standards and Technology (NIST) published on June 2002, a guidance "NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems" that provides instructions, recommendations, and considerations for government IT contingency planning. Although this guidance was designed for federal systems, it has been adopted as the guideline for contingency planning from the private organizations as well.

This guidance determines seven steps of contingency process which an organization can adopt and apply to their contingency planning program for their IT systems (section 4.2). These steps are being designed in order to be integrated into each stage of the system development life cycle (SDLC) (figure 4.1).

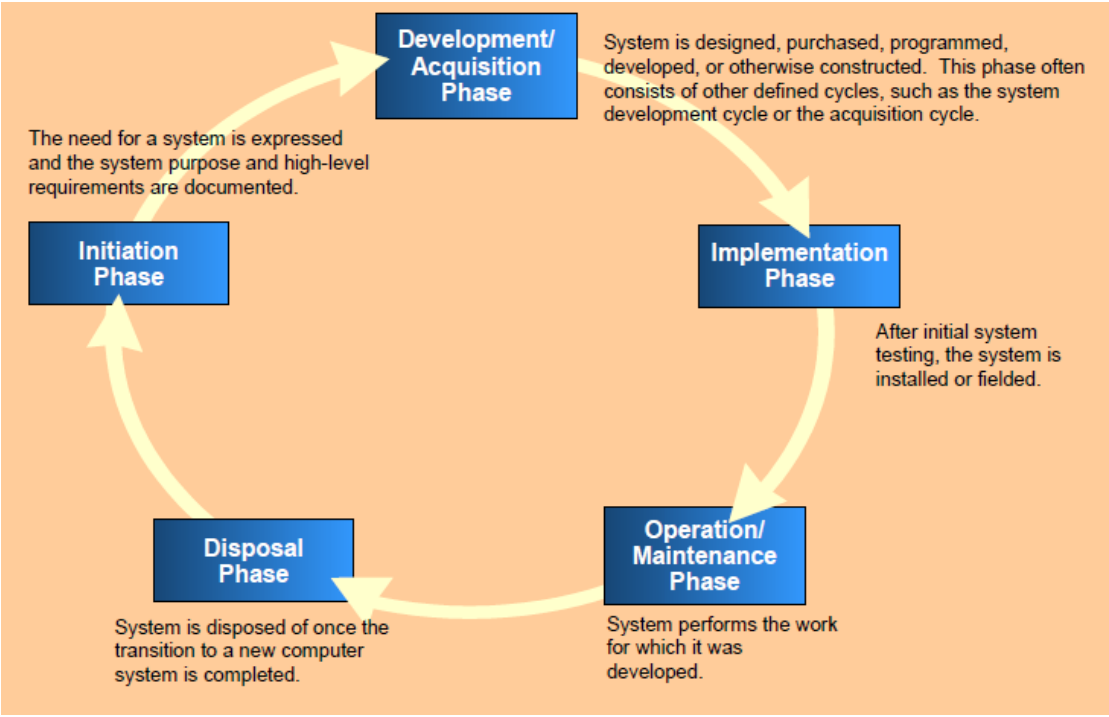

Figure 4.1: System Development Life Cycle [1]

4.2 IT Contingency Planning Process

An effective IT contingency plan consists of processes, through which the plan is developed and maintained. The proposal process can be adopted from all IT systems and includes the following seven steps:

1) Develop the contingency planning policy statement

The contingency planning policy statement should set the organization's global contingency objectives and determine the organizational framework and responsibilities for IT contingency planning.

2) Conduct the Business Impact Analysis

The Business Impact Analysis (BIA) helps the organization to understand and determine the system requirements and processes, and use this information to define contingency requirements and priorities. The scope of this analysis is to associate system components with critical services and based on this correlation, to realize the impact of a disruption to the system components. The BIA is completed via three phases:

- Identify Critical IT Resources;
- Identify Disruption Impacts and Allowable Outage Times; and
- Develop Recovery Priorities.

3) Identify preventive controls

In some cases, the outage impacts may be moderated or disappeared via preventive measures. A broad range of preventive methods are available, depending on system architecture and configuration, for example UPS, fire suppression systems, emergency master system shut down switch, off site storage of backup media, non-electronic records, and system documentation. Additionally, preventive controls should be recorded in the contingency plan, and the employees who are being involved with the system should be trained on how and when to use the controls.

4) Develop recovery strategies

Recovery strategies provide a methodology to restore IT operations quickly and effectively after a service interruption. The strategies should consider the impacts of an interruption and the admissible time which is identified by the BIA. During the course of developing the strategy the organization must take into consideration the various factors such as cost, allowable outage time, security, and integration with larger, organization-level contingency plans. The selected recovery strategy should address the following subjects:

- Backup Methods.

  The critical data should be backed up regularly. Backup policies should specify on the one hand, the data that will be stored and on the other hand, the frequency of backups (e.g., daily, weekly or monthly, incremental or full). Also, these should define the nomenclature, media rotation frequency and the location of stored data.

The ideal business practice would be the creation of a backup copy which will maintain all the vital data and which will be stored in an off-site location.

- Alternate Sites.

  The recovery plan must define a strategy to recover system operations at an alternate site for an extended period. In general, three types of alternate sites are available:

  - Dedicated site owned or operated by the organization;
  - Reciprocal agreement or memorandum of agreement with an internal or external entity; and
  - Commercially leased facility.

  These alternative sites may be categorized based on the type of operational status:

  - Cold Site, a location that is able to support the IT infrastructure after interruption of the primary site.
  - Warm Site, is a standby location which contains only necessary equipments.
  - Hot Site, usually is 7X24 (7 days of week and 24 hours of day) available location that includes the IT infrastructure.
  - Mobile Site, specific transportable IT equipment necessary to meet system requirements.
  - Mirrored Site is a redundant alternate site and provides high availability because the data is mirroring to real time.

  There are differences about cost and ready-time implementation among these sites (Table 4.1).

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

Table 4.1: Alternate Site Criteria Selection [1]

- Equipment Replacement.

  When primary location goes out of order, all the necessary equipment (hardware and software) needs to be activated quickly and directly to the alternative location. The organization for the equipment replacement can be adopted one of the three following basic strategies:

- Vendor Agreements;
- Equipment Inventory; and
- Existing Compatible Equipment.

Regardless of the strategy selected, detailed lists of equipment are necessary to be included in the contingency plan.

- Roles and Responsibilities.

  The organization must designate appropriate teams to implement the recovery strategy based on their skills and knowledge. Ideally, teams would be staffed with the personnel responsible for the same or similar operation under normal conditions.

- Cost Considerations.

  The organization should ensure that the chosen recovery strategy can be implemented effectively with existent employees and financial resources. Also, the management must perform a cost-benefit analysis to identify the optimum recovery strategy.

5) Develop an IT contingency plan

During the IT contingency plan development the organization should create a plan for restoring IT system, in which a disruption has occurred, and define the roles, responsibilities, teams, and procedures associated with this IT system. Also, plans should provide clear directions and step-by-step procedures so that it will be easy to be implemented in case of an emergency situation. A fully-developed plan reduces the possibility of confusion during the recovery phase. Additionally, the plan should be adapted, according to the organization's requirements.

The contingency plan contains at least five main components (figure 4.2):

- Supporting Information.

  The Supporting Information component consists of two sections:

  - The Introduction section contains briefly the desirability of the plan. Generally, the section includes the Purpose, Applicability, Scope, References/Requirements, and Record of Changes.
  - The Concept of Operations section provides additional information about the IT system, the contingency planning framework; response, recovery, and resumption activities.

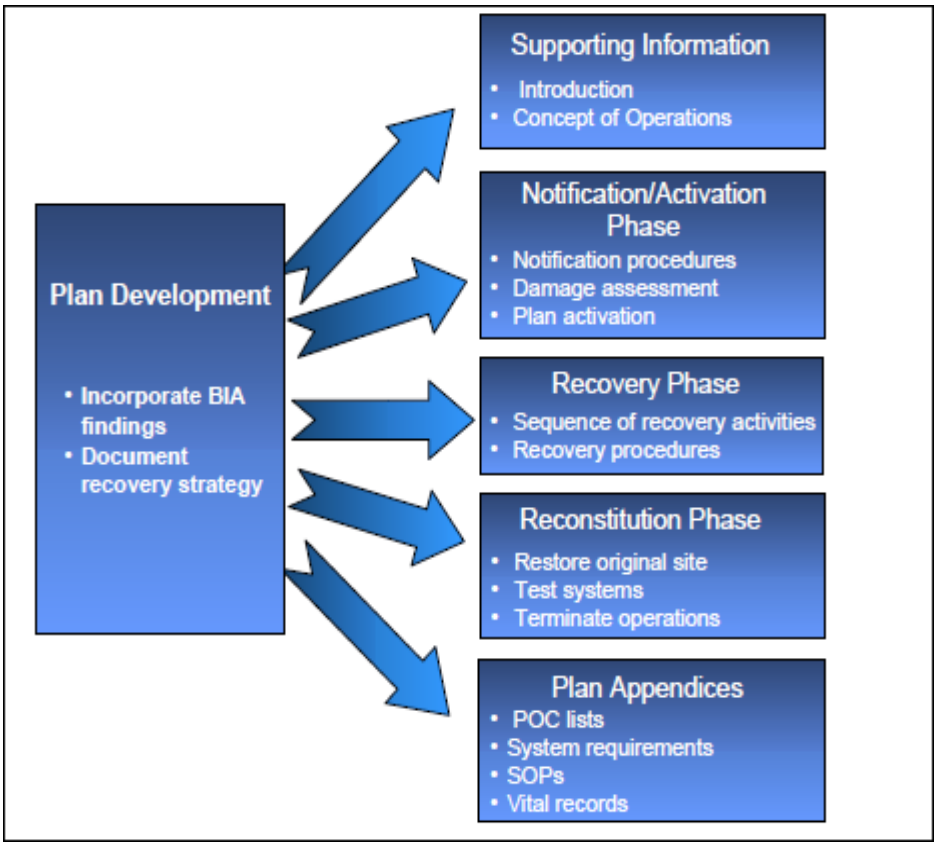

Figure 4.2: Contingency Plan Structure [1]

- Notification/Activation Phase.

  The Notification/Activation Phase determines the actions when an interruption is carried out to critical IT infrastructure. This phase must include:

  - Notification Procedures.

    The procedures should describe the methods used to notify the responsible teams for recovery during the incident.

  - Damage Assessment.

    It is necessary to assess the extent of the damage to the system after an emergency incident, so that the organization will be able to define how the contingency plan will be applied after a similar event.

  - Plan Activation.

    The IT contingency plan should be activated only when incident occurs.

- Recovery Phase.

  Recovery phase will be initiated after a serious emergency incident that affects normal business operations. Activities during this phase focus on restoration of normal business operations after an unexpected event, which may disrupt all, or

part of the IT process. After the completion of the Recovery Phase, the IT system will have to be set in order as it has defined in the plan.

- Reconstitution Phase.

  In this phase, the organization turning back to the normal IT infrastructure and operations after the recovery activities is terminated.

- Plan Appendices.

  The appendices include key details which are not contained in the main sessions of the IT continuity plan, such as Point Of Contact (POC) lists, system requirements and Standard Operating Procedures (SOPs).

6) Plan testing, training, and exercises

The IT contingency plan should be tested periodically in order for the organization to ensure the accuracy and effectiveness of the recovery plan. Tests help the organization to identify deficiencies into the IT contingency plan. In order to be efficient, the testing plan should include specific elements and case of incidents which are based on test objectives. Furthermore, the testing plan should include time frames for each test. Finally, all the employees who are involved in the recovery process must be trained so as to be more efficient.

7) Plan maintenance

The IT contingency plan is indispensable to be reviewed and updated frequently (at least once a year or whenever significant changes occur). It would be necessary to store a copy of the plan, in the alternative site, with all the necessary documents (such as contracts, software licenses, system user’s manuals, security manuals, and operating procedures).

4.3 Conclusion

The NIST published a guide that focuses on Business Continuity of IT systems because these facilities are important for the organizations' normal operation and are vulnerable to a variety of disruptions. While the major percentages of vulnerability may be minimized by using technical or operational solutions, it is practically impossible to eliminate totally all the risks. Thus, effective contingency planning, execution, and testing are essential in order to mitigate on the one hand, the risk of the system and, on the other hand, the unavailability of the service. The guide examines the elements and processes of the essential contingency plan, and also focuses to temporary measures so as to recover IT services after an incident of destruction.

5. ENISA - Business Continuity for SMEs

5.1 Overview

The European Network and Information Security Agency (ENISA) delivered "IT Business Continuity Management - An approach for Small Medium Sized Organizations" that provides an IT BCM framework for Small-Medium Sized Enterprises (SMEs). Following this simplified approach, a SME can develop and maintain a Business Continuity Plan. Consistent with ENISA [10] the BCP should be generated according the issues that follow below:

- *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 employee/team/ 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.*

5.2 IT Contingency Planning Process

This simplified BCM proposal uses four phases for creation of a BCP (figure 5.1).

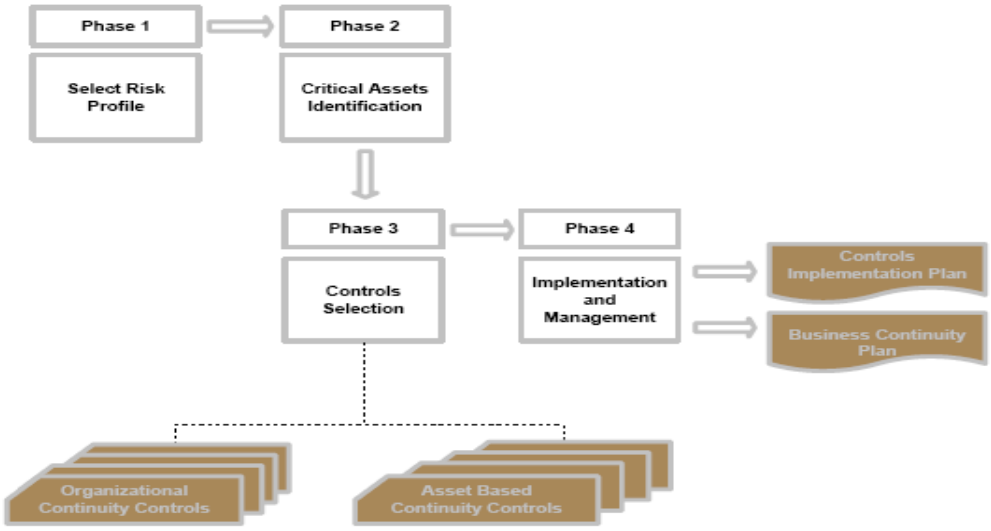

Figure 5.1: The four phase guideline the proposed BCM approach [10]

1) Select Risk Profile

In the first phase of the BCP process, the responsible employees assess the risks of the business operation, which can be divided into Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability area. During the risk assessment, the responsible team ranks each area into a risk level and defines the organization's overall risk profile, through two steps (figure 5.2).

- Identify Risk Areas.

  The responsible team defines the organization's risk profile using Risk Profile Evaluation Table (Table 5.1). From this table the team can select risk areas that are closer to their business profile and create a new table with the risk level (high, medium, low) for each area (example Table 5.2).

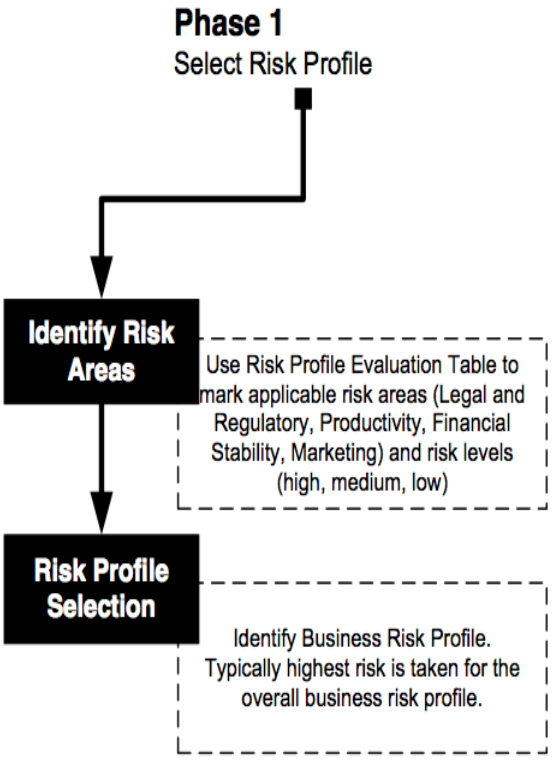

Figure 5.2: Phase 1 [10]

Risk Areas	High	Medium	Low
Legal & 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 no 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 no 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 & 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 5.1: Risk Profile Evaluation Table [10]

- Risk Profile Selection.

  Based on the results of the previous step, the team has the ability to select the organization's overall risk profile (column Risk Profile in Table 5.2). This risk matrix defines the risk area(s) that the organization should include into continuity controls and the risk areas that should prioritize depending on the risks.

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

Table 5.2: Risk Profile Evaluation Table - Example

2) Critical Asset Identification

In this phase of the BCP process the organization identifies the critical business functions that will cause problem to the normal business operation after an incident. According to these critical business functions, the organization will analyse the continuity requirements of the identified critical assets. In particular, the critical asset identification phase consists of the following three steps:

- Business Function Selection.

  The critical business functions are selected according to the impact on business after an interruption of these functions or after a destruction of the relevant assets. Once the list of the critical business function is defined, this should be recorded with the corresponding required recovery priorities (High: less than 1 day, Medium: 1 to 3 days, Low: up to 5 days). *It should be noted that the earliest possible recovery of such functions after a disruption is the main objective of a Business Continuity Plan [10].*

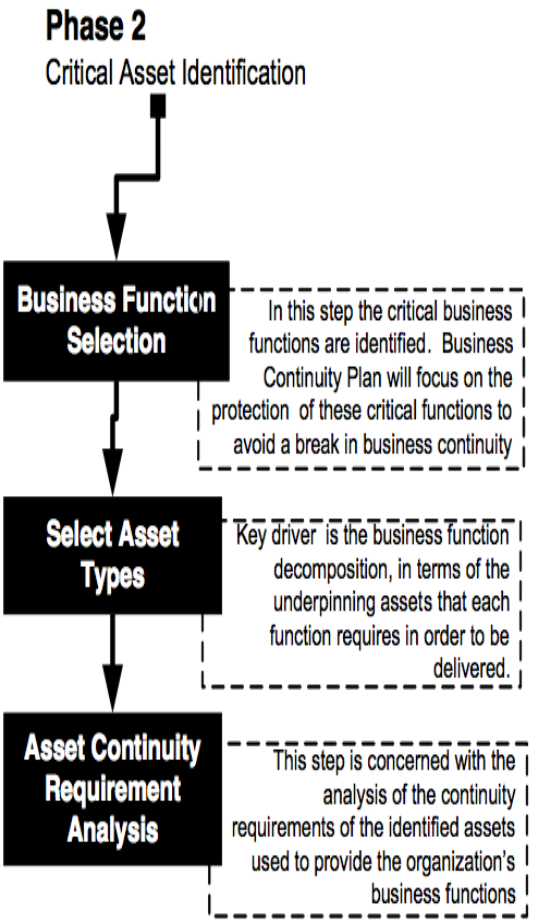

Figure 5.3: Phase 2 [10]

- Select Asset Types.

  The responsible team selects the critical assets based on the list of the critical business functions and then it will identify the alternative methods for the service delivery. *This will help the SME to focus its business continuity plan on the availability of the assets supporting critical business functions [10].*

- Asset Continuity Requirements Analysis.

  The final step of the "Critical Asset Identification" phase is associated with the analysis of the asset continuity requirements. Once this step is completed, an "asset identification card" is created for each critical asset (example Table 5.3) that will be used during the rest of the process.

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 Fulfillment
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 5.3: Email Service asset identification card- example [10]

3) Controls Selection

For each risk category, the organization defines and selects the respective controls that can be separated and grouped into (i) organization and (ii) asset-based continuity control cards. Furthermore, the "organization continuity control cards" that have been created for each risk profile is defined in phase 1 – table 5.2. Additionally, the "asset-based continuity control cards" are used for identification of appropriate asset controls (that are grouped in two categories, according to asset recovery priority and risk profile). After that, documentation will be created with the controls that have been selected (figure 5.4).

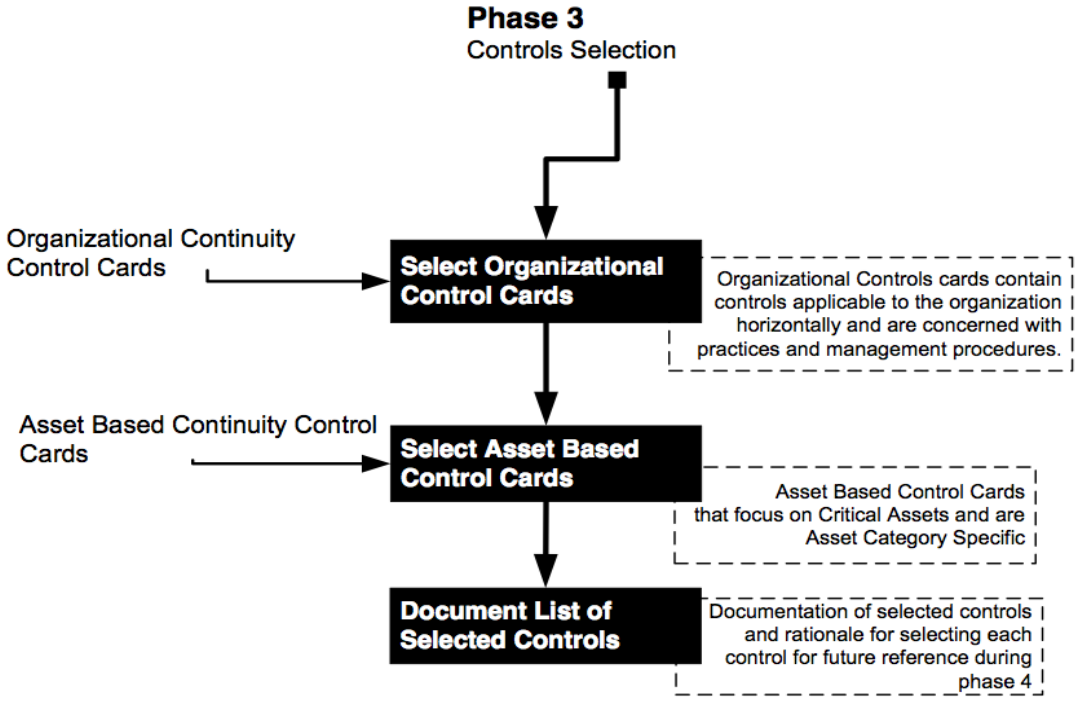

Figure 5.4: Phase 3 – Controls Selection Workflow [10]

4) Implementation and Management

The organization uses a gap analysis to evaluate the selected continuity controls based on the current business situation. Following the gap analysis the team will create the controls of Implementation Plan and form the documented BCP. In details:

- Perform Gap Analysis.

  The first action is the comparison between the actual Business Continuity practices and the Business Continuity controls that were selected from the previous phase of the process. Those results can help the team to define the procedures that will be used for the organization's continuity controls and to redesign the protection measures for the identified critical assets.

- Controls Implementation Plan.

  Once the gap analysis is carried out, the responsible team will re-determine the continuity controls of the organization. Through this process, the organization will implement a series of actions (continuity controls Action List) for the improvement of Business Continuity, by prioritizing the actions as far as the risk level is concerned (for the organizational continuity controls) and recovery priority (for the asset-based continuity controls) of the critical assets. The time frame for the control implementation depends on this classification.

  In many cases, the realisation of the priority of the controls may be influenced by a number of additional criteria, such as:

  - Personnel life health and safety;
  - Strategic alignment with organization goals;
  - Legal and Regulatory requirements;
  - System-wide benefits;
  - Cost/Time Savings;
  - Continuity Risk Reduction.

- Deliver Business Continuity Plan.

  The result of all of the above procedure is the documented BCP that includes the following:

  - BCP governance;
  - Results of Business Impact Analysis (BIA) and Risk Assessment (RA);
  - List of critical business functions and assets;
  - Plans, measures, and arrangements for business continuity ;
  - Quality assurance techniques (change management, exercises, maintenance and auditing);
  - List of continuity controls ;
  - Resource requirements;
  - Definition of roles and responsibilities about the business continuity process and corresponding contact list.

5.3 Conclusion

The ENISA provides a simplified approach for IT BCP. The base of this framework is the empirical approach for the determination of the continuity risk profile and the selection of continuity controls. The continuity strategy is defined from the employees who have the knowledge of the organization's functions and needs. Additionally, ENISA stresses in this document [10] that *"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"*. Finally, through this schema, a control's implementation plan and a business continuity plan will be created.

6. FFIEC - Business Continuity Planning

6.1 Overview

The Federal Financial Institutions Examination Council (FFIEC) published a booklet in March 2008 that provides guidance to financial institutions about processes to ensure the availability of critical financial services, through business continuity planning processes. This booklet focuses on the importance of BCP and analyses the way that the financial institution can follow in order to recover and resume processes after a business operation interruption. The BCP should be implemented for the overall business operations and facilities so as to mitigate the risk and the negative effects from a disruption.

6.2 Business Continuity Planning Process

Based on this standard a financial institution's business continuity planning process should reflect the following objectives:

- The BCP process should include the recovery and maintenance of all operations and components of the business.
- BCP involves the design of a continuity plan for the overall organization and the hierarchy of business objectives and critical operations that are necessary for the recovery process. This framework should define on the one hand, which critical operations, business units and systems should be included in a plan, while on the other hand, should determine the recovery phase.
- BCP should be regularly updated in terms of the changes in business policy, audit recommendations, and findings from testing.
- Finally, BCP should include a business impact analysis (BIA), a risk assessment, a risk management, and a risk monitoring-testing.

It would be a good idea the financial institutions to adopt a life cycle approach for the BCP. The FFEIC suggests the following four steps:

1) Business Impact Analysis (BIA)

The first step of the BCP process is a business impact analysis (BIA) which includes the following objectives:

- Recording and evaluation of all business functions and processes.
- Determination of the possible impact of unpredictable business process disruptions.

- Determination of the legal and regulatory requirements for the business functions and processes.
- Estimation of maximum permitted interruption of business functions and the acceptable level of losses.
- Estimation of Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and recovery of the critical path.

The responsible employees for the BIA should collect the necessary information for the analysis from the employees by using questionnaires and interviews. When all critical needs (functions and processes) are established, they should analyse them.

When the BIA is completed, it should be evaluated during the risk assessment process. Finally, the BIA should be reviewed and updated frequently according to the business operations changes, audit recommendations and the results of the testing process.

2) Risk Assessment

The risk assessment should include:

- Evaluation of the business processes and BIA assumptions using several threat scenarios (this process may require changes to the BCP).
- Analysing threats based upon the impact to the institution. Financial institutions should develop threat scenarios (e.g. malicious activity, natural and technical disasters) that may interrupt business function.
- Prioritizing possible interruptions based on the significance of business impact and the probability of occurrence. The most difficult threats to address are those that have a high impact on the financial institutions but a low probability of occurrence. On the other hand, a threat that has a high probability to take place, regardless of the size of the damage caused to financial institutions, will be addressed more easily because it is expected to occur.
- Develop a "gap analysis" that compares the existing BCP with the policies and procedures that should be implemented during a security incident.

3) Risk Management

During this step the institution can identify, assess and mitigate the risk level for the development and implementation of BCP. These are as follow:

- BCP based on a comprehensive BIA and risk assessment.
- Development of BCP based on valid assumptions and an analysis of inter-dependencies.
- Documented in a universal structure.

- BCP reviewed and approved by the top management.
- BCP notification to employees.
- Defines the several types of events that could cause interruption to normal operation of the financial institute and trigger the start of the BCP.
- Specifies the steps that should be taken during a disruption in order to maintain the safety of employees and minimize the damage of the interruption.
- Describes the responsibilities and procedures to be followed by each continuity team and also includes contact lists of critical personnel.
- Flexible to respond to unexpected threats.
- Targets to the impact of several threats that could have the ability to interrupt the normal operations instead of specific incidents.
- Defines relocation strategies to alternate site.
- Effective in minimizing service disruptions and financial loss through the implementation of mitigation strategies, that depends on the results of the BIA and risk assessment.

The BCP must be assessed as a part of the risk monitoring and testing phase (the final step of the cyclical BCP process), that involves the development, execution, evaluation, and assessment of a testing program. The BCP will be updated through the testing program.

4) Risk Monitoring and testing

Through this step the organization ensures the validity of BCP process. This can be achieved through principles of the business continuity monitoring and testing program:

- Assignment of roles and responsibilities for implementation of the testing program.
- Define testing policy strategies.

  The testing policy should include enterprise-wide testing strategies that establish expectations for individual business lines across the testing life cycle of planning, execution, measurement, reporting, and test process improvement. Testing strategies should include the testing scope and objectives, which clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test. The objective of a testing program is to ensure that the business continuity planning process is accurate, relevant, and viable under adverse conditions. Therefore, the business continuity planning process should be tested at least annually, with more frequent testing required when significant

changes have occurred in business operations. Testing should include applications and business functions that were identified during the BIA [11].

- Develop a test planning.

  The institute should define a test scope and the objectives of the test plan and should provide relevant employees with necessary information (e.g. test schedule, test methods, test locations).

- Review test plan from all involved departments.

- Determine the testing methods.

  The testing method that will be adopted by the financial institute should include business recovery and disaster recovery exercises. Business recovery exercises focus on testing business line operations, while disaster recovery exercises focus on testing the continuity of technology functions. Also, the testing method should be designed in order to cover all the functions that are performed during a whole working day.

When the tests are completed the following procedures should be implemented:

- Test results should be documented by including all the information such as test dates and locations, test objectivities-results and problems identified during testing.

- Test results should be evaluated, by the top management, to ensure that test objectives are achieved. Additionally, it should be used to determine the effectiveness of the BCP.

- The test results and the resolution of any problems identified during testing should be reported to all stakeholders, such as top management, auditors, risk and IT management.

- The overall testing process and the test results should be evaluated by independent parties (e.g. internal auditor).

- Update BCP and test program based upon changes in business operations, audit-examination recommendations, and test results.

Finally, based on this approach additional policy, standards, and processes should be integrated into the BCP process:

- *Security Standards;*

- *Project Management;*

- *Change Control Policies;*

- *Data Synchronization Procedures;*

- *Crises Management;*
- *Incident Response;*
- *Remote Access;*
- *Employee Training;*
- *Notification Standards;*
- *Insurance; and*
- *Government and Community [11].*

6.3 Conclusion

The FFIEC provides guidance for Business Continuity process and focuses on the needs of the financial institutions, based on the availability of financial services. An effective BCP can be achieved through a BIA, a risk assessment, risk management, and risk monitoring-testing. Additionally, effectiveness of the BCP can be confirmed by annual scheduled test and review of business continuity requirements.

7. Bank of Greece G.A. 2577 9.3.2006 - Annex 2

7.1 Overview

The Bank of Greece published a Governor's Acts, in March of 2006 with the number 2577, which provides the main guidelines (Annex 2) about the Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) for the Information Systems of financial institutions (banks). According to the GA-BG 2577, the financial institutions should have IT BCP as part of the global BCP and this should be approved by the up level management. This plan must be activated during a disaster and it will ensure the continuity of the business functions. Moreover, in cases of a disaster an effective DRP should be applied.

7.2 IT Contingency Planning Process

1) Business Impact Analysis (BIA) and Risk Analysis

Before the creation of the BCP and DRP a Business Impact and Risk Analysis must take place so as the institution can formulate the Business Continuity objectives. Through the analysis, the institute will achieve the following:

- Definition of a Business Continuity strategy.
- Identification of critical functions and relevant infrastructures and prioritization of the processes for the critical functions according to their significance.
- Definition and categorization of risk threat for the critical functions.
- Estimation of business cost, when an interruption of the critical IT system takes place and implementation cost of BCP and DRP. Through this process, the financial institute can segmentate the BCP and the DRP, so only the necessary parts of the plan will be activated after an incident occurs.
- Determination of Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for the Systemically Important Payment Systems (SIPS).

2) Backup Plan for Critical Infrastructures

It is important to have a backup plan for the critical IT equipments (hardware and software), configuration of systems and data. In this plan all the procedures about the backup/restore data must be documented in detail. Specifically, this procedure should define which data should be backed up and how often. This depends on their criticality and their frequency of change. Also, it should be determined how to store the data of backup safely, so only authorized employees can have access and to ensure the availability and integrity of backup data from natural disasters (floods and fires). Often, additional copies of backup are being transferred and stored safely to alternative off-site location, beside the safekeeping in the computer room. These

backups should be tested frequently to ensure data integrity and during this process the backup/restore time must be recorded. Additionally, in order to ensure a quick data recovery is necessary to label and document each media of the data. Finally, the approach of the backup media recycling will assist to store and manage the data media.

3) Developing BCP and DRP

During this phase the financial institute must have a complete and effective BCP and DRP for the IT. Those plans must be documented and published in a simple way so all the employees can get informed. It is important the sensitive information to be communicated only to authorized employees. Furthermore, it would be necessary, a backup of those plans to be stored with safety in an alternative location.

Such plans must include:

- Systems categorization according to business impact and risk analysis. Once categorization is completed, a list will be created including all these IT systems with detailed information (required recovery time and the expected level of functionality after the recovery).
- Definition of responsible employees and teams for continuity and recovery plans.
- Definition of disaster scale. According this scale, specific parts of the plan will be activated during a disaster event.
- Specific actions to be performed during an emergency situation which among others should ensure the safety of employees in cases of destruction (e.g. fire).
- Procedures for staff training in accordance with the responsibilities they have during the activation of the plan.
- A list of suppliers with relevant service level agreements (SLAs), the services they offer and the expected response times in emergency situations.
- Procedures to ensure that plans are maintained and updated on any relevant change.

Additionally, the Disaster Recovery Plan should include an alternative (secondary) site that can support all the critical infrastructure components that lie in the primary site. Through the DRP the financial institute can ensure the efficient operation of alternative data center, which will be located in an appropriate distance so that it will not be subjected to the same risks as the main computer center. The alternative center should have adequate equipment to provide all critical services for the predefined time frames including manuals of procedures and use of systems. Furthermore, it must operate effectively until the recovery procedure completes in the primary site. In addition, the bank can ensure the physical safety of the secondary site by using a well-designed plan and a basic level of logical security during the implementation phase of the recovery operation. In particular, in this plan the following subjects must be

defined in order to ensure the institute for the effectiveness of the continuity of the critical services:

- Alternative workplace for the employees and the relevant equipments.
- Preparation and activation procedures for the alternate data center.
- The systems and network infrastructures and topology for the data center.
- In case that the financial institute cooperates with vendors who provide equipment or service for the alternative site, it should include a process that will inform them for any changes in the systems that might require extra updates for the Disaster Recovery Plans.

Finally, the testing procedures should be included in the plan, according to which:

- The frequency of DRS site (minimum one a year) is specified.
- The goals of the testing procedure are specified.
- Ensure the participation of the internal audit team.
- Ensure the creation of a report with the results of the testing procedures. This documented report must be published to management and audit team.
- Ensure the corrections and adjustments of any problems that appear during the testing procedure.

7.3 Conclusion

This Governor’s Acts is baseline guidance from the Bank of Greece for the financial institute's SIPS (systemically important payment systems). It provides general instructions about the continuity and recovery plans that an institute is necessary to adapt. The institute through BIA and RA procedures should create and implement BCP and DRP plans.

8. Comparison of BC standards/guidelines

Reading the previous standards and guidelines, it can be concluded that these have many similarities. For the comparison of these, a table which aligns the different standards and guidelines side-by-side has been created (table 8.1). In this table the elements that were included in the five standards/guidelines are being recorded.

All these address the issues for Business Continuity Management and have common processes such as:

- Definition of BC strategy and policies based on the business needs;
- Business Impact Analysis that defines the critical services/resources/activities/ functions and prioritizes them according to the level of impact and acceptable outage times.
- Development of BCP and/or DRP includes all the necessary information for continuity/recovery process (Controls, Backup Plan, Alternate Site, Recovery Procedures/Activities, Roles and Responsibilities, etc.)
- Testing, maintaining and reviewing of plans.
- Training all the responsible employees.

Most of these are describing what should be done by providing a baseline instruction. They do not specify how each activity/process is going to be implemented (as this is usually decision of the organization).

As it has already been mentioned, the differences among these are the perspectives and approaches of the Business Continuity area. Also, there were selected because they cover various areas of business operations (independent of application area, federal departments, small and medium enterprise, financial institutions and banks).

Based on this examination, one could point out that it is impossible to define the best standard; and essentially any Business Continuity standard/guidelines can be used in an organization. The organization/company can choose the standards based on the following:

- needs and goals;
- application area (industry, government, hospital, financial, commercial, etc.);
- services and asset that provide/produce;
- company revenues;
- number of employees and locations;
- geography location;
- country regulations; etc.

From the above it is obvious that the biggest interest for further examination has the GA.BG 2577 guideline. It is the only and unique Greek guideline that corresponds to bank institutes and it is a challenge because of the complexity of their IT architecture.

Components		Standards & Guidelines				
		BS2599	NIST 800-34	ENISA	FFIEC	GA.BG 2577
Areas of Business Operation		Independent	Federal Systems	SMES	Financial Institutions	Banks
Target Area		Overall Business Functions	Government IT	IT	Overall Business Functions	IT for SIPSs
Approach		General guidelines, recommendations and processes	Instructions, recommendations and considerations with details instruction for technology functions	Simplify & empirical approach	Guidance	Mandatory guidelines
Scope		step 2	step 1			step 1
BC Lifecycle		cyclical	cyclical		cyclical	cyclical
Business Impact Analysis (BIA)	Services/Resources/ Activities/Functions	step 2	step 2	step 2	step 1	step 1
	Impact	step 2	step 2	step 2	step 1	step 1
	Allowable Outage Times		step 2		step 1	step 1
	Recovery Priorities	step 2	step 2	step 2		step 1
Risk Assessment		step 2		step 1	step 2	step 1
Gap analysis				step 4	step 2	
Business Continuity & Recovery Strategy/Plan	Critical Services/Resources/ Activities/Functions	step 3	step 2	step 2&4	step 1	step 3
	Recovery Time Objectives (RTOs)	step 4			step 1	step 1
	Recovery Point Objectives (RPOs)	step 4	step 5		step 1	step 1
	Controls	step 2&3	step 3	step 3	step 2	
	Backup Plan		step 4			step 2
	Alternate Site	step 4 (briefly)	step 4		step 3 (briefly)	step 3
	Equipment Replacement	step 4 (briefly)	step 4			step 3
	Recovery Procedures/Activities	step 4	step 5&6	step 3	step 3	step 3
	Roles and Responsibilities	step 1&4	step 4&5	step 4	step 3	step 3
Testing, maintaining and reviewing		step 5	step 6&7		step 4	step 3
Training and Awareness		step 6	step 6		step 3&4	step 3
Complexity		Normal	Normal	Medium	Normal	Normal
Level of guidance		Base	Detailing	Base	Base	Detailing

Table 8.1: Comparison of Business Continuity standards/guidelines.

9. Case Study

9.1 Overview

Following the above examination, in this chapter the creation of BCP based on Bank of Greece guidelines (chapter 7) will be presented. The goal of this case study is to acknowledge the necessary process that the financial institutions (banks) must adopt about the availability of systemically important payment systems, according to the regulations in Greece. So, this case study refers to the BCP development process for a hypothetical medium financial institute, that only provides services via a telecommunications network (internet and telephone, not branches), services through Automated Teller Machine (ATM) and Point Of Sale (POS). It includes all the necessary infrastructures that a bank must have to provide similar services to the public.

9.2 Business Impact Analysis (BIA)

1) Definition of a business continuity strategy.

The financial institute implements the business continuity strategy that aims to:

- Ensure Business Continuity and minimize business losses;
- Identify the critical functions and relevant infrastructures;
- Provide services through e-banking, phone banking, ATM and POS by ensuring integrity and availability of these services to the public;
- Ensure the integrity, availability and confidentiality of information and data from any expected or unexpected threats or hazards;
- Establish mechanisms that will provide availability of critical infrastructures and data;
- Create and verify alternative mechanisms for Business Continuity;
- Strengthen the confidence of the business partners who trust information, data and work to a supervised environment;
- Enhance the competitive advantage of business by building confidence to the customers and employees; and
- Demonstrate compliance with international and local safety standards.

2) Identification of critical functions and relevant infrastructures.

The core of a successful BCP is to identify and record all the services that the bank provides to the public. This financial institution should make available only e-services

and telephone-services. More specifically, the customer can use e-banking, telephone/voice banking, ATM and POS to fulfil their needs. Through these services they can handle the bank accounts, loans, cards and check books that owe in this financial institution. Additionally, the ability to pay bills and transfer money to another financial institution is provided. Furthermore, the customer can deposit or get money by crediting or debiting their account/card which has either in this bank or in another. Finally, the application function is available through the e-banking and phone-banking so they can request a new bank account, card, check book or loan. All these functions can be completed through the services which are provided by the financial institution and that are presented in table 9.1 ("Services - Functions") separated by operation services.

Services - Functions	Description
e-Banking	Online banking services
Bank Accounts Management	• Extrait • Mini statement • Balance • Money transfer to any bank account or credit card in the same Financial institution
Cards Management	• Extrait • Mini statement • Balance available credit limit • Future instalments • Redemption payments/instalments • Payments
Loans Management	• Extrait • Balance available credit limit • Future instalments • Loan amortization • Redemption instalments • Payments
Cheques Management	• Information on checks pledged: * Expiry date and issuing bank branch * Amount and currency of the check * Name of publisher • Management customer checks: * Check status (available, annulled, sealed, etc.) * Check amount and currency * Historical movements of the check * Online bill
Payments	• Bills of Public Enterprises and Entities -DEKO- (electricity, water, etc.) • Bills of Telephony / Internet Providers • Bills/Subscriptions for other services (gas, cable TV, etc.) • Payment of contributions (IKA, OAEE/TEVE, VAT and Income Tax) • Insurance premiums to insurance companies
Transfers	• Money transfer to any account or credit card to another Bank • Fund Transfers
Charities	Ability for donations to charitable organizations by debiting bank account
e-Payroll	Ability to create and send payroll file
Transactions Information	• Transaction Results • Pending Transactions • Schedule Transactions
Application	• Request check-books • Request for new account • Request for new card • Request for new loan

e-banking Account Management	• Change Information (address, phone number, etc.) • Change e-banking password
Website	Financial institution web page which has information about the bank
Phone/Voice Banking	Phone trading
Bank Accounts Management	• Extrait • Mini statement • Balance • Money transfer to any account or credit card in the same Bank
Cards Management	• Extrait • Mini statement • Balance available credit limit • Future instalments • Redemption payments/instalments • Payments
Loans Management	• Extrait • Balance available credit limit • Future instalments • Loan amortization • Redemption instalments • Payments
Cheques Management	• Management customer checks: * Check status (available, annulled, sealed, etc.) * Check amount and currency * Historical movements of the check * Online bill
Payments	• Bills of Public Enterprises and Entities -DEKO- (electricity, water, etc) • Bills of Telephony / Internet Providers • Bills/Subscriptions for other services (gas, cable TV, etc.) • Payment of contributions (IKA, OAEE/TEVE, VAT and Income Tax) • Insurance premiums to insurance companies
Transfers	Money transfer to any account or credit card to another Bank
Application	• Request check-books • Request for new account • Request for new card • Request for new loan
Automated Teller Machine (ATM) Transactions	Self-service transaction systems
Deposit	Cash deposits to any account or credit card
Withdrawal	Cash withdrawals to any account or credit card
All Type of Payments	• Loans and credit cards • Bills of Public Enterprises and Entities -DEKO- (electricity, water, etc.) • Bills of Telephony / Internet Providers • Bills/Subscriptions for other services (gas, cable TV, etc.) • Payment of contributions (IKA, OAEE/TEVE, VAT and Income Tax) • Insurance premiums to insurance companies
Transfer	Money transfer to any account or credit card to another Bank
Balance	Updated balances for each customer accounts
Mini Statement	Statement of the last 10 transactions of an account
Other Services	Activate Card & Change PIN
Point Of Sale (POS) & Cards	Payment transaction with bank card to POS

Table 9.1 Services – Functions

The availability and integrity of all these services that are provided by the financial institute to the public are vulnerable to threats and dangers that probably are caused by a security incident (natural disaster, malicious actions, hardware failure etc.) and create damage in the daily workflow and services. To schedule and implement the alternative procedures, so as to have those services available, which were interrupted, the institute should prioritize them according to their criticality. The level of impact can be characterized from very low (zero impact to the customer service) to very high, that is the interruption of overall business operation and customer services (table 9.2 Level of Impact). The determination of the criticality of each service will define the sequence priority in the continuity and recovery procedure.

Level of Impact	Shortcut	Evaluation of Acceptability	Impact	Info
Very Low	VL	Acceptable	No impact to the customer service.	No further action is necessary other than to ensure that the controls are maintained.
Low	L		Interruption of specific business function(s) and delays on customer services.	No additional controls are required unless they can be implemented at very low cost (in terms of time, money, and effort).
Medium	M		• Impact on the company's normal operation • Influence on many business parts. • Creation moderate load and overtime of employees during the interruption and after recovery. • Prevention customer services.	Consideration should be as to whether the risks can be lowered, where applicable, to a tolerable level and preferably to an acceptable level, but the costs of additional risk reduction measures should be taken into account. The risk reduction measures should be implemented within a defined time period.
High	H	Unacceptable	• Impact on the overall company's normal operation • Influence on many business parts. • Creation high load and overtime of employees during the interruption and after recovery. • Unable customer services.	Substantial efforts should be made to reduce the risk. Risk reduction measures should be implemented urgently within a defined time period and it might be necessary to consider suspending or restricting the activity, or to apply interim risk control measures, until this has been completed. Considerable resources might have to be allocated to additional control measures.
Very High	VH		Interruption of overall business operation and customer services.	Substantial improvements in risk control measures are necessary so that the risk is reduced to a tolerable or acceptable level. The work activity should be halted until risk controls are implemented that reduces the risk so that it is no longer very high. If it isn't possible to reduce the risk, the work should remain prohibited.

Table 9.2 Level of Impact

The criticality of any service depends on three elements: the impact of failure to deliver a service, the loss of reputation or public confidence and the financial loss. According to these elements and the relevant level of impact, for each function is determined the acceptable Maximum Tolerance Days (MTD - the maximum days that the services can be unavailable to the public) (Table 9.3).

Services - Functions	Failure to Deliver a Service	Loss of Reputation or Public Confidence	Financial Loss	MTD
e-Banking				
Bank Accounts Management	H	H	M	1
Cards Management	H	H	H	1
Loans Management	H	H	H	1
Cheques Management	H	H	H	1
Payments	H	H	L	2
Transfers	H	H	L	2
Charities	L	L	L	3
e-Payroll	H	H	M	1
Transactions Information	L	M	L	3
Application	L	M	M	3
e-banking Account Management	L	M	L	3
Website	L	M	L	3
Phone/Voice Banking				
Bank Accounts Management	H	H	M	1
Cards Management	H	H	H	1
Loans Management	H	H	H	1
Cheques Management	H	H	H	1
Payments	H	H	L	2
Transfers	H	H	L	2
Automated Teller Machine (ATM) Transactions				
Deposit	M	M	M	2
Withdrawal	H	H	M	1
All Type of Payments	H	H	H	1
Transfer	H	H	L	1
Balance	L	M	L	3
Mini Statement	L	M	L	3
Other Services	L	M	L	3
Point Of Sale (POS) & Cards	H	H	H	1

Table 9.3 Proportional business impact

The financial institute in order to deliver all these services has a relevant IT infrastructure (hardware, software, application, licensee, telecommunication lines etc). The infrastructure covers the following sectors:

- E-Banking [25].

  Management system for online banking services.

- Website.

  System for financial institution web page.

- Phone/Voice Banking.

  Management system for phone trading.

- Automated Teller Machine (ATM) Transactions [26].

  Management system for monitoring and administration ATMs.

- Point Of Sale (POS) & Cards [26].

  Management system for monitoring and administration POS transactions.

- Core Banking.

  System for core banking application and data base. The core banking system is the heart of the banking system that manages all the financial transaction and data.

- Interbanking Systems, DIAS [27].

  Management system for communication between financial institute and DIAS payment systems, which are used mostly for low value payments namely card payments, credit payments (salaries, pensions, etc.), direct debits (telecommunications, electricity, water bills, taxis etc.) and cheque clearing.

- Society for Worldwide Interbank Financial Telecommunication (SWIFT) [28].

  Management system for communication between financial institute and SWIFT systems, which provides transfer financial transactions through "financial messages" between financial institutions (through the SWIFT).

- Dealing Room & Treasury.

  Treasury management system and international capital products (e.g. rates).

- Tiresias [29]

  - Default Financial Obligations System (DFOS) & Mortgages and Prenotations to Mortgages System (MPS).

  - Credit Consolidation System (CCS).

- Basel [30]

  System for Capital adequacy framework.

- Data Warehouse (DW), Business Intelligence (BI) and Performance Management (PM).

  The centralized system for historical report current and predictive views or business operations about business data, aims to affect the decision-making to senior management levels.

- Management Information System (MIS) Reporting [31].

  System that provides information needed to management organizations effectively.

- Finance & Accounting.

  Provides general ledger, payables, cash management, fixed assets, receivables, budgeting, and consolidation services.

- Human Resources (HR).

  System for payroll, training, benefits, recruiting and diversity management services.

- Customer Relationship Management (CRM) [32].

  System for sales and marketing, commissions, service, customer contact and call center support services.

- IT Services.

  - System for backup solution;
  - Network equipment (Routers/Switches);
  - Security equipment (Firewalls, IDS/IPS, Mail-Filtering, Web-Filtering, Proxy);
  - System for Mail services;
  - System for Dynamic Host Configuration Protocol (DHCP);
  - System for Domain Name System (DNS);
  - System for Domain Account Management;
  - System for Network Time Protocol (NTP);
  - File Sharing Servers; and
  - Telecommunication Equipment.

- Peripheral equipment (work places, workstation, telephones, etc.).

The relationship between all these components is depicted in the figure (9.1) below.

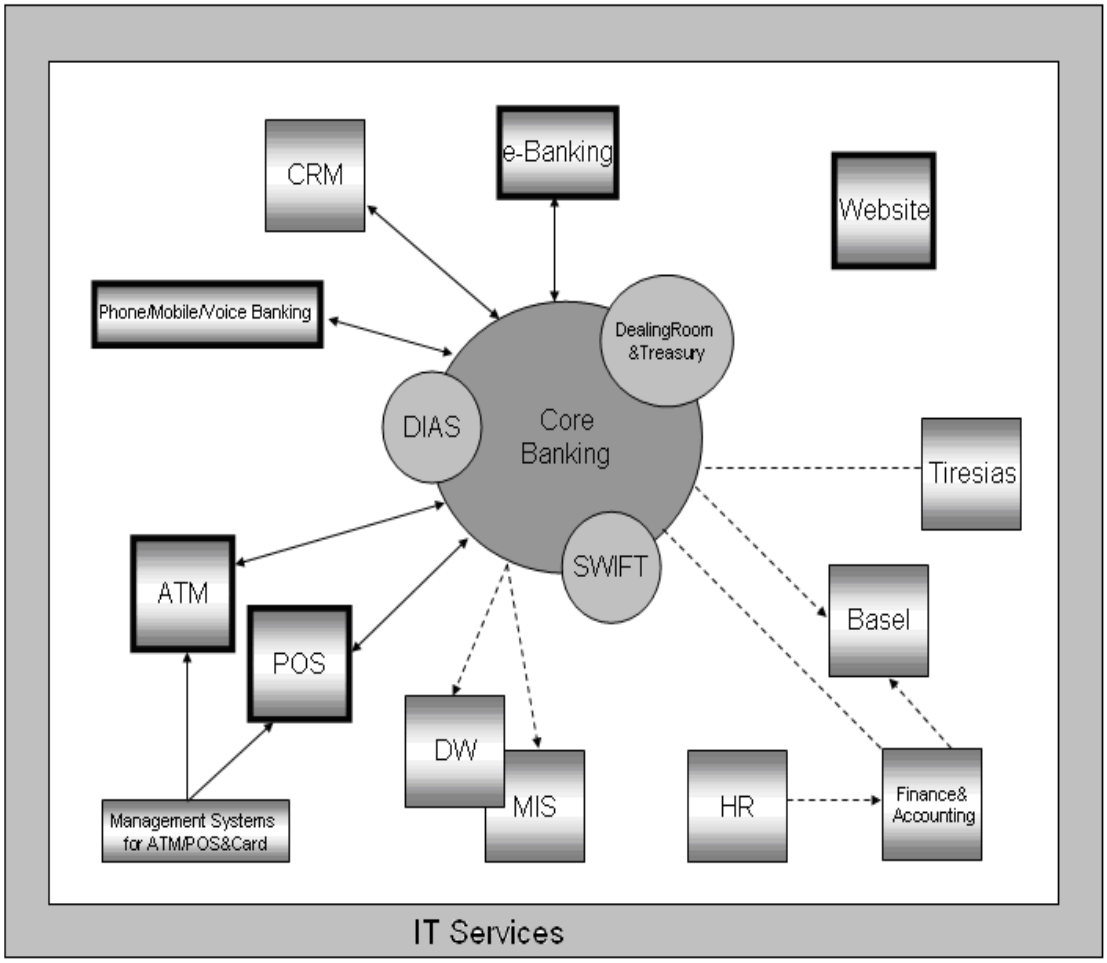

Figure 9.1 Components Relationship

Therefore, according to table 9.3 (that presents proportional business impact) and the relationship between the components, that are necessary so that the financial institute can provide critical services to its customers, the following table has been created that presents the criticality of infrastructure.

Services - Functions	Infrastructures	MTD
e-Banking		
Bank Accounts Management	e-Banking	1
	Core Banking	
	Dealing Room & Treasury	
Cards Management	e-Banking	1
	Core Banking	
Loans Management	e-Banking	1
	Core Banking	
	Dealing Room & Treasury	
Cheques Management	e-Banking	1
	Core Banking	

	Dealing Room & Treasury	
	DIAS	
Payments	e-Banking	2
	Core Banking	
	DIAS	
Transfers	e-Banking	2
	Core Banking	
	Dealing Room & Treasury	
	DIAS	
	SWIFT	
Charities	e-Banking	3
	Core Banking	
	Dealing Room & Treasury	
e-Payroll	e-Banking	1
	Core Banking	
Transactions Information	e-Banking	3
	Core Banking	
	Dealing Room & Treasury	
Application	e-Banking	3
	Core Banking	
	Dealing Room & Treasury	
	Tiresias	
e-banking Account Management	e-Banking	3
	Core Banking	
Website	Website	3
Phone/Voice Banking		
Bank Accounts Management	Phone/Voice Banking	1
	Core Banking	
	Dealing Room & Treasury	
Cards Management	Phone/Voice Banking	1
	Core Banking	
Loans Management	Phone/Voice Banking	1
	Core Banking	
	Dealing Room & Treasury	
Cheques Management	Phone/Voice Banking	1
	Core Banking	
	Dealing Room & Treasury	
	DIAS	
Payments	e-Banking	2
	Core Banking	
Transfers	Phone/Voice Banking	2
	Core Banking	
	Dealing Room & Treasury	
	DIAS	
	SWIFT	
Automated Teller Machine (ATM) Transactions		
Deposit	Management Systems for ATM & POS	2
	Core Banking	
	Dealing Room & Treasury	
Withdrawal	Management Systems for ATM & POS	1
	Core Banking	
	Dealing Room & Treasury	

	DIAS	
All Type of Payments	Management Systems for ATM & POS	1
	Core Banking	
	Dealing Room & Treasury	
	DIAS	
	SWIFT	
Transfer	Management Systems for ATM & POS	1
	Core Banking	
	Dealing Room & Treasury	
	DIAS	
	SWIFT	
Balance	Management Systems for ATM & POS	3
	Core Banking	
	Dealing Room & Treasury	
Mini Statement	Management Systems for ATM & POS	3
	Core Banking	
	Dealing Room & Treasury	
Other Services	Management Systems for ATM & POS	3
	Core Banking	
Point Of Sale (POS) & Cards	Management Systems for ATM & POS	1
Functions that serve the needs of the bank		
Finance & Accounting	Finance & Accounting System	7
HR	Human Resources System	7
CRM	Customer Relationship Management System	7
	Core Banking	
Basel	Basel System	7
	Finance & Accounting System	
	Core Banking	
MIS	Management Information System for Reporting	7
	Core Banking	
DW	Data Warehouse (DW), Business Intelligence (BI) and Performance Management (PM) Services Systems	7
	Core Banking	
IT Services		
Backup	System for backup solution	1
Network	Routers/Switches	1
Security	Firewall	1
	IDS/IPS	
	Mail Filtering	
	Web Filtering	
	Proxy	
Mail	System for email services	1
DHCP	System for Dynamic Host Configuration Protocol	2
DNS	Domain Name System	1
LDAP	System for employees accounts	1
NTP	Network Time Protocol System	3
NFS	File Sharing Server	3
Telecommunication Services	Telecommunication Equipment	2

Table 9.4 Criticality of infrastructures

9.3 Developing BCP and DRP

1) BCP

In the second phase the institute must design the Business Continuity Plan by using the information obtained from the BIA. Based on the Bank of Greece and the European Central Bank (ECB), such plans must be documented and include all necessary information, processes and policies that are needed to ensure the continuity of critical services, such as:

- The responsible teams for any phase of the continuity plan;
- The point(s) of plan activation;
- The workflow actions during an emergency situation; and
- Procedures for staff training in accordance with the responsibilities those have during the activation of the plan.

2) DRP and DRS

After, the financial institute has collected and analyzed all the necessary information, can decide the architecture of Disaster Recovery Site (DRS part of the BCP) that will be used in case of critical infrastructure destruction.

The institute can implement a redundant secondary site to a remote location, in which it will have similar infrastructures with the primary site. This architecture provides high availability (usually 7 days of week and 24 hours of day) because the data is mirroring in real time. Using the mirror site the down time of the services and the setup time of the alternative site are reduced to the minimum. On the other hand, the creation of this mirror site increases the cost of implementation and maintenance because it duplicates infrastructures and extra employees are required for daily administration and maintenance.

In contrast to the mirror site there is another that is called “cold site”. The implementation of this architecture can minimize the cost of the alternative site because the only overheads are the alternative location and the contract of the vendors that will provide all the necessary equipment. Although in this case the cost is lower, the setup time of the alternative site is time-consuming and difficult so this solution, business ways, is unacceptable.

Regardless the above, the bank can adopt an intermediate architecture, so that there is a balance between the cost of implementation-maintenance and DRS setup time. This can be achieved by using a standby location that contains only the necessary equipment for critical services. In this way, the cost of implementation and setup time can be acceptable. The institute can develop this architecture based on the BIA and RA that has been completed in the fist phase.

More specifically, in this case study the institute can use the results of the analyses (that are presented in table 9.4) and illustrate the criticality of infrastructures in order to create an effective and efficient DRS by using a remote standby location. According to these, the bank must ensure that has the appropriate equipment and

procedures for the recovery procedure of infrastructure. The recovery must be done with a priority based on the criticality of the infrastructure (starting from the smallest to the largest MTD number), so the recovery phases can be derived as follows:

First phase

(i) Core Banking , Dealing Room & Treasury, DIAS and SWIFT;

(ii) e-Banking;

(iii) Phone/Voice Banking;

(iv) Management Systems for ATM & POS;

(v) IT infrastructure for network, security, mail, DNS, LDAP and backup.

After completion of this phase the most of the services that are provided to the public will be available (all services through Phone/Voice Banking, ATM, POS and all e-banking services expect the application). Also all the necessary IT Services will be available.

Second Phase

(i) Tiresias and Web Site;

(ii) IT infrastructure for DHCP, NTP, NFS;

(iii) Telecommunication Services.

After the completion of the second phase, the institute will be able to provide all the services to the customers and all IT Services can be available for the employees.

Third Phase

(i) Finance & Accounting;

(ii) HR;

(iii) CRM;

(iv) Basel, MIS and DW.

Finally the third phase includes all reporting, management and decision systems that are used for the needs of the bank.

The DRS has to provide the necessary standby equipment that will be used during the Disaster Recovery phase. For the alternative site activation the responsible IT teams can choose the most effective and valid method for implementation of this. The basic parameters for choosing what method to follow are the recovery time, efficacy and

cost of implementation and maintenance. Also, it is not necessary to use the same method for all systems, but they must select the best way for each of them. Usually, the critical systems are standby and setup with similar configuration from the primary site. When DRS will be activated, these systems will be directly available and the only process that must be completed is the restoration of last data from the latest (archive) backup. In this approach, the recovery time and procedures are direct and simplified. On the other hand, for non-priority systems, it is not required to be in standby mode because the timeframe is not restricted. After the interruption of primary site, these systems will be created from the scratch by using the latest full backup with all the data which are available.

Because the backup infrastructure and process is vital for the Disaster Recovery phase is necessary to keep a backup plan for the critical IT equipments (hardware and software), configuration of systems and data. Usually, a backup of all critical systems occurs daily (after the end of a normal business day) and these (stored in removable media) are sent to an alternative site the next day, so that they will be available when required.

In addition, it is important to specify in which situations the DRS will be activated. As a general rule, if an individual system is damaged and can be back to normal operation in less time than it takes to activate the alternate site, then it will be recommended to start the recovering process in primary site by using the backup/restore solution.

Also, except from the IT equipment, the institute should predict alternative workplace for the employees and the relevant equipments (workstations, telephones, fax, printers, etc.).

The central bank of Greece requires the existence of DRP testing procedures, according to which the frequency of testing DR site (minimum one time of year and when occurring changes to critical equipments) and the goals of the test are specified. Additional requirement is the creation of a report that includes the results of the testing procedures. This documented report must be published to management and audit team. The results of the testing procedures will help the bank to correct and adjust any problems that will appear during the test.

Finally, the DRP, like as the BCP, must be simply documented and published so as all the employees will be informed for the plans.

10. Conclusions

The necessity of Business Continuity Management and Plan is undeniable for companies/organizations that want to ensure the continuity of critical business processes so the company fulfils its purpose and can be competitive at the market.

Since the BCM and BCP can contribute to the normal operation of the company, during the last decade many attempts have been carried out in order to create a BC framework. Additionally, many standards and guidelines have been published by internationally recognized organizations for the development of BCM/BCP. The aim of these standards and guidelines is to provide processes of business continuity to any company/organization that wants to have any critical services available. The differences among these standards are the perspectives and approaches of the business continuity strategy (for example some of the standards focus on IT, others have been created for financial or government institutions and other try to cover the entire range of a business operation). On the other hand, these standards present common process for the BCP creation, such as:

- Definition of BC strategy;
- Business Impact Analysis (BIA) and Risk Analysis (RA);
- Development of BCP; and
- Test and maintenance of BCP.

Through this research we can conclude that the effectiveness and reliability of BCP depends on the valid results from the business impact, risk analysis and the frequency of testing and maintenance.

The BIA and RA are the backbone of the process because the creation of BCP will be based on the data that arise from the analysis. When the information is incorrect or incomplete there is a high risk the company has made the wrong decisions regarding the plan, resulting to endangering the business continuity of critical services. Opposite, having created the plan based on proper data, activation of this, in case of interruption/destruction of critical infrastructure (whether it’s total or partial), will be immediate and effective because it will provide all necessary procedures and mechanisms in accordance with the company's requirements.

Additionally, as well as the plan is designed, some factors and situations can’t be predicted if this hasn’t been tested on similar conditions. The results of the testing procedures will help the company to correct and adjust any problems that will appear during the test so to avoid future problems in the real disaster.

Finally, the continuity plan it’s important to be reviewed and updated frequently (at least once a year) so that adapts to the latest significant changes and strategic company decisions.

Bibliography / Reference

[1] “NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems” by Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas, National Institute of Standards and Technology (NIST), June 2002

[2] “BS 25999-1:2006, Business continuity management – Part 1: Code of practice” by British Standard (BSI), November 2006

[3] “BS 25999-2:2007, Business continuity management – Part 2: Specification” by British Standard (BSI), November 2007

[4] “BS 25999 –a framework for resilience and success” by Robert Whitcher, BCI Webinar June, 2009

[5] “The Route Map to Business Continuity Management: Meeting the requirements of BS 25999” by John Sharp, 31 December 2007

[6] “BS 25999: Key Issues to Address for Certification” by Malcolm Cornish, the business continuity Journal, October 2009

[7] “Improving Business Continuity BS 25999 and Beyond” BSI 4th Annual Conference & Workshop by Dave Adamson, British Standards, May 2009

[8] “How to Deploy BS 25999 (second edition)” by BSI Management Systems America, 2007

[9] “BS 25999: A Standard for Business Continuity Management” by Jim Grogan, ACP Meeting – San Ramon, CA, July 2008

[10] “IT Business Continuity Management - An approach for Small Medium Sized Organizations” by European Network and Information Security Agency (ENISA), March 2010

[11] “Business Continuity Planning (BCP)”, IT Examination Handbook by Federal Financial Institutions Examination Council (FFIEC), March 2008

[12] “Acts 2577 9.3.2006 - Annex 2, Operational Risk Management Principles For Information Systems In Financial Institutions” by Bank of Greece Governor, 2006

[13] “Prudential Standard APS 232. Business Continuity Management” by Australian Prudential Regulation Authority (APRA), April 2005

[14] “ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems–Requirements with Guidance for Use” by American National Standards Institute Inc (ANSI), March 2009

[15] “ISO/IEC 24762. Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services” by British Standards Institute (BSI) and International Standards Organization (ISO), February 2008

[16] “HB 292-2006 A Practitioners Guide to Business Continuity Management” by Standards Australia, January 2006

[17] “HB 221:2004 Business Continuity Management” by Standards Australia and Standards New Zealand, 2004

[18] “ISO/PAS 22399:2007 Societal Security – Guideline for Incident Preparedness and Operational Continuity Management” by International Standards Organization (ISO), 2007

[19] “FEMA 141. Emergency Management Guide for Business and Industry” by Federal Emergency Management Agency (FEMA), October 1993

[20] “FSA BC Management Practice Guide” by Financial Services Authority (FSA), November 2006

[21] “COBIT 4.1. Framework Control Objectives Management Guidelines Maturity Models” by IT Governance Institute, 2007

[22] “NFPA 1600. Standard on Disaster/Emergency Management and Business Continuity Programs” by National Fire Protection Association (NFPA), 2007

[23] “Pas 77: 2006 IT Service Continuity Management” by British Standards Institute (BSI), August 2006

[24] “ITIL3 Continual Service Improvement” by the Stationery Office (TSO), 2007

[25] “Online banking” by Wikipedia, the free encyclopedia (http://en.wikipedia.org/wiki/Online_banking)

[26] “All glossary entries” by European Central Bank (http://www.ecb.int/home/glossary/html/glossa.en.html)

[27] Interbanking Systems S.A (DIAS) (www.dias.com.gr)

[28] Society for Worldwide Interbank Financial Telecommunication (SWIFT) (www.swift.com)

[29] Τειρεσίας www.tiresias.gr

[30] Κεφαλαιακή Επάρκεια (Βασιλεία ΙΙ) (http://www.bankofgreece.gr/pages/el/supervision/legalf/creditinstitutions/supervisionrules/capitaladequacy.aspx)

[31] “Management information system” by Wikipedia, the free encyclopedia (http://en.wikipedia.org/wiki/Management_information_system)

[32] “Customer relationship management” by Wikipedia, the free encyclopedia (http://en.wikipedia.org/wiki/Customer_relationship_management)