DOI: 10.5748/9788599693124-13CONTECSI/PS-3893

BUSINESS CONTINUITY AND DISASTER RECOVERY: AN OVERVIEW, TRENDS AND CHALLENGES

José Bras (Escola de Comunicação Arquitetura Artes e Tecnologias de Informação, Departamento de Engenharia Informática e Sistemas de Informação, Universidade Lusofona de Humanidades e Tecnologias, Lisboa Portugal) - cascaisbras@gmail.com
Rui Ribeiro (Escola de Comunicação Arquitetura Artes e Tecnologias de Informação, COPELABS, Universidade Lusofona de Humanidades e Tecnologias, Lisboa Portugal) - rui.ribeiro@ulusofona.pt

Build resilience and manage unpredictable changes within the IT and business ecosystems are fundamental to be sure the safety of a company. These key objectives need to be aligned with the continuity of their key processes in the event of a disruptive incident. For that, they need to have a well-structured business continuity plan (BCP), which complies with an enterprise wide view, meaning a covering blueprint of all the areas throughout the company, in order to achieve the objective on maintaining and restoring critical operations. Disaster recovery strategies must be well addressed and support all business continuity activities. Pinpointing and addressing these challenges is the goal of business continuity (BC). This research paper studies and presents the state-of-art of the Organizational Requirements, and conceptual foundations, more specifically about business continuity and disaster recovery concepts. Key aspects to address were found at the actual best practices of managing a business continuity plan. This paper will be the base of a wider MsC research work for the creation of a new methodology and framework to build BCP and DRPs.

Keywords: Business continuity, business transactions, business process outsourcing, business impact analysis, disaster recovery

Introduction: Business Continuity and Disaster Recovery - An overview, trends and challenges

In comparison to most other disciplines of business management, the concept of business continuity is relatively new. Born in the 1960s as IT "disaster recovery", this discipline has gained notoriety with the 09/11 terrorist attacks, in New York, and more recently with the latest wave of the Islamic state (ISIS) terrorist attacks. Due to this leverage risk, this theme is now regularly discussed in boardrooms across the global corporate landscape. However, still today, there aren't effective ways to measure objectively and consistently the level of readiness of the organization to disasters or what their disaster preparedness state is (Vistual Corporation, 2007). Business continuity and IT disaster recovery can mean the difference between life and death for a company. Together they can mean the difference in collapsing to adversities or be able to grant the continuity of a business.

A business continuity plan (BCP) and disaster recovery plan (DRP) have many definitions. The business continuity plan is more focused on planning the recovery of processes and business functions (Tashi & Ghernaouti-Helie, 2011) (Kliem & Richie, 2015), covering emergency response, business continuity, disaster recovery and also managing a crisis situation. The disaster recovery plan is the technical component of BCP and addresses the recovery of core systems, their data and communication technologies that support the business (Endorf & Johnson, 2001) (Jasper, 2007). Disaster recovery is a subset of business continuity (Snedaker, 2013).

A disaster is a catastrophic event resulting from natural causes or man, which seriously undermines or prevents entirely the normal continuity of operations. Business continuity basically establishes the strategies, procedures and critical actions needed to respond and manage a crisis situation (Tucker, 2014). It also shows, how well an organization responds to unexpected disasters, disruptions or changes (COBIT, 2013). A crisis can be a natural disaster, a catastrophe

or, might be, just a simple accident that can cause the interruption of a service, with partial or total loss of the business (ISO22301, 2012) (Heng, 2007).

The British Standards Institution defines Business Continuity (BC) as the "capability of the organization to continue the delivery of products or services at acceptable predefined levels following a disruptive event". It also defines Business Continuity Management (BCM) as an "holistic management process, that identifies potential threats to an organization and the impacts to business operations 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" (ISO22301, 2012). Moreover, The British Continuity Institute, (BCI, 2009) states that the purpose of a business continuity plan, is to provide a documented framework and processes to allow an organization to resume all of its business processes within its recovery time objective after a disruptive incident.

Having these set of objectives in mind, it is critical to have a full view of the organization and a tangible and consistent plan that ensures the completeness of the organization's mission and strategy, and ensures the continuity of the operation. For that, it is necessary to create a full map of all critical and non-critical processes to have an organization, if needed, replicated in a different environment using deputies and understudies. They will resume the mapped processes in order for reconstructing vital operations and ensure the resumption of time-sensitive operations and services in the event of an emergency, within a short time frame. Therefore, defining all critical process and elements needed to perform those tasks is fundamental to ensure the business continuity and to have the organizational resilience (Hiles, 2010). One of the main challenges to implement an in-house BCP and DRP is to establishing the required knowledge

about all the key resources, key activities and key elements. For example, after a disruptive event, an organization needs to establish re-design and re-engineering processes, in order to adapt their business to new realities. Thus, it is pertinent that in a crisis, that an enterprise has a structured methodology and a toolset which will allow to change / adapt their processes and permit the enterprise operations to continue to work, with the available/existing resources, even if in a partial capabilities of production.

In resume, a business continuity plan is an essential tool that aims to ensure that the company is prepared for immediate recovery of its critical activities and its support systems and applications, in the event of a disaster. Both plans (BCP / DRP) describe the actions to be implemented, the necessary resources and the procedures to be followed before, during and after a disaster. The plans are designed to minimize the impacts in terms of human resources, operational and financial impacts inherent of a disaster situation.

Some of the main objectives of having a BCP and a DRP described by the literature are (COBIT, 2013) (ISO22301, 2012) (Hiles & Noakes-Fry, 2014):

- Define guidelines to ensure the safety of employees;
- Minimize downtime and data loss;
- Protect and prevent the organization, in the event that all or part of its operations and/or computer services become unusable;
- Develop recovery strategies;
- Identify preventive controls;
- Address advance preparations and actions to be taken in response to disruptions;
- Address the potential impact of varying levels of disruptions;
- Ensure that business will continue offering critical services;

– Ensure that business will survive to a disastrous event.

Thus, it needs to ensure a quick and effective response to the unexpected through a framework of actions, procedures and protocols capable of managing a Severe Business Disruption (SBD). For that reason, there is the need to assure that there are predefined ways to measure and establish metrics concerned to goals, related to both program performance and recoverability.

Within this research paper, that is the base of a wider MsC research, there is a goal to work in the creation of a new methodology and framework to build a BCP and DRPs. So this first step is to present here a state-of-art of the Organizational Requirements, the conceptual foundations, particularly about business continuity and disaster recovery concepts, as well as some insights collected from key stakeholders and managers.

Organizational Requirements

The aim of this section is to provide important information to assist the understanding of the organization's needs and constraints, while building a business continuity and a disaster recovery plan.

To develop the company's mission, there are several activities that interact within the company value chain (Porter, 1985), some of which have a direct and indirect interactions with the customers and suppliers - Primary Activities (Daft, 2015). However, its performance is dependent on several other processes - support activities. Following a disaster, it matters to recover immediately the primary activities and the essential support activities towards that goal.

The interaction between all these activities, customers, suppliers, distributors and other relevant internal or external stakeholders is carried throughout organizational processes, which generate the flows of information.

Another line of work, around this theme, is that recent studies show that organizations started to moving towards, on a wide range of core and non-core critical business processes and applications (Hongyan & Meissner, 2008), that are increasingly being outsourced (Saxena & Bharadwaj, 2007), but not always the proper measures are being taken into consideration in order to mitigate the impact of losing one of their outsourcers (Engemann & Henderson, 2011). There are different types of risks (Graham & Kaye, 2006), that a Business Process Outsource supplier arose, which might include the adverse impact to organizations in areas such as customer service, call centers, IT services, business continuity, and other areas (Handfields's, 2010) .

Although, the building of an infrastructure of an Enterprise Architecture helps on understanding the concept of an extend enterprise (Winter & Schelp, 2008), by reducing its complexity, and the outsourcing market has become more mature over the recent years (Sople,

2009), organizations also have begun to examine how these complex relationships affect the continuity of their business. Organizations started to analyze what are their dependencies from the business point of view. Despite the fact that organizations' benefit, in terms of cost management focus, innovation and ultimately by providing business value for the customer / supplier by having external services (HBPO, 2006), there is a risk associated of a sudden brake of this kind of relationship (Shi, 2007).

Business Continuity Management (BCM) allows an organization to establish resilience to threats (Gallagher, 2003), but to do it, there is a need to first understand the organization, what are their commitments to customers and suppliers and what is the value added by the organization, which in this case are the products, services, activities and associated resources, essential to ensure the continuity of its critical activities at an appropriate level (Engemann & Henderson, 2011) (Drucker, 1993). Therefore, during a BCP life cycle, understanding the organization value chain is crucial and is one of the steps to take during the BCM Program Management (Watters, 2013). Figure 1 represents the BCP lifecycle where highlights the fact, that is necessary, to embed the BCM in the organization's culture.

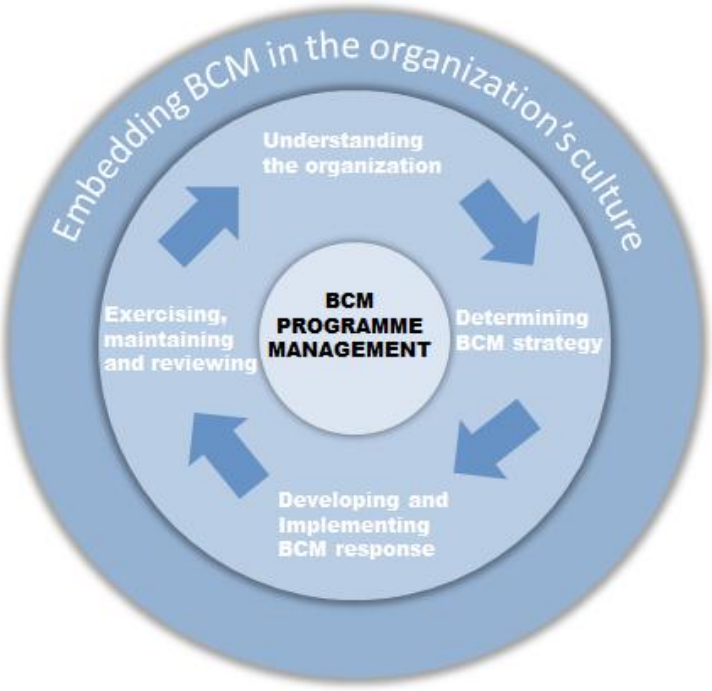

Figure 1 The BCM Lifecycle (Adapted from the British Standards Institution's BCM Code of Practice (BS25999-1. Now ISO22301) (BCI, 2009).

With the requirements to implement and maintain a business continuity plan, an organization shall then identify organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident (Drewitt, 2013). Additionally, it links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy, must also be included. These are aims to determine external and internal issues that are relevant to achieve its Business Continuity Management Solution (ISO22301, 2012).

Another key step of the BCP is the business impact analysis (BIA). As soon as the risks to an organization have been identified – normally over a risk analysis (Hiles, 2002) - the organization is ready to perform a business impact analysis.

BIA is useful to determine how the identified risks can affect specific business units operations and forms the foundation from which the BCM process is developed (Engemann & Henderson, 2011). The complete BIA sequence with all the necessary steps needed to complete the procedure, can be found on figure 2.

Figure 2 - Business Impact Analysis – This figure represents the necessary steps to manage a complete BIA sequence (Adapted from Enterprise Risk Management).

A Business Impact Analysis addresses and helps on the following subjects:

- Understanding business environments;
- Establishment of the efforts towards obtaining information related to internal and external environments;
- Gathering data and information to identify critical processes;
- Evaluation of the critical operations for the organization and determine the resources needed to run them;
- Providing meaningful information from which recovery strategies can be determined;
- Involvement of all stakeholders in the planning process to obtain their inputs about the business processes;
- Obtainment of all-important Executive Support, that will give the necessary authority to the analysis;
- Defining the recovery time objectives (RTO)
- Defining the recovery point objectives (RPO)

However, during a BIA process, mistakes should be minimized, due to the fact that this process is a central part for the development of business continuity plan (BCP). Understanding this process is critical and like detailed by Steven Ross, and resumed in Table 1, reproduces the ten most common BIA mistakes and presents a briefly explanation about them.

A Business Continuity Management lifecycle, normally addresses the following tests / exercises to be completed every year:

(i) Call tree exercise with all company members and key suppliers;

(ii) Structured walkthrough with top management;

(iii) Business Continuity test with the designated area team members;

(iv) Disaster Recovery test with IT members;

(v) Tabletop exercises with area managers.

Some other topics are also very important for this lifecycle:

(i) Update all documents is vital and needs to be reviewed frequently, as a company reality changes very often;

(ii) Testing the plans is crucial, to check the plans' effectiveness;

(iii) Cross teams to test the implemented solution is fundamental, as it ensures that the plans are well build and accurate;

(iv) Testing the solution with different levels of stress, is also desirable;

Business continuity planning should include ways to ensure the continuous delivery of critical services and products. Among other important things, like having DRP properly documented and tested, the necessary equipment identified, a backup or alternate site available, it is also crucial to create and train a team to face and deal with unexpected events. Figure 3 is an example of a BCP team organization chart showing their relationship.

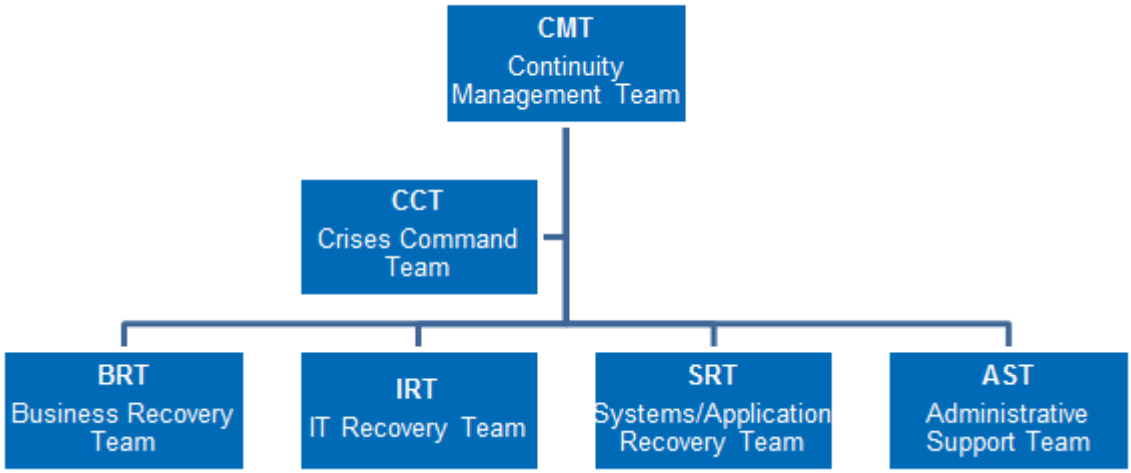

Figure 3 –Business Continuity Team organization chart

Each team should have a Team Leader and a backup Team leader. All elements for the BRT, IRT, SRT and AST should be identified inside the company and must also have a backup element. A brief summary of each team's responsibilities shall be as hereinafter:

CMT – Continuity Management Team

Consists of the most senior manager (at the moment of the SBD) and includes all elements of the management board. Responsible for the decision-making and assumes the overall management of all phases of the recovery process, until the headquarters is recovered or rebuilt in another location.

CCT – Crises Command Team

This team will support, as first line, the CMT in the activation and operation of the Business Continuity Plan. In addition to the CMT, this team is the only authoritative source to give information on the disaster situation and the state of the recovery process and is responsible for the coordination with the public authorities. All communication (external and internal) is controlled by this team, after the approval of the CMT Leader.

BRT – Business Recovery Team

This team have the responsibility to operationalize the recovery of processes / activities according to the strategy process recovery.

IRT – IT Recovery Team

This team ensures the recovery of the IT infrastructure necessary to support the recovery of all processes / activities related with the business. Also has responsibilities related with voice and data communication with other parties.

SRT – Systems / Applications Recovery Team

Responsible for the recovery of systems and applications necessary for the recovery of processes / activities that support the business activities.

AST – Administrative Support Team

This team will provide logistical and administrative support to the teams responsible for recovery, have an essential role in the inventory of the damage. In addition, will also prepare the recovery of some back-office activities, including accounting and treasury.

Insights from key stakeholders and managers

This section provides an insight from the business key stakeholders and managers, regarding the need to change the actual paradigms for conducting the Business Continuity Management Program.

In fact, the path has been to further standardize and enshrine the traditional approaches to manage BCP and DRP, instead of looking for ways to streamline processes to manage them.

For example, managers complain quite often about the lack of a common language when capturing and documenting the business processes. This sometimes creates misinterpretation among departments that interact to accomplish a specific process.

Furthermore, a number of issues that practitioners actually suffer from when dealing with conventional methods to capture business process, need a solution. These methods are based on flowchart and activity based modelling representations. They need to have a coherent design and structurally complete business process descriptions.

The incorrect documentation and description of the processes, that support the business, will affect the results of the Business Impact Analyses process. A more precise overview of the whole business process, with all the identified organization's activities, dependencies and relationships with interested parties, showing all possible interactions, would help BIA to reflect a more accurate calculation of the impact of a SBD at the business.

Moreover, managers need to reduce the complexity of some of the representation of complex business processes. They need, at the same time, to capture and preserve knowledge (essential to mitigate risk), and to have a way to share it more easily within the organization’s ecosystem.

Managers' complaint that they don't have key indicators to measure the degree of compliance of preparedness to recover from a disaster, neither a way to understand if they are to be recoverable.

Methodology

This section explains the research methodology that will be used to gather information related to the subject presented at this paper.

The research methodology used was based on four steps:

(i) Identification of the problem – based on the feedback given from the BC practitioners, from the participants of the exercises of business continuity and from managers.

(ii) Defining objectives - defined based on business needs, by reviewing literature and by observing best practices from other disciplines. The aim is to identify the possible solutions for the problems found.

(iii) Designing and developing possible solutions - creation of a new methodology and framework to build BCP and DRPs.

(iv) Presentation of the solution found - the new methodology will be presented and explained on further studies that will be the base of a wider MsC research work.

Resume and Future work

It was noted, at this research, that in the last two decades, the way business continuity professionals do their work didn't change much. Only small incremental changes, mainly focused on compliance and regulatory requirements.

There are examples from several other disciplines that have shifted their paradigms or adopted new methodologies, with major improvements and efficiency: Enterprise Engineering with DEMO (Dietz, 2006); Project Management with Lean and Agile; Enterprise Architecture with TOGAF (TOGAF, 2011), Quality control with Six Sigma and so on. Some hybrid methodologies were also found: Lean Six Sigma; Lean Project Management and Enterprise Operation Analyses (EOA) (Dudok, Guerreiro, Bakin, & Kervel, 2015), are examples.

There is also a need to engage key stakeholders to this activity in a yearly basis, even throughout the tests and all exercises related to BCP and DRP that are done to accomplish with the objectives. With this, the need to have influence/sponsorship is essential. Influence for the practitioners to have resources and to take the time to learn the business and deliver value to it.

It is also required to measure the degree of the organizations' preparedness to recover from disaster and to know which processes and operations are to be recoverable. The key milestones are counted, but measures of effectiveness for the key BC objectives don't exist. There is a need to create metrics concerned to goals, which are related to both program performance and recoverability.

With this research we point out the following major pillars for future research:

(i) Get the techniques or incentives to properly engage participants and executives;

(ii) Obtain quality metrics from the procedures (Business continuity-oriented quality metrics);

(iii) Find ways of measuring preparedness;

(iv) Arrange new ways of representing the business processes;

References

BCI, C. (2009). Risk and business continuity management guide. *Business Continuity Institute*.

Blyth, M. (2009). *Business Continuity Management: Building an Effective Incident Management Plan.* Wiley.

Braun, C., & Winter, R. (2007). Integration of IT service management into enterprise architecture. *ACM symposium on Applied computing* (pp. 1215--1219). ACM.

Cardoza, B. (2006). *Building a Business Impact Analysis (BIA) Process: A Hands-on Blueprint.* Retrieved from https://books.google.pt/books?id=EqCeGQAACAAJ

COBIT. (2013). *Cobit 5 for Assurance.* ISACA. Retrieved from https://books.google.pt/books?id=FDdbAwAAQBAJ&lpg=PA1&dq=cobit%205&hl=pt-PT&pg=PA2#v=onepage&q=cobit%205&f=false

Daft, R. (2015). *Organization Theory and Design.* Cengage Learning. Retrieved from https://books.google.pt/books?id=yPq5BwAAQBAJ

Dietz, J. (2006). Enterprise ontology: theory and methodology. 2006. *Berling: Springer*.

Drewitt, T. (2013). *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system.* IT Governance Ltd.

Drucker, P. F. (1993). *Concept of the Corporation.* Transaction Publishers.

Dudok, E., Guerreiro, S., Bakin, E., & Kervel, S. J. (2015). Enterprise Operational Analysis Using DEMO and the Enterprise Operating System. Prague: Springer International Publishing Switzerland.

Endorf, C., & Johnson, C. (2001). *Secured Computing: A CISSP Study Guide.* Trafford. Retrieved from https://books.google.pt/books?id=xqhnmTrRiasC

Engemann, K. J., & Henderson, D. M. (2011). *Business continuity and risk management.* Rothstien Association Inc., Publisher. Brookfield, Connecticut USA. Retrieved from www. rothstien. com.

Gallagher, M. (2003). Business Continuity Management. *Accountancy Ireland, 35*, 15--16.

Graham, J., & Kaye, D. (2006). *A risk management approach to business continuity: aligning business continuity with corporate governance.* Rothstein Associates Inc.

Handfields's, R. (2010, November). Are Companies Considering the Risks of BPO? NC State University. Retrieved from http://scm.ncsu.edu/blog/2010/11/07/are-companies-considering-the-risks-of-bpo/

HBPO. (2006). Secret of Organizational Sucess In An Ever Increasing Competitive Environement. *Business Process Outsourcing*.

Heng, G. M. (2007). *Managing Sustaining Your Business Continuity Management Program.* GMH.

Hiles, A. (2002). *Enterprise risk assessment and business impact analysis: Best practices.* Rothstein Associates Inc.

Hiles, A. (2010). *The definitive handbook of business continuity management.* John Wiley & Sons.

Hiles, A., & Noakes-Fry, K. (2014). *Business Continuity Management: Global Best Practices, 4th Edition.* Rothstein Associates Incorporated. Retrieved from https://books.google.pt/books?id=GmX6ngEACAAJ

Hongyan, L., & Meissner, J. (2008). *Improving Quality in Business Process Outsourcing through Technology.* Working Paper (available at http://www.meiss.com), Lancaster University Management School. Retrieved from http://www.meiss.com/download/BPO-Li-Meissner.pdf

ISO22301. (2012). *Business Continuity Management.* British Standards Institution.

Jasper, M. (2007). *Protecting Your Business: Disaster Preparation and the Law* (Vol. Legal Almanac Series). Oceana Publications. Retrieved from https://books.google.pt/books?id=wNMtAQAAIAAJ

Kliem, R., & Richie, G. (2015). *Business Continuity Planning: A Project Management Approach.* CRC Press. Retrieved from https://books.google.pt/books?id=utqYCgAAQBAJ

Porter, M. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance.* Free Press. Retrieved from https://books.google.pt/books?id=o1y1AAAAIAAJ

Saxena, K., & Bharadwaj, S. S. (2007). *Business Process Outsourcing: For Strategic Advantage.* Excel books.

Shi, Y. (2007). Today's solution and tomorrow's problem: the business process outsourcing risk management puzzle. *California Management Review, 49*, 27--44.

Snedaker, S. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals.* Elsevier Science. Retrieved from https://books.google.pt/books?id=vT8TAAAAQBAJ

Sople, V. V. (2009). *Business Process Outsourcing: A Supply Chain of Expertises.* PHI Learning Pvt. Ltd.

Tashi, I., & Ghernaouti-Helie, S. (2011). *Information Security Evaluation: A Holistic Approach from a Business Perspective},*. EFPL Press. Retrieved from https://books.google.pt/books?id=UBHlAgAAQBAJ

TOGAF. (2011). TOGAF Version 9.1. Open Group Standard.

Tucker, E. (2014). *Business Continuity from Preparedness to Recovery: A Standards-Based Approach.* Elsevier Science. Retrieved from https://books.google.pt/books?id=v95FBAAAQBAJ

Vistual Corporation, I. (2007). Business Continuity Maturity Model. Retrieved from https://www.virtual-corp.net

Watters, J. (2013). *Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference.* Apress.

Winter, R., & Schelp, J. (2008). Enterprise architecture governance: the need for a business-to-IT approach. *ACM symposium on Applied computing* (pp. 548--552). ACM.

Table 1

A business impact analysis checklist: 10 common BIA mistakes. Adapted from (TechTarget - Steven Ross, 2010).

BIA Mistakes	Explanation
"Considering the impact of interrupted applications, not business functions":	The objective to perform a business impact analysis is the business not the application itself. The focus is the organizations and the business functions that are part of it. The question here is what impact an organization would expect if a specific business function could not be executed.
"Considering applications in isolation":	The question here is not to consider the whole and look only to the application that a specific role relies on. It is extremely important to analyze what are the dependencies between applications and also in what infrastructure those applications rely on.
"Paying too little attention to financial impact":	Not knowing the organization and the business as a whole leads to paying less emphasis on certain aspects of the financial impact when a business process is not working and the consequences therefore may exist.
"Paying too much attention to financial impact":	Other impacts are also important to organizations, legal, regulatory and image, as well as reputation are a concern to senior management. Managers should have a holistic vision of the organization and need to understand the ontological essence of their enterprise as they are held accountable [5].
"Failing to distinguish enterprise applications":	Some applications, whose impact is self-evident, are easy to determine their importance for the organization. However others aren't, as they may serve only a business unity or fewer users and therefore may be difficult to determine the overall impact of those applications.

"Failing to recognize data center applications":	Determining the correct recovery sequence when we have applications that do not have business users to support can be tricky as they can be the support for all the other applications to work.
"Confusing a risk assessment with a business impact analysis":	Risk assessment is used to deliberate the causes for an outage; BIA specifies the effects if that occurs. Having the big picture helps a lot.
"Confusing risk acceptance with a business impact analysis":	The BIA process is sometimes quite di cult to perform because it is necessary to have a full map of all dependencies and interactions with all stakeholders. This isn't a quick or easy task to achieve. Managers are not willing to spend much time and tend to accept the risk rather than have the analysis done. This doesn't mean that is not necessary to determine the impact of this choice.
"Pre-determining BIA results":	Jumping to conclusions without doing the correct assessment is a common issue just because managers tend to assume what is obvious for them.
"Backing into a BIA result":	Business managers can choose to underestimate the impacts caused by their applications being unavailable because of perceived recovery cost.