


| | |
|--|--|
|  http://d2cigre.org | CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS |
| | STUDY COMMITTEE D2 INFORMATION SYSTEMS AND TELECOMMUNICATION 2013 Colloquium November 13-15, 2013 Mysore – KARNATAKA - INDIA |

D2-01_17

PREPARING ICT TOWARDS ELECTRICAL BUSINESS CONTINUITY

by

Jorge Costa*

UTE

(UY)

SUMMARY

Reliability is a major goal in the utility sector: keeping electricity supply is becoming increasingly important, even in case of fires, floods and other natural disasters. In such disaster situations, it is acceptable to provide a degraded service for a short period.

Reliability is also a usual concern of ICT services, perhaps as a result of their critical resources, which were originally quite concentrated. Because of this, the role of ICT is to promote, within the organization, awareness about this topic, get some definitions of the organization and other important inputs, and be prepared to contribute to that major goal.

The discipline that ensures the business is uninterrupted is the Business Continuity Management (BCM).

Business Continuity Management includes disaster recovery, but it is mostly oriented to prevention, looking for establishing a culture among the organization towards improving the resilience of the services.

BCM focuses on business processes rather than on particular equipment, such as IT system, since, in order to operate, an organization must continue the execution of its critical business processes.

BCM seeks to ensure that the processes of the organization are protected from disruption and that the organization is able to respond positively and effectively when disruption occurs. The organization sets its BCM priorities, and within that context, the critical ICT services must be resilient and able to recover to the default levels, within the time required and agreed upon by the organization. Therefore, an effective Business Continuity Management depends on the continuity of ICT to ensure that the organization can meet its objectives at all times, especially during downtime.

This paper includes, based on the ISO/IEC27031 and others standards, a methodology and some recommendations for ICT services to be ready to support business operations in the event of emerging events and incidents that could affect continuity of critical business functions.

KEYWORDS

Reliability of an ICT Service, Business Continuity Management, Business Impact Analysis, Critical ICT Service, Minimum Business Continuity Objective, Role of ICT

* Jujuy 2611, Montevideo, URUGUAY, 11800
 Fax: + 598 22082299 e-mail: jcosta@ute.com.uy

1. Reliability of the electrical service

Electricity is an indispensable part of modern day life. Our economy, job, healthcare, and livelihood all depend upon constant supply of power.

A disaster is a natural or man-made hazard resulting in an event of substantial extent causing significant physical or economic damages, it can also cause loss of lives or drastic changes in environment.

Faced with a disaster situation, it is usually tolerated a degradation of electric supply service for a short period of time.

2. Recently majors blackouts (from Wikipedia)

The July 2012 India blackout was the largest power outage in history, occurring as two separate events on 30 and 31 July 2012. The outage affected over 620 million people, about 9% of the World population. An estimated 32 GW of generating capacity was taken offline in the outage. Electrical power was restored in the affected locations between 31 July and 1 August 2012.

The Indian electrical infrastructure was generally considered unreliable. In the summer of 2012, extreme heat caused power usage to reach record levels in New Delhi. Due to the late arrival of monsoons, agricultural areas demanded increased power from the grid for running irrigation pumps to paddy fields. The late monsoon also meant that hydropower plants were generating less than their usual production

Before the grid collapse, the private sector spent \$29 billion to build their own independent power stations in order to provide reliable power to their factories. The 5 biggest consumers of electricity in India have private off-grid supplies.

The 2009 Brazil and Paraguay blackout was a power outage that occurred throughout much of Brazil (affecting 60 million people in Brazil) and, for a short time, the whole Paraguay on Tuesday, November 10, 2009, at approximately 22:15.

Heavy rains and strong winds caused damages on three transformers feeding a key high-voltage transmission line, causing the complete loss of 14 GW of power and the shutdown of the Itaipu Dam for the first time in its 25-year history.

3. Other kind of risk

Not all risks to business of a utility are linked to a prolonged outage.

In 1993 the upper floors of the headquarters of UTE (the Uruguayan electricity company, www.ute.com.uy) were burned.

Although this caused chiefly the loss of human lives, there were also there the only processing data centre, the PBX, the call centre for customer care, and the leased lines connecting the central office with other administrative or technical offices.

There was no blackout, but the commercial system stopped working for a month and support services were seriously affected. The situation returned to normal after a year, taking significant losses.

4. Reliability of an ICT service

Technological issues and vulnerabilities arising from resources concentration, as the example above, have historically pushed to increasing reliability in ICT services. Nowadays is not uncommon to find: external data storage for backup, double data centre, server virtualization, cloud computing, ring topologies and redundancy of equipment or media for increase ICT service availability.

However, it should not be forgotten that in an electric utility, the ultimate goal is not the ICT service, but the electrical business. Therefore, the reliability of ICT services will be relevant to the extent that they support the business objectives.

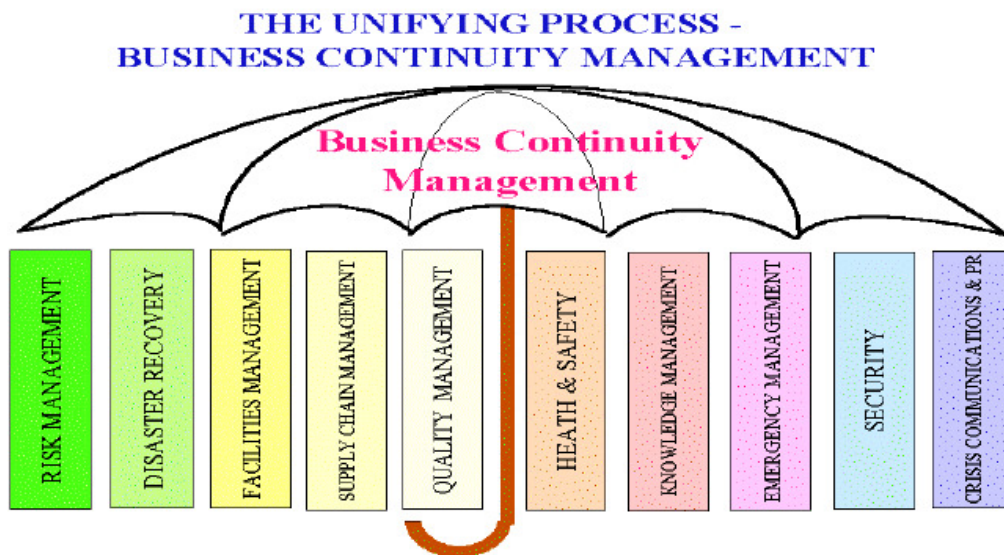
5. Business Continuity Management (BCM)

BCM is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.

Traditional disaster planning has focused on the restoration of facilities after a major incident, such as the loss of a building or plant through fire, flood or loss of computer or telecommunications across the enterprise.

The disaster recovery plans are generally written to the base of the recovery after a major event: the loss of a plant through fire or flood or the loss of computer or telecommunications systems across the enterprise.

BCM is about prevention, seeks to establish a culture within organizations to generate greater resilience to ensure continuity of service delivery.



(From Business Continuity Institute)

In order to operate, an organization must execute its critical business processes. BCM focuses on the entire business processes and not in certain assets such as ICT systems

6. Evaluating Threats to Critical Activities

In a BCM context, the level of risk should be understood specifically regarding to the organization's critical activities and the risk of a disruption to these.

Critical activities are underpinned by resources such as people, processes, technology infrastructure and physical infrastructure

The organization must understand the threats to these resources, vulnerabilities of each one, and the impact of a threat if it became an incident and caused a business interruption. The risk assessment method chosen depends on the organization, and it is important that this approach is adequate to meet its needs.

7. Business Impact Analysis (BIA)

The whole concept of business continuity is based on the identification of all business functions within an organization, and the assignment of a level of importance to each business function. A business impact analysis is the main tool to collect this information and assigning criticality, is therefore part of the foundation of business continuity.

Most standards require the business impact analysis should be reviewed at defined intervals appropriate for every organization and whenever any of the following cases occur:

- Significant changes in internal business process, location or technology
- Significant changes in the external business environment - such as market or regulatory change

As a result of a business impact analysis (BIA) and risk assessment, the organization must identify measures to:

- Reduce the chance of an interruption
- Shorten the interruption period
- Limit the impact of a disruption in the organization's key products and services

Since not all risks can be avoided or reduced to an acceptable level, loss mitigation strategies can be used.

As part of its program of BCM, the organization shall classify their activities according to their priority for recovery.

8. Maximum Tolerable Downtime

Top management should agree on the requirements of business continuity

For each critical process, the organization needs to determine the longest amount of time the process can be unavailable before that unavailability threatens the survival of the business.

This figure is known as the maximum tolerable downtime (MTD).

After the organization has established the MTD for each critical process or activity, it is time to set some specific goals for each process recovery. The two primary recovery objectives established in a BIA are:

1. Recovery Time Objective (RTO) - Target of time set for the resumption of delivering a product, service or activity after an incident
2. Recovery Point Objective (RPO) - previous point in time at which the data should be recovered to resume service.

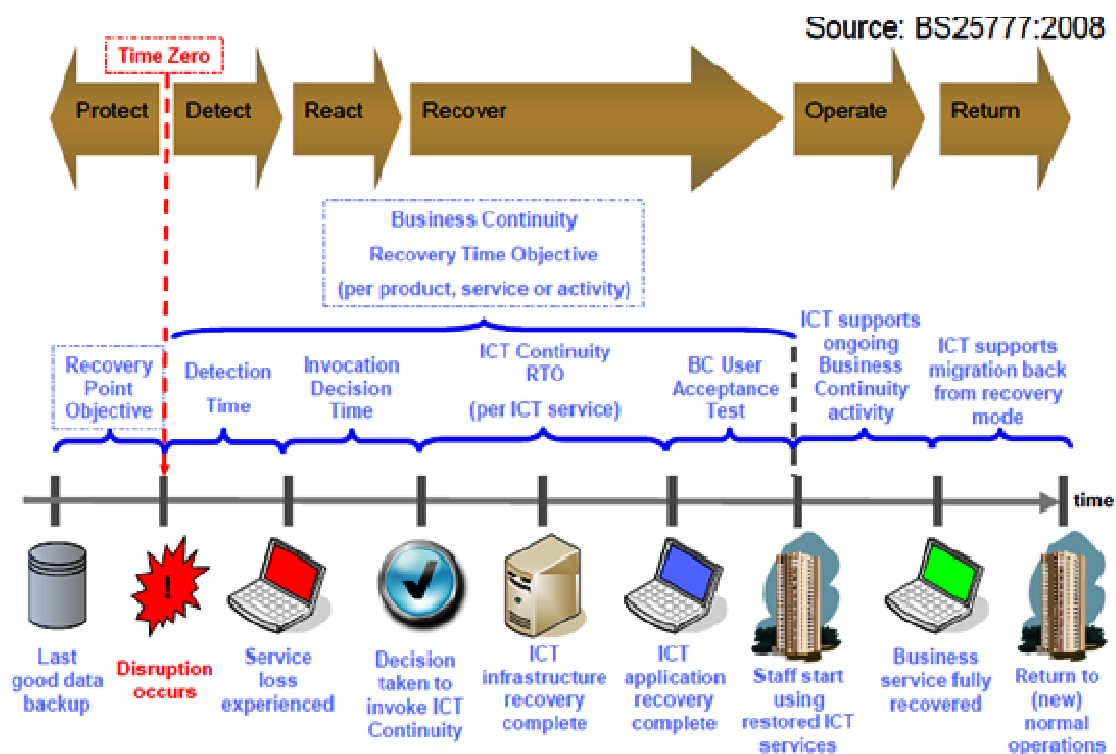
9. Critical ICT services

The organization must define its significant ICT services.

Within these ICT services, it must identify those required to achieve RTO and RPO objectives for each critical activity, as prioritized by the BCM program. These services are called critical ICT services.

The organization shall document the list of critical ICT services and ICT components that make up the end-to-end service and how they are configured or linked to deliver each critical service,

along with the required values of own RTO and RPO of that service for contributing to the achievement of the target for critical business activity.



It may also be necessary to specify the minimum capacity required for ICT services in the restoration and how this capacity should increase. Top management should agree on the list of critical services and associated ICT continuity requirements.

The resilience for each critical ICT service must be evaluated from a prevention perspective, to assess the risk of service interruption or degradation (eg., a single point of failure) and to highlight the opportunities of ICT to enhance the capacity of service recovery and therefore, reduce the probability or impact of service disruption.

This risk assessment can also advise investing to increase capacity for early detection and response to disruption of critical ICT services. The organization can decide whether to invest in these areas and how this investment is linked with business continuity management.

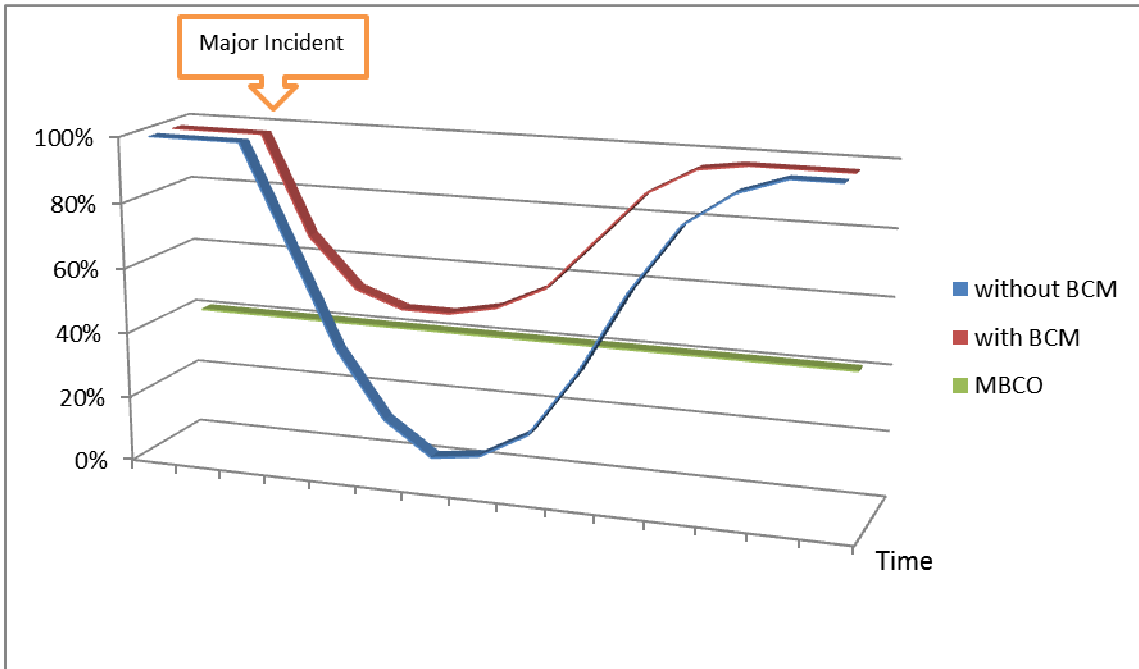
10. Precedent

Fortunately for those that are not familiarized with Business Continuity Management, this is not an unprecedented task. Although in a lesser extent, such analysis of critical business activities and their dependence on ICT services, was already made during the preparation for the potential harm from the millennium change, the Y2K issue.

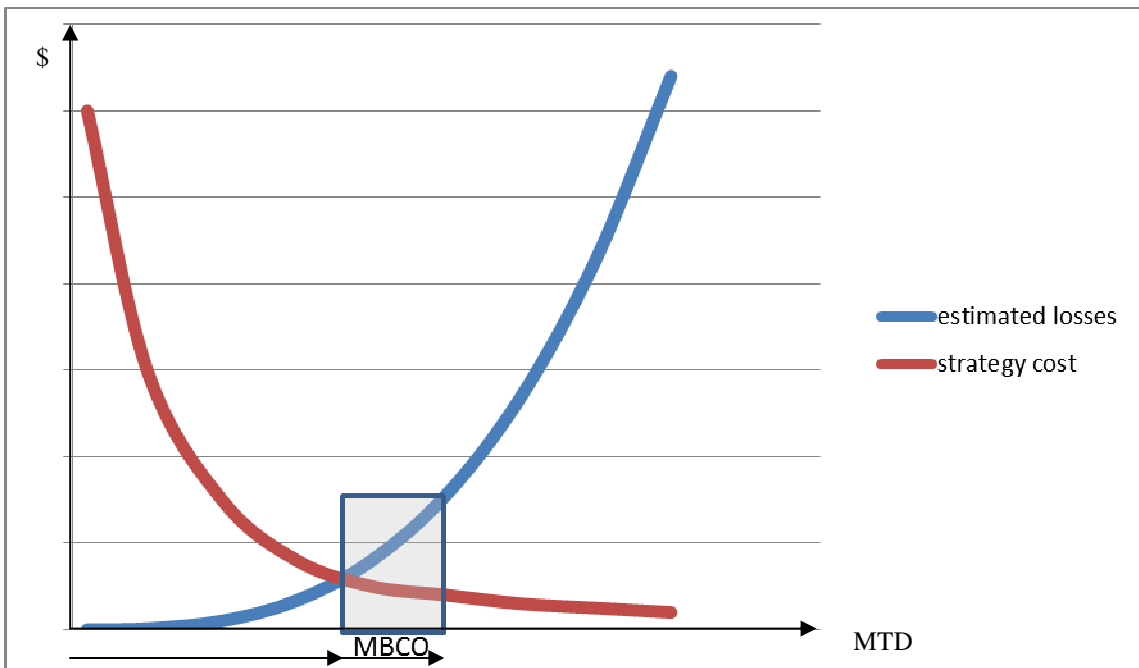
11. Minimum Business Continuity Objective

More comprehensive than MTD is the Minimum Business Continuity Objective (MBCO) MBCO is the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster. MBCO is set by the executive management of the organization and can be influenced, dictated and/or changed by current regulatory requirements or industry practices. (Source: Singapore Standard 540 - SS 540:2008)

The goal of BCM is to keep operation above the MBCO level, even facing a major incident.



Each critical activity has its own MBCO. This value could be established from an economic analysis.



The costs of losing a critical activity, including aspects such as reputation and others, rise rapidly in a function of time. Moreover, the cost of implementing a strategy to avoid disruption, or mitigate its effects, decreases while increasing the tolerated downtime. If the probability of occurrence of the event which causes loss of a critical activity is high, the appropriate value for the MBCO (or MTD) as a result of the economic analysis is the intersection of these curves. If the probability is not so high, the MTD value can increase.

The scattering of MBCO is inversely proportional to the likelihood of occurrence of the analysed threats to the critical activity.

12. The ICT Continuity approach

ICT continuity focuses not only on the likelihood and impact of disruptive incidents, but also on the ability of the organization to detect and respond to the occurrences of such incidents. This requires the organizations to control their ICT services to ensure that:

- They are resilient and recoverable at the appropriate level
- Any unexpected event within a service is detected and investigated in a timely manner
- Dependencies between ICT services and external factors are known and used in risk assessing and the impact analysis of a change
- Dependencies on the technical components are known and used in risk assessing
- ICT continuity processes are also intended to ensure that legal obligations (such as protecting personal and other sensitive data) are not breached.

13. Principles of ICT Continuity

1. **Protect:** Protecting the ICT environment from environmental problems, hardware failures, operations errors, malicious attack and natural disasters is critical to maintain the desired levels of system availability for an organization.
2. **Detect:** Detecting incidents at the earliest opportunity minimizes the impact to services and reduces the recovery efforts.
3. **React:** Reacting to an incident in the most appropriate manner leads to a more efficient recovery and minimizes any downtime.
4. **Recover:** Implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first.
5. **Improvement:** Lessons learned from large and small incidents should be documented, analyzed and reviewed. Understanding these lessons allow the organization to be better prepared to control and prevent incidents and interruptions.

14. Key elements for preparing ICT toward BCM

- a) **Staff:** specialists with appropriate knowledge and skills, and competent support staff.
- b) **Facilities:** physical environment in which ICT resources are located;
- c) **Technologies:**
 - hardware (including cabinets, servers, storage, and accessories);
 - network (including data connectivity and voice services), switches and routers
 - software, including operating systems and applications software, management software, links or interfaces between applications and batch processing routines;
- d) **Data:** application data, voice data and other data types;
- e) **Processes:** including supporting documentation to describe the configuration of ICT resources and allow operation, recovery and effective maintenance of ICT services, and
- f) **Providers:** some components of end to end services where ICT service provision could depend on an external service provider or other organization within the supply chain, for example, a telecommunications operator or an Internet service provider.

15. Role of ICT toward Business Continuity Management

ICT has the most expertise and background on this topic, therefore it must:

- promote awareness within the organization on this subject
- get from the organization the figures RTO and RPO of each critical activity which depend on ICT services
- define their own RTO and RPO for these critical ICT service
- work on the six key elements mentioned above and be prepared to contribute to the major goal.

ACRONYMS

- ICT: Information and Communication Technologies
- UTE: Usinas y Trasmisiones Eléctricas
- BCM: Business Continuity Management
- BIA: Business Impact Analysis
- MTD: Maximum Tolerable Downtime
- RTO: Recovery Time Objective
- RPO: Recovery Point Objective
- MBCO: Minimum Business Continuity Objective
- Y2K: Year 2000

BIBLIOGRAPHY

- Continuidad del Negocio (conference held at UTE in July 2012) – Juan Pablo Ruiz Naranjo, KPMG
- Business Continuity Institute
- An Introduction to ICT Continuity Based on BS 25777 - Haris Hamidovic, ISACA Journal
- BSI - British Standard BS 25777 for Information and Communications Technology continuity management.
- ISO/IEC 27031:2011 - Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity