

# 4 火

## Section Four

# Infocomm Technology Readiness for Business Continuity

## - The International Standardisation Effort on ICT Continuity

**In 2007, a new work item proposal on ICT Readiness for Business Continuity** was proposed and circulated by ISO/IEC JTC 1 SC 27 and was balloted in favour by the National Bodies. Since then, much progress has been made to prepare an international standard on the areas of ICT continuity and responsiveness. The article intends to update the readers on the recent development of the standard, namely ISO/IEC 27031, which Singapore has been actively contributing by providing co-editorship, as well as submitting the SS540 standard as input for the development of the international standard.

“ Philip Sy  
Principal Consultant, e-Cop  
ISO/IEC JTC 1 SC 27 WG 4 Secretariat  
ISO/IEC 27031 Co-Editor  
Convenor, ISMS Working Group  
Security & Privacy Standards Technical Committee ”

### 1 BACKGROUND

On its 18th Plenary meeting held in Madrid on 16-17 May 2006, ISO/IEC SC 27 resolved to establish a new Working Group 4 “Security controls and services” in addition to its three working groups. The new working group, WG 4 in short, covers the development and maintenance of standards and guidelines addressing services and applications supporting the implementation of control objectives and controls as defined in ISO/IEC 27001 [1].

Since its incorporation, SC 27/WG 4 has published standards addressing the provision of disaster recovery services (ISO/IEC 24762), network security (ISO/IEC 18028), intrusion detection systems (ISO/IEC 18043), and information security incident management (ISO/IEC TR 18044). Whilst WG 4’s standards supports the implementation of the ISO/IEC 27000 series of standards developed and standardised in WG 1, its scope of work may not necessarily be confined to those scoped within the ISO/IEC 27000 series of standards. One of such an example is the ICT readiness for business continuity (ISO/IEC 27031). Although ISO/IEC 27031 supports clause 14 (Business Continuity Management control objectives) of ISO/IEC 27002 in the management of information security, its scope extends well beyond the information security management domain and intends to elaborate how to plan and maintain an organisation’s ICT readiness in support of its business continuity management effort.

## 2 IMPORTANCE OF ICT READINESS FOR BUSINESS CONTINUITY (IRBC)

Over the years, Information and Communication Technology (ICT) has become an integral part of many of the activities which are elements of the critical infrastructures in all organisational sectors, whether public, private or voluntary. The proliferation of the Internet and other electronic networking services, and today's capabilities of systems and applications, meant that organisations have become ever more reliant on reliable, safe and secure ICT infrastructures and services.

Meanwhile, the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has been recognised and supported with specific domains of knowledge, expertise, and standards developed and promulgated in the recent years.

However, although a number of Business Continuity Management Standards have emerged, the standards usually focused on the overall framework for managing the continuity of an organisation's business activities and therefore are usually lack of elaboration of essential elements such as Infocomm technology services and systems. The Singapore standard, SS540 goes extra mile to elaborate the four essential elements in BCM - namely policy, people, process and infrastructure [2] - and hence provides a very good starting point for establishing a standard focusing on the ICT continuity aspects. (Singapore has submitted SS540 to SC27 in 2008 for use as input in developing the new standard on ICT readiness.)

In planning for business continuity, the requirements for information processing and communication facilities need to be effectively planned and implemented so that they are ready to support the business continuity management requirements to ensure information and service availability. In the context of ISO/IEC 27031, the scope of business continuity is expanded to include preparedness for focusing events such as ICT security incidents and failures of ICT systems; and intend to provide the guidance for planning and maintaining ICT infrastructure and services required for effective and efficient response to those focusing events, including emergency situations [3].

ICT continuity is a crucial element of an overall BCM strategy and will help an organisation survive a crisis. Customers are more likely to desert suppliers if they are not immediately responsive to system problems. As part of the implementation and operation of an information security management system (ISMS) [4] and IPOCM (Incident preparedness and operational (business) continuity management) [5] specified in ISO/IEC 27001:2005 and ISO-PAS 22399:2007 respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity. IRBC provides a meaningful way to determine the status of an organisation's ICT services in supporting its business continuity objectives by addressing the question "is our ICT capable of responding" rather than "is our ICT secure".

It is the intention of the ICT Readiness standard to be in line with and support current and emerging BCM standards. The published Singapore Standard for Business Continuity Management (BCM) SS540:2008 was submitted as input document for the ISO/IEC 27031. Furthermore, liaison has been established with ISO TC223 which targets to develop the first international Business Continuity Management System Specifications ISO 22301 (which Singapore has been contributing both co-editorship and the SS540 standard itself for valuable input).

### 3 OVERVIEW OF IRBC FRAMEWORK [6]

ISO/IEC 27031 describes the concepts and principles of ICT Readiness for Business Continuity, and provides a framework of methods and processes for any organisation – private, governmental, and non-governmental – irrespective of size, to identify and specify all aspects (such as performance criteria, design, and implementation) for improving its ICT readiness to ensure business continuity. It also enables an organisation to measure performance parameters that correlate to its IRBC in a consistent and recognised manner.

In order for an organisation to achieve ICT Readiness for Business Continuity, it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. This can be best achieved by applying the Plan-Do-Check-Act (PDCA) cyclical steps as part of a management system in ICT Readiness for Business Continuity (IRBC). In this way IRBC supports BCM by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organisation.

As part of the BCM process, IRBC refers to a management system which complements and supports an organisation's BCM and/or ISMS programme, to improve the readiness of the organisation to:

- Respond to the constantly changing risk environment;
- Ensure continuation of business operations supported by the related ICT services;
- Be ready to respond before an ICT service disruption occurs, upon detection of one or a series of related events that become incidents; and
- Respond and recover from incidents/disasters and failures.

IRBC is to be established based on the following key principles:

- Incident Prevention
  - Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an organisation.
- Incident Detection
  - Detecting incidents at the earliest opportunity will minimise the impact to services, reduce the recovery effort, and preserve the quality of service.
- Response
  - Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimise any downtime. Reacting poorly can result in a minor incident escalating into something more serious.
- Recovery
  - 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.

As shown in the figure below, at the time of the happening of a major ICT disruption, such readiness activities aim to:

- Improve the incident detection capabilities;
- Prevent a sudden or drastic failure;
- Enable an acceptable degradation of operational status should the failure be unstoppable;
- Further shorten recovery time; and
- Minimise impact upon eventual occurrence of the incident.

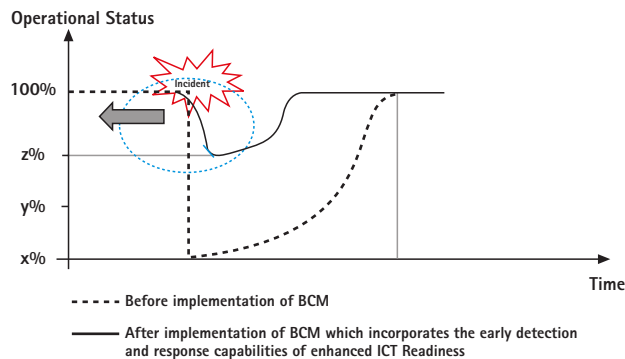


Figure 1: Before and after implementation of BCM

The key elements of IRBC can be summarised as follow:

- a) People: the specialists with appropriate deputies and knowledge;
- b) Facilities: the physical environment in which ICT resources are located;
- c) Technology:
  - i) the racks, servers, storage arrays, tape devices, other hardware and other permanent fixtures;
  - ii) network (including data connectivity and voice services), switches and routers;
  - iii) software, including operating system and application software, links or interfaces between applications and batch processing routines;
- d) Data: application data, voice data and other types of data;
- e) Processes: including supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services; and
- f) Suppliers: other components of the end-to-end services where ICT service provision is dependent upon an external service provider or another organisation within the supply chain, e.g. a financial market data provider, telecoms carrier or internet service provider.

## 4 CONCLUSION

The ISO/IEC 27031 standard has gone through the stage of working draft and is now being balloted and reviewed within SC 27/WG 4 as a Committee Draft (CD). It is targeted to proceed to the Final Draft of International Standard (FDIS) stage by end 2010 (refer to the stages of JTC 1 standard development illustrated below [7]).

| Stage                     | Document   |
|---------------------------|--|
| Stage 0                   |  |
| Stage 1 Proposal Stage    | NP (New Work Item Proposal)                        |
| Stage 2 Preparatory Stage | WD (Working Draft)                                 |
| Stage 3 Committee Stage   | CD / FCD (Committee Draft / Final Committee Draft) |
| Stage 4 Approval Stage    | FDIS (Final Draft International Standard)          |
| Stage 5 Publication       | IS (International Standard)                        |

Figure 2: Stages of JTC 1 standard development

When finally ISO/IEC 27031 is released, organisations will be provided with an effective way to determine the status of an organisation's ICT services in supporting its business continuity objectives by addressing the question "is our ICT capable of responding" rather than just "is our ICT capable of supporting the daily operation".

## 5 REFERENCES

- [1] ISO/IEC JTC 1 SC 27 N5173 document - Terms of reference for Working Group 1 'Information security management systems' and the new Working Group 4 'Security controls and services'.
- [2] SS540:2008, Singapore Standard for Business continuity management (BCM).
- [3] ISO/IEC JTC 1 SC 27 N5726 document - New Work Item Proposal on ICT Readiness for Business Continuity.
- [4] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements.
- [5] ISO/PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management.
- [6] ISO/IEC JTC 1 SC 27 N7556 document - ISO/IEC 27031 Committee Draft, Information technology - Security techniques - Guidelines for ICT readiness for business continuity
- [7] ISO/IEC JTC 1 Directives, 5th Edition, Version 3.0, available at:  
- [http://isotc.iso.org/livelink/livelink/fetch/2000/2489/186491/186605/Jtc1\\_Directives.pdf?nodeid=3959538&tvernum=0](http://isotc.iso.org/livelink/livelink/fetch/2000/2489/186491/186605/Jtc1_Directives.pdf?nodeid=3959538&tvernum=0)

## BIOGRAPHY OF AUTHOR



**Philip Sy**

Principal Consultant, e-Cop  
ISO/IEC JTC 1 SC 27 WG 4 Secretariat  
ISO/IEC 27031 Co-Editor  
Convenor, ISMS Working Group  
Security & Privacy Standards Technical Committee

As one of the pioneers in Information Security (IS) management and BCM, Philip has contributed to both local and international standardisation in the areas of IS and BC/DR, providing consultancy and audit services to local and overseas organisations. He was in charge of editing the ISO/IEC 24762 standard (Guidelines for ICT Disaster Recovery Services) and in the recent revision of SS507 standard.

Philip chairs the ISMS Working Group and is an active member of the Security & Privacy Standards Technical Committee (SPSTC) under ITSC, the BC/DR Working Group as well as joint BCM Working Group of the TC.