

The Business Case for BCM

Case Studies

Foreword by Lyndon Bird FBCI



Table of Contents

Foreword by Lyndon Bird FBCI	Page 3
Case Study 1: Terrorist attack on Glasgow airport	Page 4
Case Study 2: BCM in residential care homes	Page 5-6
Case Study 3: Continuity in a difficult environment	Page 7
Case Study 4: BCM in an outsourcing services company	Page 8-9
Case Study 5: Reducing factory downtime with BCM	Page 10
Case Study 6: Earthquake in Japan	Page 11
Case Study 7: Inui Steamship and BS25999-2	Page 11
Case Study 8: Integrating BCM with IT Service Management	Page 12
Case Study 9: The benefits of exercising	Page 13
About the BCI	Page 14
Contacting the BCI	Page 14

Foreword

“Where’s the beef?” is a popular rhetorical phrase and there have been a fair number of management methods that have come and gone over the last twenty years, however, I’m pleased to say that Business Continuity Management is not one of them.

While the published report on the business case for BCM demonstrates that tangible benefits are being enjoyed by many organizations, the case studies in this document provide greater insight into how individual companies are applying BCM.

The case studies cover a wide range of issues but the most obvious observation is the international adoption of BCM practice: Contributors come from the UK, Pakistan, Switzerland, Japan and Saudi Arabia.

The case study around the terrorist attack on the UK’s Glasgow airport in 2007 is remarkable in terms of getting back to business in less than 24 hours; the application of BCM thinking to residential care homes shows that it is not just commercial organizations that can benefit from BCM; and the submission from Pakistan shows how BCM works in know difficult environments; the contribution from

B-Source picks on a very important topic of supply chain resilience; and the case study from a telecoms manufacturer shows how substantial revenue streams can be protected through BCM. We also received three case studies from organizations in Japan dealing with complex issues around recovery after earthquakes, integrating BCM with other disciplines and improving business resilience through certification. Finally, it can never be over stressed that a plan is no good if it hasn’t been tested and the assumptions validated and the contribution from Arab National Bank completes a fascinating collection of case studies.

In closing, I would like to thank the contributors for their efforts in documenting their successes for the benefit of the wider BCM community and would take this opportunity to encourage others to share their knowledge and experience in the future.



Lyndon Bird FBCI

Technical & International Director
Business Continuity Institute

Contributors

Any views or opinions expressed are those of the contributors and not of the BCI.

- Abdulrahman Alonaizan MBCI, Arab National Bank
- Colin Ive MBCI, CoDRIM
- Gillies Crichton AMBCI, BAA Glasgow Airport
- Hideo Nakamura AMBCI, NTT Facilities, Inc.
- Kuniyuki Tashiro MBCI, InterRisk Research Institute & Consulting, Inc.
- Lesley Pretlove, Suffolk Joint Emergency Planning Unit
- Patrick Burki, B-Source SA
- Salman Tariq, Telenor Pakistan

Terrorist Attack on Glasgow Airport

*Gillies Crichton AMBCI
Head of Assurance
BAA Glasgow Airport*

At 15:11 hours on Saturday 30 June 2007 (the second busiest day of the year), a Jeep Cherokee 4x4 vehicle was deliberately driven into the main terminal building at Glasgow Airport and set alight.

A well rehearsed emergency plan was put in place to evacuate the building and deal with the fire. It was established quite quickly that this was in fact a terrorist attack and the perpetrators were arrested at the scene.

The Airport integrated emergency plans include a support mechanism whereby off duty persons were called in to support the front line staff. This is in the form of a Crisis Management Team who look after the tactical command and a Business Recovery Team who look after the strategic command on behalf of the Airport. The crisis team was initiated and operational within 45 minutes with a business recovery team operational an hour later.

No single Business Recovery plan exists for this type of incident as the entire incident is complex with a large number of stakeholders involved. We do however, have plans based on cause & effect and these main plans were utilised including short term loss of the terminal building and loss of road infrastructure. The latter was of particular use as traffic was initially banned from the forecourt area of the Airport.

In total, around 3,500 passengers were evacuated to the Scottish Exhibition & Conference Centre (SECC) to allow the Police to interview them as potential witnesses.

Our holistic strategy is based around “7 R’s”.

1. Risk
2. Resilience
3. Rehearse
4. Response
5. Recovery
6. Review
7. Reputation

Our BCM strategy served us well on the day of the

incident as we knew our business end to end processes; we had analysed what can go wrong and how; we had plans in place, we had tested, rehearsed and fine tuned them. This enabled us to protect our reputation by showing the world how effective our plans were as we reopened the terminal building in 23 hours 59 minutes after the attack.

This was a high profile event for Glasgow Airport in particular and the aviation industry in the UK in general. This was more challenging as it happened during our busiest period of the year. Through having robust BC plans in place, we were able to deal effectively with the incident and return the airport to normality in a staggeringly short period of time.

I cannot over emphasise the benefit of robust, workable plans with a team dedicated to dealing with the crisis and a separate team dedicated to restoring normality as quickly as possible. These plans are only effective if they are tested regularly and all members of the responding teams fully participate in these tests. This was from the Managing Director downwards.

Our airport suffered what could have been a catastrophic event, was it just good luck? From identification of our risks and subsequent mitigation of the risks, the plans in place and most importantly, well trained and competent staff, we were able to demonstrate that Business Continuity Management is an essential part of our ongoing lives.....the unthinkable can and does happen, you need to be prepared for it.

The recovery was recognised at the Business Continuity Awards in May 2008, winning the “Business Continuity Recovery of the Year”.

BCM in residential care homes

*Lesley Fayers
Business Continuity Officer
Suffolk Joint Emergency Planning Unit*

Executive summary

Suffolk County Council (SCC) installed external generator access points to their sixteen residential care homes for older people after the Business Impact Analysis (BIA) exercise highlighted loss of electricity as a key threat to this critical service. Just two weeks after testing the plan for loss of electricity, they had a real power outage at one of the homes. As a result of the updated plans and greater staff awareness there was a quicker response, swifter connection to temporary power and reduced impact on the elderly residents.

Background

SCC Adult and Community Services (ACS) run sixteen homes for elderly people across the county. Any threat to residents' health or wellbeing needs to be addressed promptly due to the frail and vulnerable nature of this group of people. The BIA for ACS had highlighted the threat of loss of electricity as being a high likelihood and high impact event. This was based on historic evidence of power failures at several of the homes, sometimes lasting for many hours at a time. A generator solution had been applied in the past, but without the connection box, it had taken several hours to connect and was not powerful enough to heat and light the whole home. There was also a disconnect between the ACS Directorate Business Continuity Plan (BCP) and the emergency procedures held at each home leaving the managers feeling isolated and unaware of how they could call for additional support.

Clearly it seemed sensible to focus attention on this threat to this service: The ACS Head of Risk worked on making a case to install generator connection points at each site; Inviron, the council's supplier of electrical services, calculated the power consumption each home used; and the Business Continuity Team worked with the home managers to produce consistent Incident Management Plans (IMP) which would dovetail with the ACS Directorate BCP.

Challenge

Although it was easy to make a good business case to install generator supply points, funding still had to be secured. Consideration was given to purchasing a generator, but it was deemed more cost effective to let Inviron supply one as and when required. This was built into the existing working arrangements. Once the funding was agreed it took a year to complete the work due to the complex involvement of the energy supply companies that stretched across the globe. To book an appointment for an engineer to disconnect and reconnect the power supply at each home involved contacting the Oxford office of British Gas with the appointment request, who then contacted their Cardiff office to raise a job quote. Once the fee was paid an appointment was requested via Siemens in Leeds which was in turn booked by Siemens in India before it was passed back through the chain.

To ease the process the County Council energy buyer contacted Siemens directly to arrange the appointments, saving cost and reducing time. Bypassing the care homes' energy supplier became necessary to achieve the appointments in a timely manner. Inviron and the County Council worked closely together to achieve the complicated process

The Exercise

Once the work was nearing completion, a two-part exercise was planned at one of the homes. First the home managers held a desktop exercise to test their loss of electricity plan. This was followed by a live switch over to generator power led by the County Council's property manager and the Inviron manager to test the new connection and load capacity.

Both elements of the exercise went well. All the staff at the home took an enthusiastic part making sure at all times that there was no impact on the residents, most of whom suffered from dementia. The switch over from grid to generator was seamless and tests conducted whilst on generator power proved that it was capable of providing all the electricity supply to the two-storey home, including the lift, kitchen and laundry equipment and heating.

Improvements gleaned from the exercise were fed back into to the IMP of all sixteen homes.

Cont

Live event

Two weeks after the exercise, a power cut was experienced at a home in the west of the county. The manager lost no time in putting the new procedures in motion which meant managers were alerted, the generator dispatched and temporary power to the home was restored within a couple of hours. The generator remained on site until the next day when the home was reconnected to the grid. Residents remained unaware of the problem.

Benefits

All sixteen care home managers are confident that they have good and consistent plans that have proved to work well through test and live event. They know they have the right processes in place to summon the necessary help when needed and the supply chain is robust and dependable. The benefits have been achieved by working through the BCM process to highlight the risk, implement a solution, write a plan, test it and make staff aware.

Under the UK Civil Contingencies Act, Local Authorities have a duty to promote business continuity within the private and voluntary sector. The Business Continuity team from the Suffolk Joint Emergency Planning Unit have subsequently run Incident Management training events with ACS to private residential care homes across Suffolk. The response has been very good.

Continuity in a difficult environment

*Salman Tariq
Director, Corporate Security
Telenor Pakistan*

Telenor Pakistan is a subsidiary of Telenor ASA, Norway, the world's sixth largest cellular mobile operator. Commencing Pakistan operations in 2005, the company achieved exponential growth and is now one of the largest organizations in Pakistan.

Telenor's Pakistan head office is located in Islamabad. Due to quick growth, the company had to lease more buildings in a city where there was a severe shortage of suitable office space. This led to choosing less than ideal premises in terms of physical security measures.

One such leased office was a building called Sardar Arcade located in the central business district of Islamabad. Though commercially the building was located in a good location, it was near some very sensitive installations and organizations with notorious reputations. This building housed the company's IT function and at that time the technical division as well. These two functions comprised about 250 staff at any one time.

In the middle of 2007, a militant group of religious fundamentalists occupied two buildings in Islamabad, one of them called the Lal Masjid (Red Mosque) and the other, a neighbouring children's library. This led to a confrontation between the Government and these rebels, which continued for a period of more than six months.

The culmination of this event was the raid by a military commando unit, which itself lasted about three days. There was a severe exchange of firing between the two groups, with many deaths. During this exchange of shooting some stray bullets hit Telenor's office building, Sardar Arcade, which was located almost one kilometre away from this incident. One stray bullet also ricocheted off a wall and hit a member of staff in the leg.

This caused immense alarm amongst all staff and the Crisis Team immediately got in to action.

Telenor had a very good response unit in place. Due to the prevailing situation in the country, there

was already built-in resilience in the organization and a culture of awareness and camaraderie. Therefore, when this situation arose, the company made the following decisions very quickly:

- This building would be closed down temporarily until the fighting stopped and complete peace and safety returned to the area.
- For business continuity and to make sure these departments continued to function, a large hall room was booked at a leading hotel in the city. This room was converted within 24 hours to look just like our office in terms of wireless connectivity, printers and copiers, down to the tea/coffee stations.
- Support staff were placed with this group to provide anything they may want to make their time as productive and normal as possible.
- A trauma counsellor was put in place.
- Internal communication channels were established for staff to call with any enquiry 24/7.

Due to the above steps taken, **not a single day of work was lost for the affected staff**. An SMS was sent to all relevant staff informing them one day before that on the next day they would report to the hotel; movement to the office area was restricted to business critical activities only.

The hotel room was used as their office for five days in the month of July, 2007.

After this experience, the importance of business continuity measures and building resilience in organizations became very apparent. It is also critical to include this in the culture of the organization, so there is buy in, not only from the top but also in lower echelons of the organization. It is also key to have an effective communication system so real time updates can be given to the maximum number of people.

BCM in an outsourcing services company

Patrick Burki

Head of Risk Management Services

B-Source SA

Executive summary

In response to the recent pandemic threat, B-Source SA undertook a review and risk/compliance analysis of its business continuity management (BCM) readiness including that of its stakeholders and own suppliers. As an international multi-outsourcing service provider that is dependent on a variety of sub-contractors and vendors this proved to be a challenging exercise. The business continuity planning team not only had to consider the company's own employees and processes but also those of their supply chain.

A widespread use of a standard benchmark like the BS25999 would have helped immensely in evaluating the state of readiness of our suppliers and subcontractors. As a direct result of the review, plans have been made to enhance and improve communication around BCM involving all staff.

B-Source SA

B-Source provides bank back office and IT services to insurance and private banks in Switzerland and selected other countries.

Being a service provider for the financial industry in Switzerland B-Source does not require a specific authorization, as the financial supervisory body considers that the clients remain fully responsible for the outsourced activities, "as it would operate themselves".

Therefore, one of the challenges for a multi-outsourcer is to have best practice internal controls, risk management, security and a business continuity framework in place. It is therefore very important to be able to communicate at all levels (international regulators, boards of directors, auditors, other stakeholders) with a common global language/framework.

The challenges and advantages of business continuity with a multi-outsourcing company

A Business Process (BPO) and IT Operations (ITO) outsourcer for different customers demands

efficient and standardized processes based on widely recognized frameworks. This is especially true for the financial industry, where internal control, risk management and compliance must be formally and extensively implemented and audited.

A service provider such as B-Source is obliged to communicate regularly on the adequacy and efficiency of its internal control activities. Nowadays most of the service providers have adopted the Statement on Auditing Standard (SAS) 70 reports, so that communication on the controls performed can be officially audited and communicated to a large audience of stakeholders, including clients.

However, as plans are not controls, a Business Continuity Plan (BCP) is not part of the description of controls performed, but, in a SAS 70 report, is part of the general information provided by the service provider. In this sense, a BCP is therefore not officially audited, only communicated.

From a business continuity point of view, the outsourcing of some or all business processes and IT Operations can bring advantages such as:

- Clearly defined outsourced processes, based on a recognized frameworks, like CoBiT or ITIL, allowing the implementation of recognized control objectives, benchmarking and the measurement of them (maturity analysis)
- Contractual description of the services provided, formalized in a Service Level Agreement (SLA), with clear Key Performance Indicators, allowing and End-to-End business continuity description
- Clear cost allocation to specific processes, thus allowing the service provider to offer differentiated levels of business continuity services
- Access to a community of banks or enterprises, sharing experience in terms of compliance, reporting and testing

Nevertheless, a service provider can face several BCM challenges such as:

- Avoiding/managing expectation gaps with its clients by clearly defining the level of business continuity services offered

Cont

- Regular testing of the level of business continuity services provided by B-Source's sub-contractors and continuous alignment and testing of these services with SLAs signed by clients
- Managing as efficiently as possible the "force majeure" disruption of services, this is particularly true for a full BPO and ITO service providers, as it could be difficult for the clients of service providers to contract another service provider at very short notice
- End-to-end business continuity plans between several outsourcers and the service provider, taking into account a possible priority of services to be delivered during a crisis

In order to reinforce the credibility of the BCM organization of a service provider or a sub-contractor, a recognized certification like the BS25999 provides a level of comfort to the outsourcer that its business continuity organization can meet a measurable standard, has been described in an internationally recognized way, meets a first class standards and can be benchmarked.

Key learnings, in particular in view of the H1N1 pandemic experience

The recent H1N1 pandemic provided us with the opportunity to adapt our crisis scenarios, in order to avoid disruption to services due to the physical non availability of a potentially great number of key people.

Following the publicity and the official announcements around this crisis, it was difficult to hide problems behind a contractual "force majeure" clause, as the unforeseen nature of event was not relevant anymore. From a reputation point of view anyway, it also could have been very damaging not to have been prepared for this pandemic.

Therefore the impact on the company of the loss of key people was reviewed and the most common mitigation measure implemented. Like in many other companies the solution was to provide remote access working places to ensure a certain level of business continuity for certain processes, at the same time avoiding contacts between staff. A staff sharing concept was implemented for the most critical processes.

As B-Source had to carry out the same analysis with many different sub-contractors, it was difficult to evaluate the level of readiness of these companies. Although all had already confirmed that they had a functioning BCP, it was difficult to have a quick and efficient evaluation of their level of preparation.

In this sense, a broad implementation of a recognized business continuity standard like BS25999 can allow clients of service providers to:

- Understand that there is a recognized standard in place which guarantees a certain level of readiness
- Improve BCP communication between all the service providers and the outsourcer, based on a common language

For the key sub-contractors or service providers, it could even be contractually requested, that the BS25999 certification be obtained and maintained.

Reducing factory downtime with BCM

*Colin Ive MBCI
Principal Consultant
CoDRIM*

In recent years this global telecommunications company introduced BCM across its IT infrastructure. As they did so there was particular emphasis placed upon their factories scattered around the world and as a direct result they were able to reduce factory downtime due to IT failures. So much so that they saved \$355M USD in potential lost production over period of 3.5 years.

The company had during the past two decades established factories across the world to meet the demand for mobile phones. A demand which has seen explosive growth since the opening up of markets and implementation of new infrastructure for mobile telecommunication networks across such places as China, India and Brazil. These factories are hugely impressive with state of the art manufacturing technology being employed to support the mass production of an ever developing range of products.

To underline the level of production these factories are capable of some can achieve a production level of 5 million units per week (by working 24 hours a day).

It is important to understand that once produced from the end of the assembly line these units do not then get taken off to be stored in a warehouse. In one of the best possible examples of 'Just in Time' manufacturing they are quickly out in the market place and moved on to the customers as soon as possible.

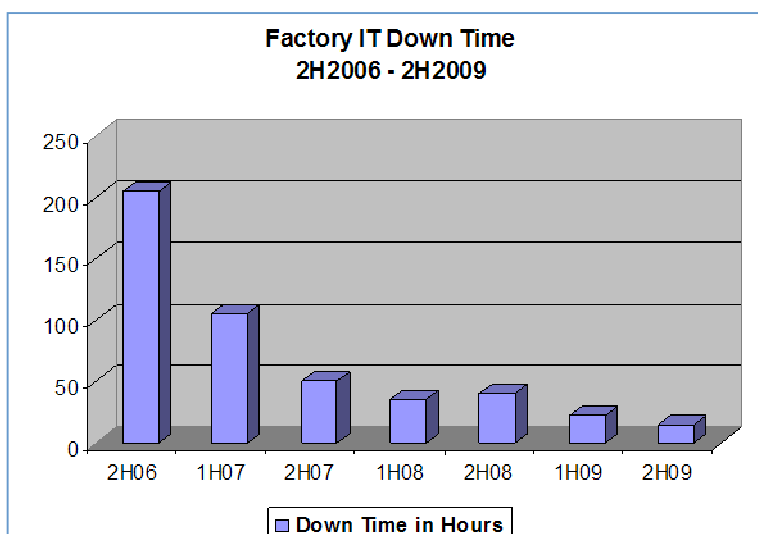
The use of state of the art manufacturing technology today means a very heavy reliance upon Information Technology and its associated infrastructure. As a consequence of it being so important to the life of the factory and in turn its efficiency, it is essential that the IT function operates to its maximum capability, i.e., 24 hours a day. Unfortunately in 2006 this was not happening. A series of problems resulted in the shutdown of

part or all of the production lines. A situation repeated across most factory sites.

In the second half of 2006 these losses had totalled 205 hours of lost production or, in financial terms, \$51.25M of lost revenue in 6 months (based on a figure of US\$6M per day). It was at this point that BCM was introduced in earnest. The solutions put in place were built closely around the BS25999 standard, although their implementation was complex involving as it did the many and differing cultures of those involved.

This was especially true with regard to the conducting of exercises, and by exercises it should be understood that this involved technical recovery etc and not just a table top 'chat'.

The work took several months to complete but it quickly became clear over the following year that the adopted measures had been highly effective in dramatically reducing lost hours and potential loss of revenue. This success can be seen in the figure below, which shows the total number of hours of



factory downtime from 2H2006 to 2H2009.

Based upon the predicted figure of US\$6M per day of lost revenue, a figure supplied by factory managers at the end of 2006. It is not difficult to deduce that had this loss of hours been permitted to continue to the end of 2009 it would have cost the company a total of US\$355M dollars of lost revenue. The estimated total costs during this time regarding the setting up of the BCM system, staff training and facilitation of exercises was around US\$1.8M. A good example of the value of BCM and the Return on Investment (RoI) it can deliver.

Earthquake of magnitude 6.8 in Japan

*Hideo Nakamura AMBCI
BCP Business Headquarters
NTT FACILITIES, INC.*

Background

NTT FACILITIES, INC., which is a subsidiary of Nippon Telegraph and Telephone Corporation, manages the maintenance of the power and building facilities for telecommunications. It establishes a business continuity plan for continued power supply, and conducts the annual exercise, assuming a large-scale earthquake.

Incident

On July 16, 2007, the Chuetsu Offshore Earthquake of magnitude 6.8 occurred in Niigata Prefecture. Due to this, about 900 buildings were damaged or collapsed, and more than 56,000 houses were blacked out.

Actions

Immediately after the earthquake, Disaster Countermeasures Headquarters was organized in the Tokyo Head Office to control the local prefecture branch and service center.

Since blackout occurred to six NTT buildings without engine generators, Disaster Countermeasures Headquarters determined the priority for preparing mobile engine generators, considering the battery backup time. Within 3 hours after the main shock, eight truck-mounted engine generators started to leave for the buildings, and supplied power.

While the commercial power supply to the buildings resumed after two days of the disaster, no failure of telecommunications services arose due to shutdown of power. This means that continuous power supply was achieved during a long-term power failure caused by a large-scale earthquake.

Inui Steamship & BS 25999-2

*Sarah Pottier
Bureau Veritas*

Inui Steamship was founded in 1904 and operates 23 vessels for the world wide transportation of grain, logs, cement, steel products and other bulk cargoes to/from Southeast Asia.

Inui Steamship had already put in place a safety management system in 1995 and had obtained ISO 14001 certification in 2006, but wished to further improve and extend their systems to efficiently manage other aspects of their business and demonstrate this through BS 25999-2 certification.

Inui Steamship first performed an in-depth risk analysis. They established a risk committee to examine all operations and identify any risks and made numerous improvements to their processes. To ensure business continuity, they set up a backup server that can be restarted remotely for the Kobe office.

Additionally, Inui Steamship reviewed their employees' assembly system and established corporate housing close to the head office and a contact system so that, even with a limited number of staff, smooth operations are ensured. As a result of these measures, a BCMS (Business Continuity Management System) was put into operation on August 1, 2008. Over the next 4 months the first and second audits were performed and certification was granted in December 2008.

Through the implementation of a BCMS, Inui Steamship has a better overview of all of their operations and can efficiently manage main business processes such as new client orders, planning its operational schedule, coordinating the contractors needed for loading and unloading at a port etc.

Establishing corporate housing close to their Head Office has the added benefit of being able to be used as a backup office, should the Head Office be damaged in a disaster. Inui Steamship is assured that their business operations are reliable and also more efficient.

BS 25999-2 certification further demonstrates the rigor of their systems and translates into client confidence.

Integrating IT service management and BCM

Kuniyuki Tashiro MBCI
Senior Consultant
InterRisk Research Institute & Consulting, Inc.

Company name: Open System Production Inc.

Business outline: Support service of implementing/operating IT system infrastructure and the related works.

Location: Tokyo, Japan

Employees: 45

Open System Production Inc. (OSP) has implemented four management systems and achieved certification as set out in the table below. The trigger to consider implementation of information security management system (ISMS) was the requirement from their customers. According to the president, the company was so small and internal management was immature at that time. Therefore they set their objective to obtain the framework and methodology for internal management by studying and working with ISO standard, not only to get certified. By setting the objective as above, they started their work to implement ISMS proactively.

When OSP decided to implement IT service management system (ITSMS), the trigger was not their customer. They started to study ITIL (IT Infrastructure Library) proactively for improvement of their internal management, and they got certified ISO/IEC 20000 as the result.

After that, OSP decided to implement BCMS. The main reason was the threat of pandemic flu. They recognized the impact of disruption caused by pandemic, and their customers also concerned about that.

OSP implemented ITSMS effectively by using the fruits of ISMS. The typical fruits of ISMS are: document architecture and control rules for ISMS documents, Plan-Do-Check-Act system, and education system for employees. These were helpful to implement ITSMS with very limited resources.

Furthermore, the fruits of ITSMS were also helpful to establish BCMS. In the process of implementing ITSMS, they analyzed service level agreements (SLA) between OSP and their customers. The conditions and levels of SLA vary among customers, so analysis was necessary to clarify their target for IT service in ITSMS. The result of the analysis was helpful to understand the requirements for their BCM.

The key players in implementing the BCMS were the sales manager, IT support manager, and BCM manager. During the business impact analysis (BIA) process they met frequently and shared the following information:

- Impact on customers of a disruption to OSP
- Customer requirements
- Readiness and resilience of their IT system

From these discussions, they developed their strategy on business continuity. Moreover, there were additional fruits from the discussion: The sales manager clearly understood the impact on their customers; the IT support manager clarified the resources needed for resumption/recovery in a short period of time. The process raised their awareness of business continuity thereby facilitating preventative actions against business interruption in each department.

Date of certification	Management system	Standards
2006.6	Information security management system (ISMS)	ISO/IEC 27001:2005
2007.9	IT service management system (ITSMS)	ISO/IEC 20000-1:2007
2008.11	Environment management system (EMS)	ISO 14001:2004
2009.11	Business continuity management system (BCMS)	BS 25999-2:2007

The benefits of exercising

*Abdulrahman Alonaizan MBCI
Arab National Bank (ANB)*

Regular testing is necessary to validate Business Continuity Plans. For each test that is conducted at ANB, the first thing is to determine the scenario under which the test is going to be performed. Then, for that scenario, the test objectives have to be defined. The flow of the test scripts follows these objectives.

The following is a sample of the objectives for the Business Units:

- Determining the integrity of recovered data at the Business Continuity Center (BCC)
- Ensuring that business operations can be performed efficiently from BCC as in a real disaster scenario
- Checking of transactions in BCC environment against production environment

The following is a sample of the objectives for Information Technology:

- Measuring the recovery time
- Validation of the Disaster Recovery Procedures for activating the services
- Verification of the network, hardware and application performance

Guidelines are prepared for the test as a whole, for both Business Units and Information Technology. In addition, Guidelines for the preparation of test scripts are also provided for the Business Units.

For each objective, the application for which the test is going to be performed has to be identified. The Business Units have to document specific test steps, expected results, actual results and the resultant status for the test step of the application. This is done for all test steps, for each application and each test objective. The test participants are expected to follow the scripts during the test and sign test reports verifying that tests have been completed as per the scripts. Where applicable, printout and logs of the tests are taken and included – as evidence – with the filled test scripts.

All test scripts are reviewed and approved by the Head of the Business Unit to ensure their completeness and adequacy for the test. Business

Units and BCM agree on the last date for submission of the completed test scripts for review prior to the test.

During the test, the scripts have to be followed and entries made in the actual results and the resultant status columns.

At the end of the test, the Business Continuity Team Leader has to do an evaluation of the test results. Questions like the following have to be answered:

- Could you access your business applications according to your test scripts?
- Does the performance of the systems meet business expectations?
If NO, please elaborate.
- Was all data recovered automatically?
- Did you have to post any missing transactions manually?
- If your answer is 'yes', how many such transactions had to be posted manually?
- Could you successfully do reconciliation of the recovered data?

At the end of the evaluation, the Business Continuity Team Leader has to decide the overall test result (Pass – Partially Pass – Fail). This has further got to be verified by his senior manager.

About BCM

Business Continuity Management (BCM) identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.

About the Business Continuity Institute

Based in Caversham, United Kingdom, the Business Continuity Institute (BCI) was established in 1994 to *promote the art and science of business continuity management* and to assist organizations in preparing for and surviving minor and large-scale man-made and natural disasters. The Institute enables members to obtain guidance and support from their fellow practitioners, as well as offers professional training and certification programmes to disseminate and validate the highest standards of competence and ethics. It has over 5,000 members in 90 countries active in an estimated 2,500 organizations in private, public and third sectors. For more information go to: www.thebci.org

The BCI Partnership, established in 2007, offers corporate membership of the BCI with over 70 member organizations including BAE Systems, BP, BSi Group, BT, Community Resilience, ContinuitySA, DNV, Continuity Shop, EADS, Garrison Continuity, HP, Link Associates, Lloyds Banking Group, Lockheed Martin, Marsh, Milton Keynes Council, Prudential, PwC, Royal Mail, SunGard, Vocalink, and Zurich. To join as a corporate member, go to: www.bcipartnership.com

Contacting the BCI

Lee Glendon, Head of Campaigns
The Business Continuity Institute
10-11 Southview Park, Marsack Street
Caversham, RG4 5AF
UNITED KINGDOM
Phone: +44 (0) 118 947 8215
Fax: +44 (0) 118 947 6237
E-mail: lee.glendon@thebci.org