Business continuity
ISO 22301 when things go seriously wrong

By Dave Austin, ISO 22301 Project Leader and CEO at Operational Resilience Limited (OPREL)

Key note speaker at the 1st BCM Forum 2014

Contingency planning and disaster recovery were largely information technology-led responses to natural disasters and terrorism that affected businesses during the 1980s and early 1990s.

There was a growing recognition, however, that this needed to become a business-led process and encompass preparing for many forms of disruption.
In light of this, the discipline became known as Business Continuity Management (BCM).

As governments and regulators began to recognize the role of Business Continuity in mitigating the effects of disruptive incidents on society, they increasingly sought to gain assurance that key players had appropriate
business continuity arrangements in place.

Similarly, businesses recognized their dependence on each other and sought assurance that key suppliers and partners would continue to provide key products and services, even when incidents occurred.

A recognized benchmark of good practice in BCM was therefore needed and several national standards sought to address this issue, including those from Australia, Singapore, the United Kingdom (UK) and the USA. In the UK, BS 25999 was introduced to provide a management systems standard to which organizations could obtain accredited certification for the first time.

When organizations operating internationally started calling for a single International Standard, the ISO/TC 223 committee responded by developing ISO 22301:2012. The new standard is the result of significant global interest, cooperation and input.

Demonstrating good practice, ISO 22301 is a management systems standard for BCM which can be used by organizations of all sizes and types. These organizations will be able to obtain accredited certification against this standard and so demonstrate to legislators, regulators, customers, prospective customers and other interested parties that they are adhering to good practice in BCM.

ISO 22301 also enables the business continuity manager to show top management that a recognized standard has been achieved. While ISO 22301 may be used for certification and therefore includes rather short and concise requirements describing the central elements of BCM, a more extensive guidance standard (ISO 22313) is being developed to provide greater detail on each requirement in ISO 22301.

ISO 22301 may also be used within an organization to measure itself against good practice, and by auditors wishing to report to management. The influence of the standard will therefore be much greater than those
who simply choose to be certified against the standard.

Growing pains

The work on ISO 22301 started in 2006 when an ISO workshop on “Emergency Preparedness” was held in Florence, Italy. At the time, many experts argued that their own national standard was best suited to be
developed into an International Standard.

As this was clearly no way forward, all the major players were gathered to identify the similarities between the standards. This spirit of consensus led to the publication of a guidance document for incident preparedness and continuity management called ISO/PAS 22399:2007.

A challenge with ISO 22301 has been the large number of national documents on the subject, which has caused difficulties in gaining agreement. The committee was then ready to create a management system standard with requirements and intended for certification. Input from the national standards was used to develop the initial draft wordings and gradually refined to become a new document bringing together good practice from around the world.

Significant input came from Australia, France, Germany, Japan, the Republic of Korea, Singapore, Sweden, Thailand, the UK and the USA. Many others contributed to its development, showing the truly international interest and
input involved.

ISO 22301 explained

ISO 22301 is the second published management systems standard that has adopted the new high-level structure and standardized text agreed in ISO. This will ensure consistency with all future and revised management system standards and make integrated use easier with, for example, ISO 9001 (quality), ISO 14001 (environmental) and ISO/IEC 27001 (information security). The standard is divided into 10 main clauses, starting with scope, normative references, and terms and definitions. Following these are the standard’s requirements:

• **Clause 4** – Context of the organisation
The first step involves getting to know the organization, both internal and external needs, and setting clear boundaries for the scope of the management system. In particular, this requires the organization to understand the requirements of relevant interested parties, such as regulators, customers and staff. It must in particular understand the applicable legal and regulatory requirements. This enables it to determine the scope of the Business Continuity Management System (BCMS).

• **Clause 5** – Leadership
ISO 22301 places particular emphasis on the need for appropriate leadership
of BCM. This is so that top management ensures appropriate resources are provided, establishes policy and appoints people to implement and maintain the BCMS.

• **Clause 6** – Planning
This requires the organization to identify risks to the implementation of the management system and set clear objectives and criteria that can be used
to measure its success.

• **Clause 7** – Support

Since resources are required for implementation, Clause 7 introduces the important concept of competence. For business continuity to be successful,
people with appropriate knowledge, skills and experience must be in place
to both contribute to the BCMS and respond to incidents when they occur.

It is also important that all staff are aware of their own role in responding to incidents and this clause deals with all of these areas.

The need for communication about the BCMS – for instance in telling customers that the organization has appropriate BCM in place – and preparedness to communicate following an incident (when normal channels
may be disrupted) is also covered here.

• **Clause 8** – Operations
This section contains the main body of business continuity-specific expertise.
The organization must undertake business impact analysis to understand how its business is affected by disruption and how this changes over time.

Risk assessment seeks to understand the risks to the business in a structured
way and these inform the development of business continuity strategy.

Steps to avoid or reduce the likelihood of incidents are developed alongside steps to be taken when incidents occur. As it is impossible to completely predict and prevent all incidents, the approach of balancing risk reduction and planning for all eventualities is complementary. It might be said, “hope for the best and plan for the worst”.

ISO 22301 emphasizes the need for a well-defined incident response structure. This ensures that when incidents occur, responses are escalated in a timely manner and people are empowered to take the necessary actions to be effective.

The requirements for business continuity plans are laid out in Clause 8, too. Quickly understood, user-focused documents are more suitable than the large, unwieldy documents suited to auditors. Smaller plans are therefore more likely to be needed than one large plan.

A requirement not previously addressed in business continuity standards is the need to plan for a return to normal business. This simple requirement forces organizations to determine what to do once the initial emergency has been addressed.

The final subsection of section 8 covers exercises and tests, a key part of BCM. Tests are where some element of the business continuity arrangements is demonstrated to work (a pass) or not (fail). For instance, I can test if the generator will run when I switch it on. An exercise may include tests, but is generally a more nuanced approach that simulates some aspect of responding to an incident.

This will usually include elements of training and building awareness of how to handle disruptive incidents with difficult and unusual characteristics, as well as finding out if processes work as expected.

Exercises and tests are fundamental in ISO 22301: it is only through structured exercises – which should stretch the individuals and teams involved – that an organization can achieve objective assurance that

its arrangements will work as anticipated and when required.

• **Clause 9** – Evaluation
For any management system, it is essential to evaluate performance against plan. ISO 22301 therefore requires that the organization selects and measures itself against appropriate performance metrics. Internal audits must be conducted, as well as reviews of the BCMS, and appropriate action must be taken.

• **Clause 10** – Improvement
No management system is perfect at the outset, and organizations and their environments are constantly changing. Clause 10 defines actions to take to improve the BCMS over time and ensure that corrective actions arising from audits, reviews, exercises and so on are addressed.

Successful implementation
To work well, ISO 22301 will need organizations to have thoroughly understood its requirements. Every line and word has meaning and the relative importance is not necessarily reflected by the number of words devoted to a topic.

Rather than being simply about a project or developing “a plan”, BCM is an ongoing management process requiring competent people working with appropriate support and structures that will perform when needed.

Published in netfax 24.01.2014