Organizations have various ways of judging business success. In the public sector, one success criterion is quality of service to the citizens. In the private sector, growth of market share is a success measure. In all sectors, a condition for success is that business should continue to function in the face of fire, flood and other disasters. The discipline that ensures that the business can continue is business continuity management (BCM).1

In most organizations, the processes that deliver products and services depend on information and communication technology (ICT). Disruptions to ICT can, therefore, constitute a strategic risk, damaging the organization’s ability to operate and undermining its reputation. The consequences of a disruptive incident vary and can be far-reaching, and they may not be immediately obvious at the time of the incident.

In 2008, the British Standards Institution (BSI) released BS 25777:2008, Information and Communications Technology Continuity Management: Code of Practice, to help organizations plan and implement an ICT continuity strategy. BS 25777 gives recommendations for ICT continuity management within the framework of BCM provided by BS 25999-1:2006, Business Continuity Management: Code of Practice. This article provides an introduction to the key elements of ICT continuity based on BS 25777.

THE CONCEPT OF BUSINESS CONTINUITY
BCM grew out of requirements in the early 1970s to provide computer disaster recovery for information systems (IS). Traditional disaster planning had concentrated on the restoration of facilities after a major incident such as the loss of a building or plant through fire or flood or the loss of computing or telecommunications throughout an enterprise. Disaster recovery plans, in general, are written on the basis of recovery after an event.

BCM is about prevention—it is not just a cure. It is not only about being able to deal with incidents when they occur and, thus, prevent crisis and subsequent disaster, it is also about establishing a culture within organizations that seeks to build greater resilience to ensure the continuity of product and service delivery to clients and customers.2

BCM is focused on entire business processes rather than on particular assets, such as IT systems, because, in order to operate, an organization must continue to execute its critical business processes. These processes may be contained within one business function, or they may integrate or impact a number of them. Recovery of IT systems alone will not keep such business processes running if staff do not have proper working conditions, if critical paper records have been destroyed, or if the organization cannot communicate with its customers and suppliers.3

THE CONCEPT OF ICT CONTINUITY
Historically, business continuity planning (BCP) has resided in the IT department of most organizations. For this reason, most companies have some disaster recovery alternatives in place for their IT systems. The most common disaster recovery alternative used is offsite data storage, in which data are regularly backed up to tape or disk and kept at a remote location. Although several other technological alternatives for IT recovery are available, especially for larger
corporations, such as hot and cold sites, electronic vaulting, shadowing, mirroring, and disk-to-disk remote copy, they are not used by many corporations. In this tough economic environment, it is very tempting to cut resources for BCP. Many enterprises mistakenly view BCP as an insurance policy for which they will likely never have to place a claim.4

ICT continuity supports the overall BCM process of an organization. BCM seeks to ensure that the organization’s processes are protected from disruption and that the organization is able to respond positively and effectively when disruption occurs. The organization sets out its BCM priorities, and within that context, ICT activities take place. ICT continuity ensures that required ICT services are resilient and can be recovered to the predetermined levels within the timescale required and agreed to by top management. Thus, effective BCM depends on ICT continuity to ensure that the organization can meet its objectives at all times (see figure 1), particularly during times of disruption.5

Figure 1—Relationship Between ICT Continuity and BCM

THE FOCUS OF ICT CONTINUITY
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 monitor their ICT services to ensure that:

- They are resilient and recoverable at the appropriate level
- Any unexpected event within a service is detected, addressed and investigated in a timely manner
- Dependencies between ICT services and external factors are known and used in assessing risk and the impact of a change
- Dependencies on the technical components are known and used in assessing risk and the impact of change

ICT continuity processes and solutions are also intended to ensure that legal obligations (such as protecting personal and otherwise sensitive data) are not breached.

PRINCIPLES OF ICT CONTINUITY
ICT continuity is based on six key principles:7

1. Protect—Protecting the ICT environment from environmental failures, hardware failures, operations errors, malicious attack and natural disasters is critical to maintaining the desired levels of system availability for an organization.

2. Detect—Detecting incidents at the earliest opportunity minimizes the impact to services, reduces the recovery efforts and preserves the quality of service.

3. React—Reacting to an incident in the most appropriate manner leads to a more efficient recovery and minimizes any downtime. Reacting poorly can result in a minor incident escalating into something more serious.

4. Recover—Identifying and 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. Services of a less-critical nature may be reinstated at a later time or, in some circumstances, not at all.
5. **Operate**—Operating in disaster recovery mode until return to normal is possible may require some time and necessitate “scaling up” disaster recovery operations to support increasing business volumes that need to be serviced over time.

6. **Return**—Devising a strategy for every IT continuity plan allows an organization to migrate back from disaster recovery mode to a position in which it can support normal business.

**EVALUATING THREATS TO CRITICAL ACTIVITIES**

In a BCM context, the level of risk should be understood specifically in respect to the organization’s critical activities and the risk of a disruption to these. Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders. The organization should understand the threats to these resources, the vulnerabilities of each resource, and the impact of a threat if it became an incident and caused a business disruption.

Which risk assessment approach is chosen is entirely the decision of the organization, but it is important that the approach is suitable and appropriate to address all of the organization’s requirements.

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

- Reduce the likelihood of a disruption
- Shorten the period of disruption
- Limit the impact of a disruption on the organization’s key products and services

These measures are known as loss mitigation and risk treatment. Loss mitigation strategies can be used in conjunction with other options, as not all risks can be prevented or reduced to an acceptable level.

**UNDERSTANDING THE ICT REQUIREMENTS FOR BUSINESS CONTINUITY**

As part of its BCM program, the organization should categorize its activities according to their priority for recovery. Top management should agree on the organization’s business continuity requirements.

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 sets the MTD for each critical process, it needs to establish some specific recovery objectives for each process. The two primary recovery objectives that organizations set in a BIA are:

1. **Recovery time objective (RTO)**—Target time set for resumption of product, service or activity delivery after an incident

2. **Recovery point objective (RPO)**—Point in time at which data have to be recovered to resume services

The organization should define its ICT services, and ICT service names should be meaningful to the organization.

The ICT services that are required to support achievement of the RTO for each critical activity, as prioritized by the BCM program, should be identified. The organization should document the list of critical ICT services, together with an RTO and RPO for each service. Some indication of the ICT service minimum capacity required at reinstatement and how quickly this capacity may need to be increased could also be necessary. The ICT service RTO should generally be less than the RTO for the critical activity it supports. (This may not be the case when the business continuity strategy calls for an interim measure, such as a manual procedure, instead of depending entirely on the ICT service.)

Top management should agree on the list of critical ICT services and their associated ICT continuity requirements. For each critical ICT service listed and agreed on by top management, the organization should describe and document the ICT components that make up the end-to-end service and how they are configured or linked to deliver each service. This analysis should consider physical and logical configurations. The normal ICT service delivery environment and the ICT continuity service delivery environment configurations should be documented.

The current continuity capability should be reviewed for each critical ICT service, from a prevention perspective, to assess risk of service interruption or degradation (e.g., single points of failure) and to highlight opportunities to improve ICT service resilience and, thus, the likelihood and/or impact of service disruption. It may also highlight opportunities to enable early detection and reaction to ICT service disruption. The organization can decide whether there is a business case to invest in identified opportunities to improve service resilience. This service risk assessment may also advise the business case for enhancing ICT service recovery capability.
IDENTIFYING GAPS

For each critical ICT service, the current ICT continuity service delivery environment configuration should be compared to the normal ICT service delivery environment, from a recovery perspective, to identify gaps or mismatches that may compromise ICT service recovery, such as inadequate data storage capacity.

Gaps identified among critical ICT service continuity capabilities and business continuity requirements should be documented. These gaps may indicate additional resources that each critical ICT service will require during recovery, but that are not already in place.

DETERMINING CHOICES

The organization should consider a range of options for each critical ICT service. The organization may include one or more or all of the following strategies.10

Business Continuity

Continuity strategies seek to improve the organization’s resilience to a disruption by ensuring critical activities continue at, or are recovered to, an acceptable minimum level and at time frames stipulated within the BIA.

Acceptance

A risk may be acceptable without any further action being taken. Even if it is not acceptable, the ability to do anything about some risks could be limited, or the cost of taking any action could be disproportionate to the potential benefit gained. In these cases, the response may be to tolerate the existing level of risk if top management deems the risk to be acceptable and within the organization’s risk appetite. In some circumstances, the impact of a risk may be outside the organization’s normal risk appetite, but due to the low likelihood of the risk occurring and/or the uneconomic cost of control, top management may accept the risk.

Transfer

For some risks, the best response may be to transfer them. This may be done by conventional insurance or contractual arrangements, or it may be done by paying a third party to take the risk in another way. Risks may be transferred to reduce the risk exposure of the organization or because another organization is more capable of effectively managing the risks. It is important to note that some risks are not fully transferable; in particular, it is generally not possible to transfer reputational risk, even if the delivery of a service is contracted out.

Change, Suspend or Terminate

In some circumstances, it may be appropriate to change, suspend or terminate the ICT service, product, activity, function or process. This option should be considered only when there is no conflict with the organization’s objectives, statutory compliance or stakeholder expectation.

EXERCISING AND TESTING

An organization’s ICT continuity plans cannot be considered reliable until exercised. An exercise program may involve a number of tests.

The organization should exercise not only the recovery of the ICT service, but also the service protection and resilience elements to determine whether:

- The service can be protected, maintained and recovered regardless of the incident severity
- The continuity arrangements can minimize the impact to the business

The exercise is a businesswide activity and not just the domain of the ICT department. The ICT department may retain the planning and execution aspects of the exercise, but the organization still has a key role to play.

CONCLUSION

All activity is susceptible to disruption from internal and external events such as technology failure, fire, flood, utility failure, illness and malicious attack. ICT continuity provides the capability to react before a disruption occurs or on detection of one or a series of related events that become incidents, and to respond and recover when those incidents result in disruption.

ICT continuity is integral to ICT strategy and ICT service management, which align to organizational strategy. It is the element of ICT strategy and service management that enables an organization to continue to meet its goals and deliver its products and services when adverse conditions occur.

ICT continuity supports the overall BCM process of an organization. BCM seeks to ensure that the organization’s processes are protected from disruption and that the
organization is able to respond positively and effectively when disruption occurs. The organization sets out its BCM priorities, and it is within this context that ICT activities take place.

ICT continuity management and BCM form an important part of effective management, sound governance and organizational prudence. Top management is responsible for maintaining the ability of the organization to continue to function in the face of disruption. Many organizations also have a statutory or regulatory duty to maintain effective risk-based controls, including BCM. BS 25777 will help any organization plan and implement an ICT continuity strategy within the framework of BCM as provided by BS 25999.

ENDNOTES
1 Her Majesty’s Stationery Office (HMSO), *An Introduction to Business Continuity Management*, UK, 1995
2 Sharp, John; *The Route Map to Business Continuity Management: Meeting the Requirements of BS 25999*, British Standards Institution (BSI), UK, 2007
3 Op cit, HMSO
4 Rittinghouse, John; James F. Ransome; *Business Continuity and Disaster Recovery for InfoSec Managers*, Elsevier Digital Press, UK, 2005
6 Ibid.
7 Ibid.
9 Op cit, BSI, *BS 25777:2008 Information and Communications Technology Continuity Management: Code of Practice*

ACKNOWLEDGMENT
Permission to reproduce extracts from British Standards is granted by the British Standards Institution (BSI). No other use of this material is permitted. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: [http://shop.bsigroup.com](http://shop.bsigroup.com) or by contacting BSI Customer Services for hard copies only: Tel: +44 (0)20 8996 9001, E-mail: cservices@bsigroup.com.