Disasters and Business Continuity Plans in insurance companies

Lionel Güitta
Assistant Director of Business Continuity and Contingency
MAPFRE
Madrid - Spain

Globalised world, complex business environment

The world is currently globalised and therefore companies have multiple interdependencies and connections with other companies - both clients and suppliers of goods and services.

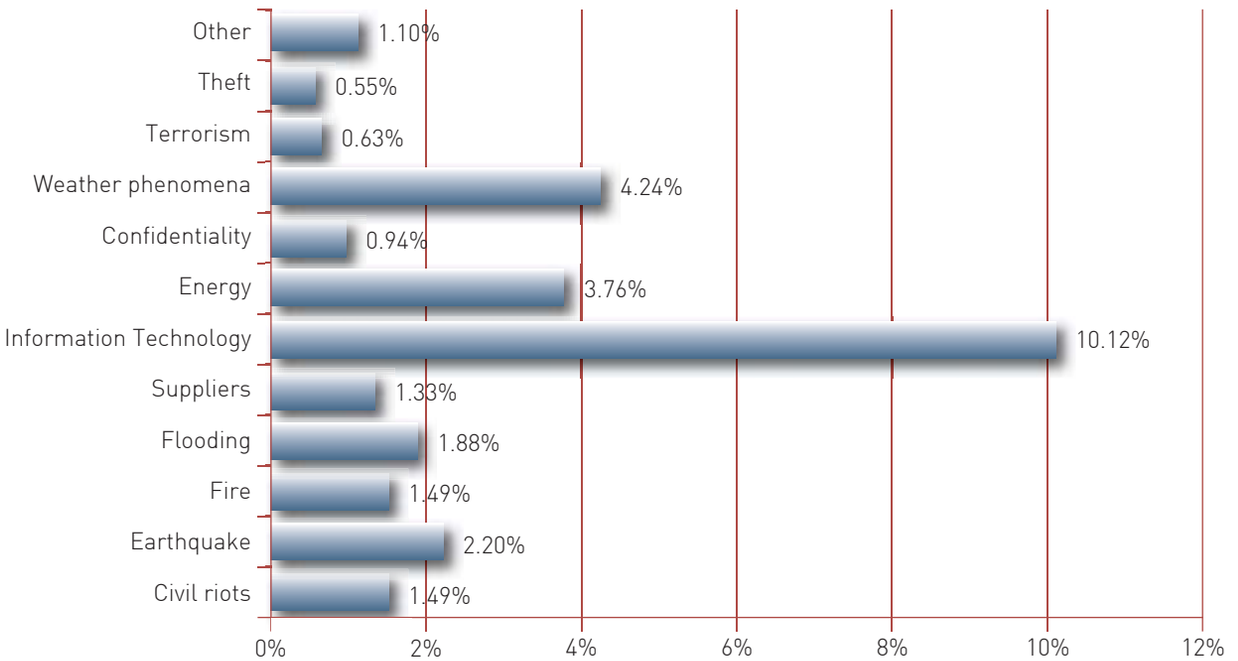
There are multiple threats in this complex environment, some of which, if they materialised, could affect not only the survival of the company that undergoes them, but also its entire network, as well as third parties that are directly or indirectly related to it.

Concerns about protecting companies against disasters emerged, first and foremost, in computing, when people became aware of the impact of technological failures -resulting in business interruption or data loss- on enterprises.

Nowadays, all companies make backup copies of the information stored on their servers or have alternative solutions that would allow them to recover their information processing capacity via alternative data processing centres, whether their own or outsourced.

Concerns about protecting companies against disasters emerged, first and foremost, in computing, when people became aware of the impact of technological failures -resulting in business interruption or data loss- on enterprises

Disasters also happen in insurance companies: Has your company had to activate the Business Continuity Plan (BCP) in the last year due to any of these reasons?
Drafted in-house.
Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.



The study was conducted between November 2011 and January 2012, with answers from 685 officers of organisations located in over forty countries, a quarter of these located outside of the USA. The results shown refer exclusively to companies in the insurance sector, which make up 10.6% of the companies participating in the study. Information Technology is the principal trigger for business continuity plans, and this includes scheduled lapses in service due to updates, maintenance and change management, as well as unscheduled interruptions due to virus attacks, denied access or communications.

Once a disaster has occurred, fully restoring a company's operations is a complex undertaking; an analysis must thus first be conducted to determine the order in which the processes should be recovered, the minimum time required for their recovery and the resources needed

However, disasters of different types and magnitudes have led companies to understand the need not only to guarantee technological recovery, but also to ensure they can continue operating their business processes and all associated resources, such as infrastructure, workstations, personnel and supplier networks.

In order to guarantee the recovery of a company's business processes after a catastrophic event, we must work in «normal times» to analyse, design and implement solutions that will enable it to recover in «times of disaster». These solutions span not only preventive or mitigating measures, but vital measures that can be deployed if the company is put out of action due to the magnitude of a disaster, maintenance shortcoming, calculation error or any other cause. They may include alternative physical locations, training employees in other areas of the business, reassigning tasks or having duplicate suppliers.

Clearly, once a disaster has occurred, fully restoring a company's operations is a complex undertaking; an analysis must thus first be conducted to determine the order in which the processes should be recovered, the minimum time required for their recovery and the resources necessary

to provide a minimally acceptable quality of service. Then solutions that will enable the company's response to the disaster will be developed: plans for recovering activity, communication plans, testing and training plans.

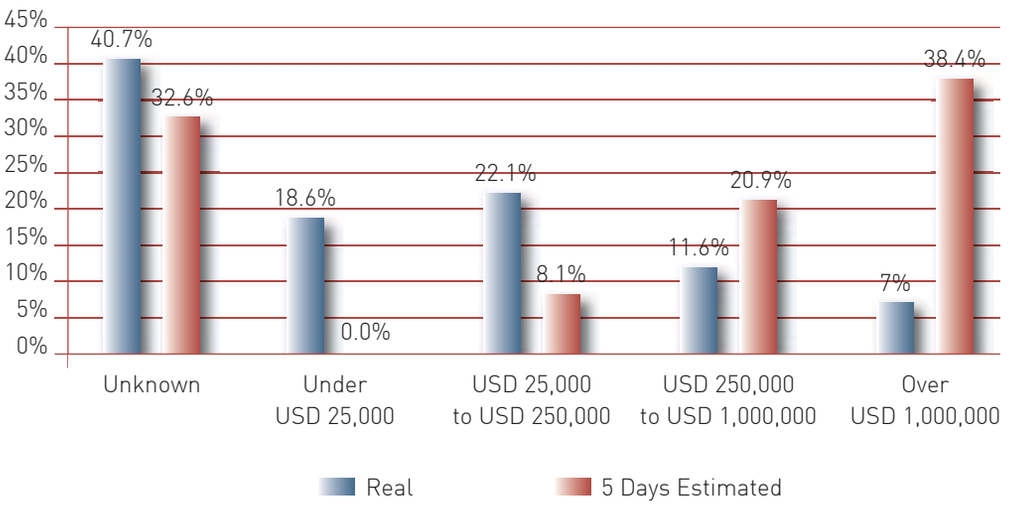
In recent years several international standards have been defined pertaining to business continuity to help organisations manage key factors for guaranteeing, as far as possible, a company's resilience in the face of disaster. The most recent international standard was published in May 2012: «ISO 22301 Societal Security - Business Continuity Management Systems - Requirements».

As regards the financial sector -and, specifically, the insurance sector- the regional or national regulator requires that companies guarantee their business continuity. Thus we can see how, in Europe, the Solvency II directive mentions the need to guarantee operational continuity:

Art. 41.4: Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertaking shall employ appropriate and proportionate systems, resources and procedures.

Several international standards have been defined pertaining to business continuity to help organisations manage key factors for guaranteeing, as far as possible, a company's resilience in the face of disaster

What are the estimated financial losses caused by incidents that have occurred in your company over the last year? And the estimated financial losses if the business were interrupted for five days? (USD)
Drafted in-house.
Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.



Significantly, 40% of the organisations do not know the financial cost of the losses caused by the incidents, whereas almost 40% put the losses from a five-day business interruption at over one USD million.

In addition to defining «Operational Risk» as:

The risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events.

Measurement of this Operational Risk is part of the calculation of the Solvency Capital Requirement (SCR).

Main factors for developing a Business Continuity Plan

When it comes to making a decision to develop a BCP, be it to meet legal requirements or because a company believes it to be necessary, the following factors should be considered:

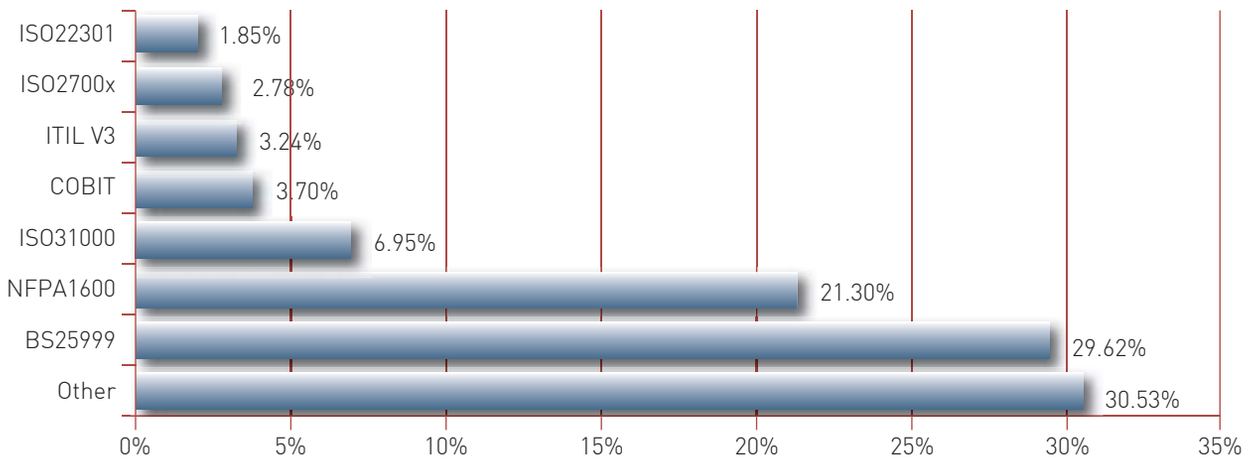
- **Ensure the commitment of one of the company's senior managers**: Having a project sponsor that has sufficient influence in the company to ensure the backing of all of the units involved.

- **Scope of the plan to be developed**: Clearly identify which areas of the company are to be analysed, and which physical locations will be considered.

- **Resources to be allocated to the project**: These may be human resources from the same company, who are to be dedicated almost exclusively to the project development and/or financial resources for the project to be elaborated. This may also be performed by a specialised company; however the company's employees must always dedicate a percentage of their time to providing information and validating results.

- **Business continuity becomes just one more process within the company**: After the project ends, in addition to implementing the solutions, the BCM plan must be updated regularly

What business continuity management standard do you apply in your insurance company?
Drafted in-house.
Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.

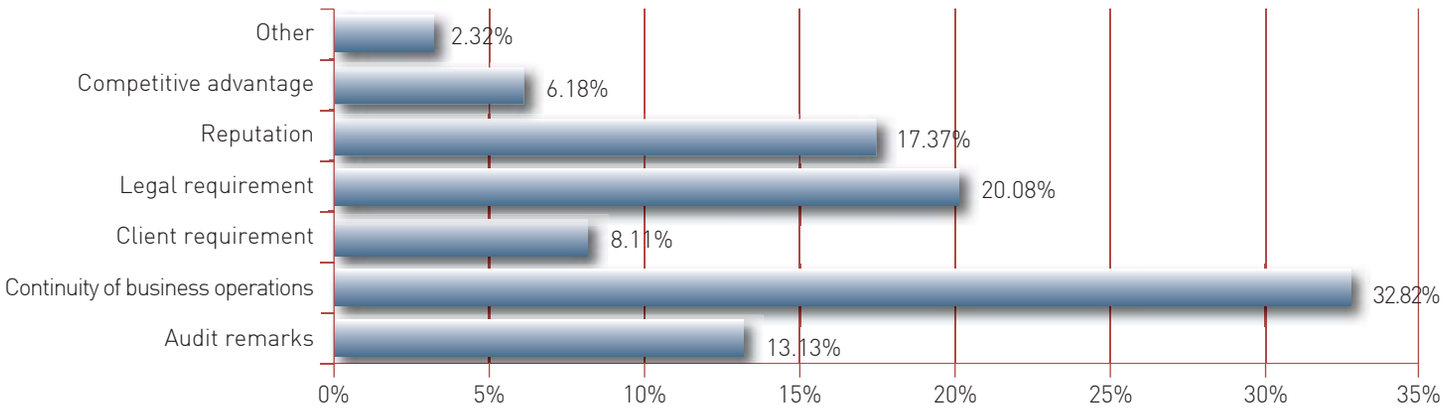


A third of companies base their business continuity management system on local standards in their own country or on non-specific business continuity standards (Others). The high proportion of companies applying standard NFPA1600 is mainly due to the fact that most of the companies participating in this study are located in the US. Only a low percentage of companies use ISO22301, which replaces BS25999, because at the time the study was performed it was still in draft stage (published in May 2012). It is also noteworthy that almost 7% of the companies base their business continuity management system on standards mainly related to technology (ITIL, COBIT).

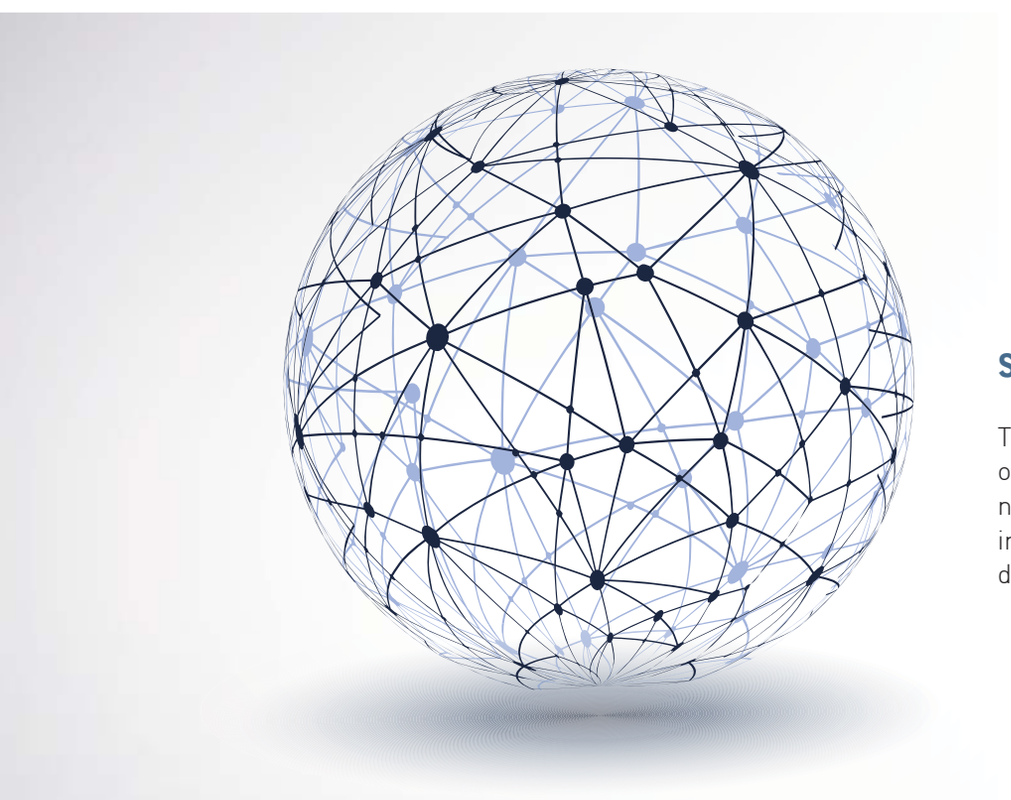
What are the main reasons for implementing a Business Continuity Management System in your insurance company?

Drafted in-house.

Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.



One in three insurance companies has developed a BCP (or is in the process of developing one), mainly to maintain the continuity of their operations, whereas one in five does so to meet legal requirements.



and whenever there are important changes in the company. The new process must be allocated enough managers and resources for its development and to handle the design, preparation and performance of tests that guarantee the suitability of the solutions implemented, as well as the training of personnel.

Stages of development of the BCP

The purpose of a BCP is to enable an organisation to react effectively and return to normal following a disaster-related business interruption. The ISO 22301 standard formally defines a Business Continuity Plan as:

> ***Set of documented procedures that provide guidance to organisations for responding, recovering, resuming and restoring, after an interruption, to a predefined level of operation. This usually covers the resources, services and activities required to guarantee the continuity of the critical operations of the business.***

In an insurance company, developing a BCP includes four phases, as described below:

1. Analysis of the risks in the event of unavailability

To complete a BCP in an insurance company, five elements must be investigated:

- People.
- Buildings/infrastructures.
- Information.
- Technology.
- Suppliers.

The risk of unavailability of each of these elements must be analysed, and probabilities must be assigned to each of the threats. This enables the company to ascertain which additional measures it needs to take to detect or reduce the consequences of a given scenario; it also acts as a decision tool for prioritising recovery strategies. The difficulties associated with this phase are similar to those encountered in any risk analysis, and include:

- Having a log of incidents that have affected the company.
- Access to the necessary information.

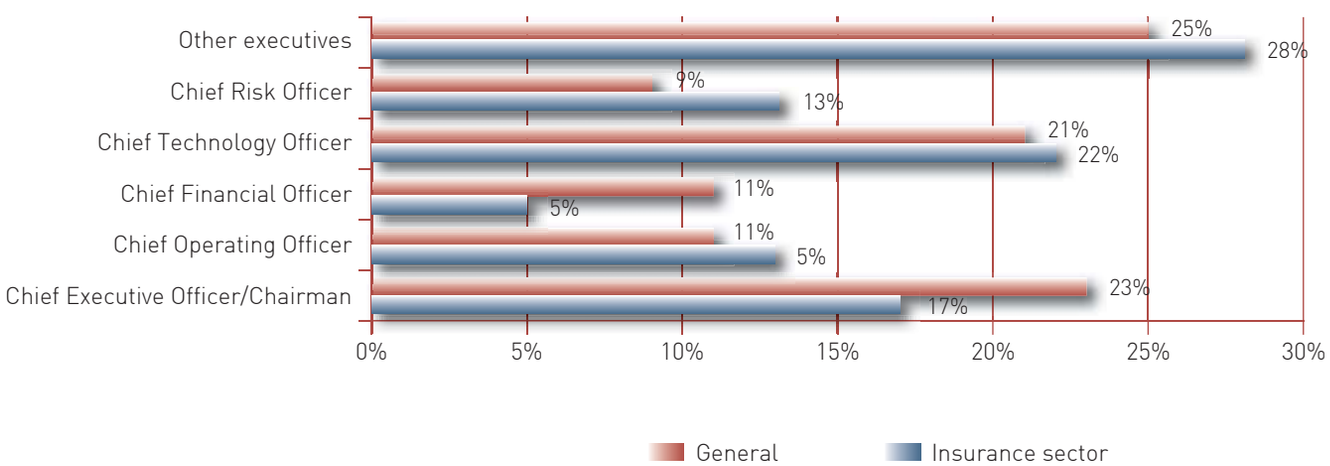
2. Business Impact Assessment

A Business Impact Assessment analyses the effect of not performing a set of business continuity processes, listing and sorting them according to criticality and recovery time post-disaster.

This is the most important step when defining a Business Continuity Plan, as the rest of works to be performed will be based on the results obtained in this stage.

The purpose of a BCP is to enable an organisation to react effectively and return to normal following a disaster-related business interruption

Who is the main person in charge of developing the business continuity management systems?
Drafted in-house.
Sources: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG and Business Continuity Preparedness Survey, Q4 2011. Forrester/Disaster recovery Journal.



The graph does not show significant differences between the results obtained from the insurance sector and those from other business sectors. It is worth noting how influential the Chief Technology Officer is in implementing a business continuity management system.

The main difficulties of the Business Impact Assessment are:

- **The need for those in charge of the processes to be involved in order to determine the impacts**. Providing information for the analysis to be performed effectively requires time which, if added to day-to-day tasks, entails an additional effort.

- **To reduce the subjectivity of each person in charge in determining the impact of the processes**. In order to avoid the results being tainted by those who consider themselves indispensable to the company or those who consider that their work provides little value, educational talks or workshops may be held to explain the purpose and/or gather information in an indirect manner. The latter technique requires work beforehand, i.e. formulating the right questions, deciding which response criteria are to be used, weighting the questions and deciding which mathematical process should be used for the final calculation. Furthermore, the results obtained must be reviewed with senior executives, as they have a global view which enables them to detect inconsistencies in the classification of the processes for which they are responsible.

- **Assess the criticality of activities**. Given the in-depth analysis performed, employees in charge may see the analysis as an attempt to evaluate the relative importance of their activity to the company. This is an important aspect that must be clarified, especially given the current financial climate. It is essential to emphasise that the goal is to measure the criticality of each activity in the event that the company is affected by a disaster, not the importance of the activity *per se*. All of the activities carried out in a company are important, but if it is affected by a disaster, the company must prioritise

Given the in-depth analysis performed, employees in charge may see the analysis as an attempt to evaluate the relative importance of their activity to the company. This is an important aspect that must be clarified, especially given the current financial climate

Number of FTE (Full-Time Equivalent) employees dedicated to Business Continuity Management in insurance companies.
Drafted in-house.
Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.

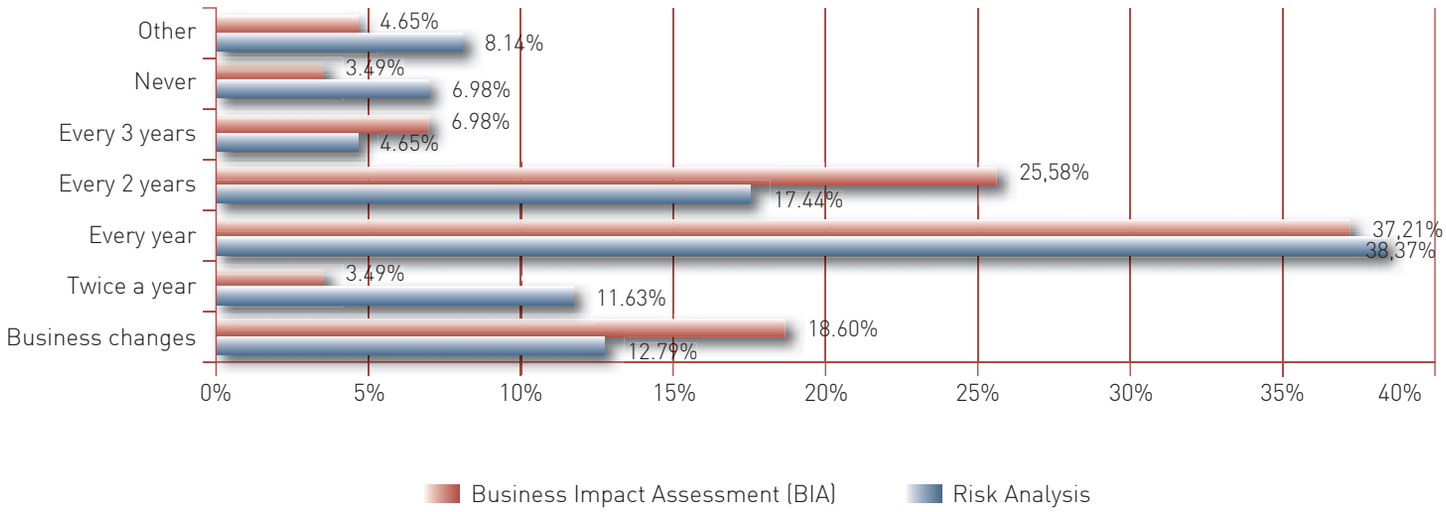
FTE number	0/2	3/5	6/9	10/20	+20
Corporate level	22.89%	7.63%	3.21%	1.61%	0.40%
Business units	15.26%	4.82%	2.41%	2.81%	5.62%
Information technology	16.47%	8.43%	2.41%	3.61%	2.41%

A key component of Crisis Management is the ability to communicate the situation and its evolution to both internal and external stakeholders

the recovery of some over others. Initially, it must focus its efforts on resuming those activities without which the company would be harmed (higher level of criticality); only then will it move on to the next level and so on until all of the activities have been re-established or all of the available resources have been used.

- **Determine which processes must be analysed**. It is recommendable to analyse all of a company's processes so as not to issue any ill-considered judgements on their criticality, without formal analysis; doing so runs the risk of excluding certain processes which may later turn out to be highly critical. The scope of process analysis may be organised by breaking them down into different stages and proceeding until all have been worked through. For example, we could begin by contemplating all of the processes in a single area of the company, before expanding the scope to others in other areas until the company's process map has been fully evaluated. This approximation of analysis may entail additional work, as new results may have to be consolidated with those from previous stages (principally affects processes that cut across multiple areas). Nonetheless, in large companies this could be the best approach towards a complete analysis. This «divide and conquer» strategy attempts to optimise BCP despite the large number of processes to be analysed and the finite resources available.

How often is Risk Analysis performed in your insurance company? And the Business Impact Assessment?
Drafted in-house.
Source: 2011-2012 Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.



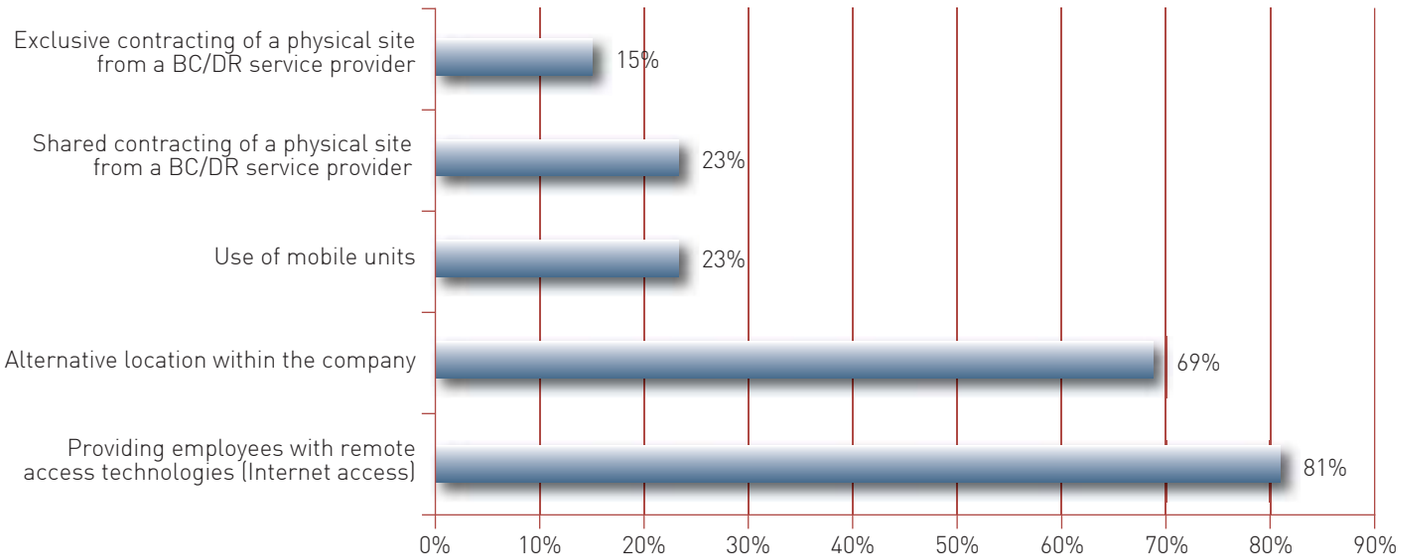
Half of the insurance companies surveyed said they reviewed the results of their risk analysis in the course of the year following the last analysis; 11.63% said they reviewed their results sooner. In the case of the business impact assessment, 40% of the companies said they reviewed their results in the course of the year following the last analysis; 3.49% said they did so sooner. It is important to note that relatively few companies perform reviews when there have been changes in the company.

- **Study of the dependency between processes**. This aspect relates to the above item and it studies the possible dependency between processes. If, for example, process A receives a certain criticality value, the processes on which it depends must have a higher criticality value, so that when process A is resumed, the processes that it requires for its operation have been re-established beforehand.

- **Determine the level of depth to be analysed**. Companies may have compiled a map of processes at different levels (processes, sub-processes, activities, tasks), or if they do not have them, the analysis may be performed on the basis of organisational structure (directorates, areas, departments, management). In either case, the depth of analysis must be determined, so that the results are homogenous. It is also important to avoid being overly generic, as this may set in motion a search for solutions that involves many resources, but fails to specify their object. Likewise, it is necessary not to go into excessive details; while precision in terms of resources to be used, etc may be useful in some ways, if a disaster strikes, proposed solutions must be sufficiently flexible to respond to the scenario at hand.

- **Determine the thresholds of the criticality values and their correspondence with the Recovery Time Objective (RTO)**. The RTO is measured from the time when the incident is detected to the re-establishment of the activity. This time must be determined for each of the processes and will depend on the criticality of the process analysed. We must bear in mind that usually the lower the RTO required by the processes, the higher the financial investment and/or effort required in the preparation of the procedures to reactivate the activity, as there is less time for reaction.

What Business Continuity solutions do you apply in your company?
Source: Business Continuity Preparedness Survey, Q4 2011. Forrester/Disaster recovery Journal.



The solutions shown in the graph mainly relate to a disaster scenario that has affected a company's buildings, requiring that employees be relocated or given remote access to computer systems; the latter is the most frequently implemented solution. (BD/DR: Business Continuity and Disaster Recovery).

3. Selection and design of solutions for recovering the activity

Having analysed the impacts of not performing the processes when the company is struck by a disaster and having determined the time in which the activities should be reinstated, solutions must be designed that would enable business requirements to be met while minimising recovery time and resources usage. These solutions will be defined depending on the unavailability scenarios of the elements required to perform the processes.

The main difficulties during this stage are:

- **Determining the minimum degree of service that must be provided**. The solutions that are specified for the disaster scenario must consider the minimum essential resources required to perform the activities.

- **Estimating the cost of developing the solutions**. This is a crucial factor for decision making, especially when there are several alternatives. We must identify the parameters that have a bearing on the cost of the proposals and apply them to the resources that will be required to resume the activity.

- **The company senior management must approve the BCP and costs**. Derived from the above, developing the proposed solutions may exceed the competences of the business continuity unit; the process may thus require the approval of senior management, and other departments involved in implementation may need to be notified.

In addition to selecting and implementing the solutions, the procedures for Crisis Management must be specified, as well as the operations for reinstating affected activities. A key component of Crisis Management is the ability to communicate the situation and its evolution to both internal and external stakeholders.

4. Performing tests

In order to determine whether the company is ready to face a disaster, exercises must be performed that will enable business continuity staff to:

- Verify that the solutions implemented and the procedures developed are suitable and sufficient to meet the business requirements.
- Identify aspects to be reviewed or improved.

Tests may be performed in stages depending on how mature the solutions/implementation procedures are. To begin with «desk tests» may be performed in order to verify that all of the tasks to be performed -as well as their interfaces- are shown. A «simulation» is then organised in which the procedures and solutions are tested operationally. A company can only confirm that it has a BCP if it has performed tests and the results are considered satisfactory.

Conclusion

The BCP must fall within the framework of a Business Continuity Management system that allows for ongoing development, monitoring, review, maintenance and improvement; this includes defining an organisational structure and associated responsibilities, drafting policies, assigning resources and planning activities to be performed.

Once these plans are in place, business continuity simply becomes one more process for the company. Notwithstanding this, it is crucial that these procedures are properly managed and kept up to date so that the company is optimally prepared should a (worst-case) scenario occur.