



# Averting Disaster

## - Business Continuity Management

**B**usiness is often never a straight, smooth road. Even the biggest giants of the world face potential disruptions that could come from a variety of sources. Some events when they happen might be so debilitating that huge corporations can face a real danger of collapse. If these companies with huge infrastructure and resources are potentially vulnerable to forces beyond their control - smaller companies – such as the SMEs would be ill-equipped to handle a situation like this.

A good example is when severe flooding occurred in 2011 in Thailand, a major global hub for the manufacture of motor vehicle components. Leading motor vehicle manufacturers such as Toyota and Honda, whose assembly plants in countries such as Malaysia as well as in Japan relied on their supply of components from plants in Thailand, had to slow down production or shut down as they could not assemble the vehicles due to supply disruption.

Organised companies or organisations will have a plan to deal with the most severe of crises. The solution is implementing Business Continuity Management (BCM). A recognised benchmark of good practice in BCM is specified in the International Standard ISO 22301:2012, Societal security – Business Continuity Management Systems – Requirements.

Parama Iswara, Senior General Manager of Management System Certification Department, SIRIM QAS International Sdn Bhd, the management system certification arm of SIRIM, explained that Business Continuity Management (BCM) is a holistic business management process that identifies potential threats to an organisation and the impact to the business if those threats are realised.

BCM also provides a framework for the organisation to establish its resilience and capability for an effective response that safeguards the interests of its stakeholders, its brand, its reputation and its value creation - ensuring that the organisation effectively responds to any situation that could potentially disrupt its normal operations. The organisation is required to look at ways of mitigating the effects of potential threats or the likelihood of certain occurrences by having a response in place such that it is able to return to an acceptable level of performance within a specified time frame. This Recovery Time Objective has to be less than the Maximum Tolerable Period of Disruption (MTPD) or the longest time frame the company allows for the return to almost normal performance.

## Good for All

Companies big or small should have this solution in place as an assurance of the continued longevity of their businesses. BCM is especially important in organisations where disruptions to business will have the biggest impact to their customers or stakeholders.

This is especially so in industries such as power and water utilities and telecommunication companies – where any stoppage could have great impact on the economy of a nation as well. At the moment however, there is very little in the form of legislation relating to business continuity and those adopting these practices are doing so on a voluntary basis.

Initially, business continuity was limited to disaster recovery plans tailored specifically for the IT industry. Now it is recognised that this discipline is needed well beyond that industry. For instance in IT, they have ISMS or Information Security Management System which deals with the confidentiality, integrity and availability of information or data. So, in fact within the IT industry, they are already practising some form of BCMS as the loss of data can cause business disruption in their case. Their strategies for this would be for example, backing up their data in remote sites or other places - and usually there was no need to physically relocate the business.

“

Initially, there were disaster recovery plans but tailored specifically for the IT industry. Now it is recognised and goes well beyond that industry. For instance in IT, they have ISMS or Information Security Management System which deals with the confidentiality, integrity and availability of information or data.

”

*Parama Iswara  
Senior General Manager  
Management System  
Certification Department,  
SIRIM QAS International Sdn Bhd*



## Dealing with Danger

There are various ways that companies deal with disruptive events. Those facing physical threats to their business may relocate their facilities or staff to remote sites; or they may relocate their operations to third party sites. Then there are those who go to the extent of maintaining duplicate sites with facilities that can continue performing daily business (albeit not at its maximum level) when the threatening event is ongoing. This type of manoeuvre can be costly – but at the end of the day, it ultimately depends on the company's BCM strategy.

All crucial factors have to be weighed before embarking on a plan. The organisation has to look at the cost of not recovering a business within a specified timeframe against the cost of maintaining such a site.

*And how does a company decide on its strategy?* Parama says that it a step-by-step process. Firstly, the organisation will carry out a Business Impact Analysis where they will look at its critical business operations and the impact of any disruption to it (meaning there is a failure in its ability to deliver products/services). Subsequently, the organisation will decide on its permissible recovery time post event.

This is then followed by risk assessment - this involves identifying and quantifying the risk, i.e. the likelihood and consequences of a particular disruption to any of its prioritised activities, and deliberating over which action to take (i.e. weighing the impact of not recovering against the cost of executing the plan).

## Identify the Threat and Deal with it

The scenarios they identify would be the possible events they want to address - those that would affect the normal running of the business or the ones that are the least tolerable to the continuity of the business or the everyday running or performance of the business. As part of the Business Impact Analysis and Risk Assessment process, the organisation would look at the impact of severe disruptions to the business, identify risks of disruption to prioritised activities and evaluate which disruption related risks require to be acted upon. Because the BCM standard requires the organisations to document their business continuity strategy and plans - they would already have identified the possible scenarios through the rigorous methodology.

Incidents may happen at any time. However the most important thing that must be decided is whether the incident has reached a level that requires a response. The organisation will have to decide at which point where an event will be deemed a crisis and start to invoke the necessary actions. These will clearly be specified in the organisation's business continuity plans and related procedures. These are elaborate plans which describe what is expected to be done in the event of an occurrence. There could be different business continuity plans to address various scenarios.





*Car manufacturing plant in Thailand was disrupted with the floods that occurred there. The car plants that were relying on their supply in the region had to shut down as they couldn't supply the cars for lack of the parts.*

## Seriously, No Jesting

The recovery activities are taken very seriously as it can determine the future of the company. The organisation should have an incident response structure in place - with a dedicated team of people with clearly defined responsibilities ready to act in the event of disruptions.

## Peace of Mind to the People

In implementing BCM, organisations are also required to give due consideration to internal and external communication relevant to the BCM system. Commenting on communicating to the external parties, Parama explained that this gives an assurance to the customers and other stakeholders that the organisation concerned has a recovery system in place and that they will at the very least minimise the impact of a disruption to their business. This is prior to any incident occurring. When an incident actually occurs, the organisation is expected to communicate internally with employees and other interested parties and externally with customers, partner entities, local community, the media and appropriate authorities in accordance with the provisions of its Business Continuity Plan and related procedures.

As a parting note, Parama would like to see more organisations taking up BCM as it would be very beneficial for the long-term sustainability of their businesses. Obtaining third-party certification to ISO 22301 from certification bodies such as SIRIM QAS International will bring the added benefit of providing confidence to customers and other stakeholders that they are dealing with organisations which are well prepared for any potential disruption.

## Testing for Preparedness

If an event doesn't occur, the organisation will not know if the plans that have been established are workable or not. This is where exercising and testing is important. One of the requirements for effective implementation of BCM in accordance with ISO 22301 is for the organisation to regularly exercise and test its business continuity plan and procedures.

Organisations are encouraged to carry out simulations of scenarios as close as possible to the real event. It is up to the organisation to identify the scenarios and to carry out the exercise and testing to relate to the scenarios that they are expecting and very importantly, learning and improving from the results of the exercises so that when an incident actually occurs, they will be better prepared.

At the end of exercising and testing, the BCM standard requires the organisation to come up with a detailed report of the exercise. Hence, regardless of whether the plan works or not, the organisation will have to conduct a post mortem and decide on any improvements to the plan. Quite often there needs to be a tweaking of the plans as it is not possible to simulate or prepare for every possible scenario.

The teams involved should be stretched to the limits as much as possible in a simulation of an event to ensure that they perform their duties as best as possible. There are some organisations that do not give prior warning before the commencement of an exercise.