

Since 2001, acts of terrorism in New York, London, Istanbul, Madrid and elsewhere, outbreaks of Severe Acute Respiratory Syndrome (SARS) and the Avian Flu, various widespread natural disasters have served to **heighten at international level** the priority of **Business Continuity** by underlining the substantial risk of major operational disruptions (systemic, related to certain sectors or to individual companies).

It is undoubtedly vital to have well prepared plans to cope with such calamitous events, which may even devastate an enterprise to the extent of it being left with no fixed assets, virtually no personnel and little left except a depleted balance sheet and an insurance claim, as some businesses in New York found in 2001. However, it is important not to be fixated with Doomsday scenarios, since there are many events which do not necessarily involve such drama and tragedy, but which can have terrible consequences for an enterprise of any type.

Therefore the main focus should be, as recent international statistics **more relevant for our region** revealed, on the facts that major events happened due to:

- ✓ hardware and/or system problems (44-56%)
- ✓ human mistakes (26-32%)
- ✓ software mistakes (9-16%)
- ✓ viruses (4-7%)
- ✓ natural disasters (2-3%)

**Business continuity** is an ongoing priority for all industries, including financial industry participants and the financial authorities.

Financial industry participants and financial authorities have a **shared interest** in promoting the resilience of the financial system to operational disruptions.

#### What are the factors of the interest?

- The **essential role that financial intermediation plays** in facilitating and promoting national and global economic activity by providing the means for making and receiving payments, for borrowing and lending, for effecting transactions, for insuring risks, and for raising capital and promoting investment;
- The **concentration of clearing and settlement processes** in most financial systems. Disruptions of these processes can have material adverse consequences for a financial system and prevent significant market participants from completing transactions and meeting their obligations;
- **Deepening interdependencies among financial industry participants** within and across jurisdictions. The velocity with which money and securities turn over on a daily basis underpins the considerable interdependencies – in the form of settlement risk and, ultimately, credit and liquidity risks – among financial industry participants and investors. The result is that operational disruptions at one financial industry participant can cause difficulties at others.
- The **possibility of malicious attacks** targeted, directly or indirectly, at the infrastructure or IT system of a certain major financial player or to the entire financial system;
- The **importance of public confidence in the ability of financial institutions to function smoothly**. Repeated or prolonged interruptions to the operation of a financial institution undermine confidence and could result in a withdrawal of capital from that entity by domestic and business participants.

#### Other fundamental risks

At the same time, however, other factors such as the **increasing complexity and operational risk** in all areas of the financial institutions add to the challenge of promoting the flexibility of each of these institutions and of the whole system.

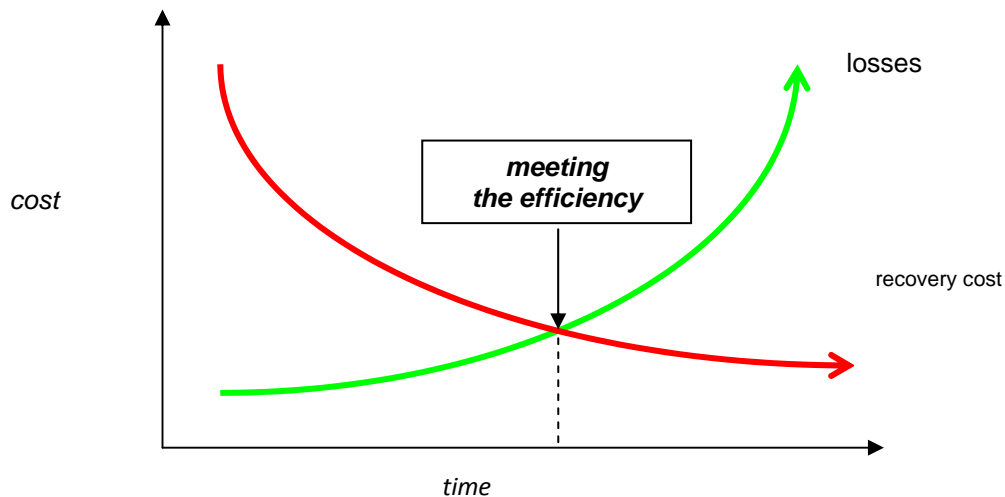
For example, every financial entity is keenly dependent on automation and, in turn, on those elements of the physical infrastructure that support automation, such as telecommunications and power.

While the organizations that provide the facilities and services comprising the physical infrastructure are actively engaged in efforts of their own to improve their resilience to major operational disruptions, financial

authorities and financial industry participants have no direct control over their decisions when major operational disruptions occur.

### Business Continuity Management

**Business continuity management**, a significant component of operational risk management, is a whole-of-business approach that includes policies, standards, and procedures for ensuring that **specified operations can be maintained or recovered efficiently** in the event of a disruption. Its purpose is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption.



Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords each financial entity a greater flexibility to address a broad range of disruptions. (e.g.: *it doesn't matter why workers cannot get in to the workplace, because of strike or epidemic. The point is that they cannot work*). At the same time, however, organizations cannot ignore the nature of the risks to which they are exposed in order to efficiently allocate the resources to the right plans and actions.

### Steps of BCM

Effective business continuity management typically incorporates

- **risk analysis,**
- **business impact analyses,**
- **recovery strategies and business continuity plans**
- **testing** programmes,
- **training and awareness** programmes,
- and **communication and crisis management** programmes.

The first step in a sensible business continuity process is to consider the potential impact of each type of disaster or event, **risk analysis**. This is critical how you can properly plan for a disaster if you have little idea of the likely impact on your business/organization. Having determined the impacts, it is now equally important to consider the magnitude of the risks which could result in these impacts. This is a critical activity-it will determine which scenarios are the most likely to occur and which should attract most attention during the planning process.

A **business impact analysis** is the starting point – it is a dynamic process for identifying critical operations and services, key internal and external dependencies and appropriate resilience levels. It assesses the risks

(with focus on operational, financial, legal and reputational risks) and potential impact of various disruption scenarios on an organization's operations and reputation.

A **recovery strategy sets** out recovery objectives and priorities that are based on the business impact analysis. Among other things, it establishes targets for the level of service the organization would seek to deliver in the event of a disruption and the framework for ultimately resuming business operations.

**Business continuity plans** provide detailed guidance for implementing the recovery strategy. They establish the **roles**, allocate **responsibilities** for managing operational disruptions, and provide clear guidance regarding the succession of authority in the event of a disruption that disables key personnel. They also clearly set out the decision-making authority and define the triggers for invoking the organization's business continuity plan. The safety of staff should be the paramount consideration of an organization's business continuity plan; but in any case, BCP has the role to cover the absence of Human, Physical, IT and also External Supplier resources.

Comprehensive, multi-dimensional and ongoing **testing programmes** are the only way to achieve the level of confidence a company needs for being sure the BCP deals effectively with a wide range of potential disruptions or disasters. They should check and validate in as realistic manner as possible whether all the critical necessary components of the business will recover using these plans.

Each plan should be the subject of **comprehensive awareness and training programmes** to ensure each employee knows what to do in case of an emergency and to allow the company to keep employees interested in the criticality of business continuity. All these should be recorded, de-briefed and subject to remedial action when deficiencies are revealed.

The **communication programmes** should outline internal and external communication channels (with regulators, investors, customers, business partners, service providers, staff, the media and other stakeholders) in the event of an operational disruption. The BCP should also incorporate comprehensive emergency communication protocols and procedures in the case of a major operational disruption.

An effective BCP should set out a **crisis management programme** that serves as documented guidance to assist a company in identifying potential crisis scenarios and develop procedures for managing these scenarios. Companies should establish crisis management teams, comprised of senior management and heads of major support functions, to respond to and manage the various stages of a crisis.

## Regulations

All these have been thoroughly analysed and promoted by many regulatory bodies, not to force other stringent regulations to the financial organizations, but to provide a framework for a stable and equilibrated financial environment.

The Basel Committee of Banking Supervision, the British Standards Institute, the American Bankers Association and the Banking Administration Institute, even the IFRS and US GAAP refer to business continuity as a foundation element for the activity of every financial institution and altogether for the whole financial system.

## Romanian situation

The Romanian banking and generally the Romanian financial landscape has changed radically in the last years and the operational risks shaped themselves into new dimensions. If a bank or a financial services provider has problems, no matter the nature of them, these can start a chain reaction able to affect the entire system.

Some operational risks have been, are and will be understood and considered by the local bankers and financial market players, even if the costs for implementing such measures to reduce the impact of these risks are quite hard to undertake or justify.

But still, it is questionable for some financial institutions or service providers for financial institutions whether they miss the real monitoring of their operational risks, if they invest in protecting themselves against the major risks. Missing one banking day can endanger their businesses, clients and partners.

It's not about having a "pretty face" in front of the Central Bank (i.e. National Bank of Romania), other financial authorities or the internal or external audits, it's about **protecting the clients and business itself**.

## What should the BCM focus on?

It about keeping the focus on the bigger but still comprehensive picture of the business itself:

- ✓ corporate/brand survival
- ✓ insurance/auditing requirements
- ✓ regulatory requirements
- ✓ due diligence
- ✓ obligation to shareholders/employees/clients/business partners

Common misconceptions like:

- ✓ "...that never happens here",
- ✓ "...we never had an outage before",
- ✓ "...we have an insurance policy, that's enough",
- ✓ "...we are immune to disasters",

are quite widespread. And as a small example, a recent study<sup>1</sup> discovered that, of the companies experiencing a "major loss" of computer records, 43% never reopened, 51% closed within two years of the loss, and a mere 6% survived over the long-term.

Business Continuity Management should be an integral part of the overall risk management program of financial industry participants. Business continuity management policies, standards and processes should be implemented on an enterprise-wide basis or, at a minimum, embedded in an organization's critical operations.

Each organization's board and senior management are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to, and continuity in the event of, operational disruptions. They should recognize that outsourcing a business operation does not transfer the associated business continuity management responsibilities to the service provider.

Therefore the board and senior management should create and promote **a real organizational culture that places a high priority on business continuity.**

## Conclusion

Any financial system is a set of interlinked networks of different types of smaller financial markets, subsystems and participants. While business organizations acknowledge the need to strengthen their resilience against disruptions, they also recognize that **the network is only as strong as its weakest link** and the potential impact of a major operational disruption may incapacitate the financial system.

That's why every financial entity which has not thought yet seriously about their business continuity should start with the **first essential step** for an organisation in the planning process - to answer in detail ten fundamental, and apparently simple questions:

- ✓ Who are we?
- ✓ What do we do?
- ✓ Why do we do it?
- ✓ Whom do we do it for?
- ✓ How do we do it?
- ✓ When do we do it?
- ✓ Where do we do it?
- ✓ What do we need to do it?
- ✓ What does it cost us to do it?

<sup>1</sup> Cummings, Maeve; Haag, Stephen; McCubbrey, Donald. 2005. [Management information systems for the information age.](#)

- ✓ Who does what for us in order to enable us to do it?

Unless organizations have that information at their fingertips they cannot say what business it is whose continuity they are trying to protect, nor can they set about planning for it. Essentially, we need that information as the basic blueprint for our enterprise: without blueprints one cannot successfully rebuild. It is surprising how many organizations will struggle to answer these questions in a structured, accurate, and succinct way.

**[Appendixes to be introduced as text boxes within the article]**

**Appendix A - Basel Committee's definitions for BC terms:**

<b>Business continuity</b>	<i>A state of continued, uninterrupted operation of a business.</i>
<b>Business Continuity Management (BCM)</b>	<i>A whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption.</i>
<b>Business Impact Analysis (BIA)</b>	<i>A component of business continuity management. Business Impact Analysis is the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements, and essential staff and to help shape a business continuity plan.</i>
<b>Business Continuity Plan (BCP)</b>	<i>A component of business continuity management. A Business Continuity Plan is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organization in the event of a disruption.</i>

Source: Basel Committee on Banking Supervision - **The High-level principles for business continuity** August 2006

**Appendix B – Business Continuity Causes and Effects (Scenarios & Outages)**

OUTAGE CATEGORIES	Human Resources	Buildings	Other fixed assets	Intangible and information assets	Services from third parties
	Loss of or injury to personnel to prevent them working	Loss, damage or denial of access to buildings	Loss, damage or disablement of other physical assets or infrastructure	Loss, damage or disablement of intangible or information assets	Loss, denial or disruption to critical third party assets or services
<b>SCENARIOS</b>					
Natural disasters e.g. storm, flood, earthquake	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
War, terrorism, hostage taking, sabotage, organizational blackmail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Man-made catastrophes e.g. fire, gas explosion, chemical spillage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Utility failures e.g. power cuts, network carriers		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transportation strikes and breakdowns	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Communications and postal disruptions				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hardware or software failures e.g. overloads, bugs				<input checked="" type="checkbox"/>	
Electronic attack e.g. virus infection, hackers, website hijack			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Employee action e.g. strikes, mass walkout, protests, sabotage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Civil disorder e.g. riots, vandalism, disruptive protests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vendor failures e.g. contractual disputes, insolvency, crashes			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Theft, fraud, embezzlement, extortion, blackmail of staff				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security compromised through error e.g. building left insecure		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Failures of internal predecessor, successor operations, supports	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Management failures e.g. damaging actions by rogue managers	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Source: Philip Cassidy - *The Essentials of BCP* Presentation to British Universities Finance Directors London Group  
25th November 2005