STANDARD ISO/IEC 22301: Business Continuity Management in a single framework

By Matthieu Aubigny, Alex Mckinnon, itrust consulting

In a world where business management is synonymous with strict management, the continuity of business activities has become more and more important. If business continuity management needs some operational rules, the new standard ISO 22301 published in June 2012 gives the missing strategic guidelines to improve the quality of business continuity: a Swiss army knife for the new Business Continuity Officer and future quality criteria through Certification based on this new standard.

At present, business continuity management involves strict management to improve the profitability of each activity and to avoid sleeping assets or processes. However, another side of that business philosophy is not well known: minor incidents can affect the entire framework. For this reason, assuring business continuity, by overcoming incidents or security breaches, becomes more and more important. Moreover, as all business activities, including critical activities from a societal point of view, are interdependent to provide services to the citizens of the world, business continuity management is not just an option but one of the fundamental harmonics to ensuring societal security in the worldwide economic environment.

Business continuity is not a new topic and has been addressed in two different ways:

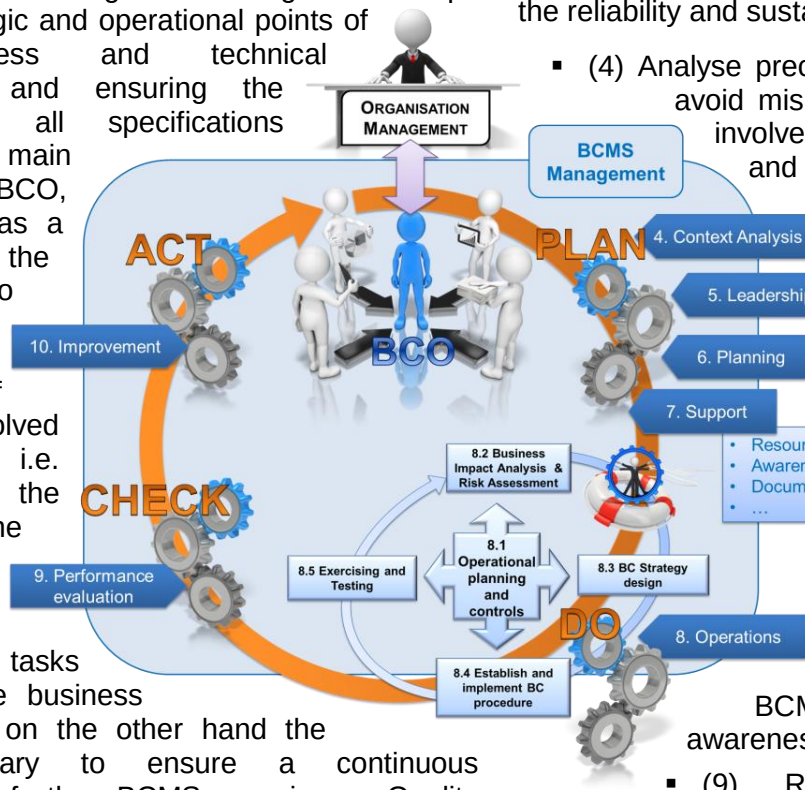
- Firstly, by international, European or governmental regulations which give strict guidelines to avoid threats on business continuity or to decrease impact on societal security. For example, the financial regulations (Sarbanes-Oxley Acts) to mitigate corporate and accounting risks, the banking regulations (Basel Accords) to mitigate financial and operational risks in the banking sector, and the European commercial regulations (MIFID) to control the market and protect investors. In Luxembourg, the CSSF regulations encourage transparency of the financial market to avoid disruption and financial cascading effects.
- Secondly, by more technical guidelines to implement continuity developed by professional groups such as the British Standard Institution with the BS 25999, the Federal Office for Information Security (BSI) BSI-Standard 100-4, the US DRII (Disaster Recovery Institute International), and the British BCI (Business Continuity Institute). We could also mention more recently (2011), the ISO 27031 which addresses "*the concepts and principles of information and communication technology (ICT) readiness for business continuity*" and provides a framework of methods to implement this readiness. Specific standards are also directly linked to business continuity such as the standards provided by NFPA (National Fire Protection Association), to enforce the protection of business assets.

However, to ensure business continuity, an organisation which binds together all these aspects still misses the master piece to perform an accurate management of the continuity, to balance strategic regulations and technical points of views, and to harmonise business efficiency, risk and societal security: this Standard, published in June, exists in the form of ISO 22301.

The BCO as master key for the systemic framework

If the notions described in the standard are perfectly in line with the referential mentioned above, the major points of the document are on one hand to

underline that business continuity management has to be considered as a systemic framework and for that reason shall be based on a specific system of management titled BCMS (Business Continuity Management System); and on the other hand that this BCMS requires a dedicated team and especially a person responsible for BCMS implementation: "*Top management shall provide evidence of its commitment to the establishment, implementation […] of the BCMS by appointing one or more persons to be responsible for the BCMS with appropriate authority and competencies…*". Even if the standard does not underline this point, the BCO (Business Continuity Officer) becomes the master key of this new standard, in charge of building relationships between strategic and operational points of view, business and technical requirements, and ensuring the alignment of all specifications together. The main role of the BCO, more defined as a watermark in the standard, is to be the conductor of the whole set of processes involved in the BCMS, i.e. (as shown in the figure) on one hand the management of the operational tasks involved in the business continuity and on the other hand the tasks necessary to ensure a continuous improvement of the BCMS as in a Quality Management System or an ISMS and to ensure relations with top management. The standard also allows defining the profile of the future BCO: even if their responsibilities include operational tasks, their main duty requires more management qualities and, without contest, knowledge of the whole chain of the business activity and a high level of responsibility in the organisation to be able to ensure a good relationship with every actor involved.



The BCMS in detail

The description of the operations (chapter 8) can be described as a sub-cycle under the direct responsibility of the BCO (8.1), which includes four phases:

- (8.2) A Business Impact Analysis (BIA) and a Risk Assessment (RA) which shall cover all relevant activities of the business, involve all persons responsible, and take into account the results of former tests of the BC infrastructure.
- (8.3) the design of a BC strategy taking into account the most critical activities according to the BIA and RA and involving a societal security point of view (financial and economic stability, interdependence of activities...).
- (8.4) the implementation of procedures and processes necessary to deploy the strategy.
- (8.5) the tests and exercises performed regularly to verify the operational level of the BC framework.

The management task of the BCO aims to ensure the reliability and sustainability of the BC activities:

- (4) Analyse precisely the business context to avoid misunderstanding of societal risk involved by the business activities and to define the target of evaluation (TOE).
- (5) Implement a real relationship with stakeholders and top management according to a defined BC policy.
- (6) Plan the BCMS strategy according to business priorities.
- (7) Organise management support i.e. the BCMS documentation, resources, awareness, training, etc.
- (9) Review and assess the performance of the BC framework.
- (10) Improve and verify the compliance of the BC framework.

In order to be operational for any business activities and organisation, the standard focus still remains generic but should be complete with specific approaches provided by other standards.

- The ISO 27005 which provides a recommended risk analysis framework.
- The ISO 22313 (12/2012) which provides technical guidelines to apply the standard.
- The ISO 22300 and ISO 22312 which specify on one hand the BC vocabulary and on the other hand

the modelling frameworks of threats, specific targets and counter-measures.

- The ISO 27031 to deploy a BC framework in an ICT environment.

The certification process

The implementation of the standard's requirements can lead to the acquisition of an ISO certificate by the dedicated certification body. The process will be similar to ISMS certification 27001 or quality certification 9001. It is well known that this type of certification requires significant workload, not only to set up but also to maintain the certification of a BCMS. Therefore, the main question is on the opportunity for the organisation in order to assess the balance between benefits and costs. The workload is similar to the workload of an ISO 27001 certification. What could be the benefits to initiate such certification?

- As a management standard, the ISO 22301 will improve the quality of the management and the business reactivity of the organisation.
- As the standard process requires assessing all business processes and their relative risks, its implementation will improve the organisations knowledge of the whole chain of business processes especially their criticism and interdependent aspects.
- Linked to the previous benefits and based on the dedicated responsibility of the BCO, the implementation of the standard will improve the reactivity of the organisation in case of real crisis and avoid risk cascading effects in case of security incident.
- The improvement of the legal compliance of the organisation.
- The improvement of the organisation's resilience.
- The improvement of the organisation's competitiveness by increasing the customer's confidence level.
- And last but not least, the improvement of the societal security at any level (national, European or worldwide).

As certification bodies, organisations such as SNCH, LSTI, AFNOR Certification, BSI already propose to assess ISO 22301 compliance. Compliance to legal requirements at national or European level, customers' expectancies or requirements, reduction of capital equity could lead to initiating the certification process or audit; but in all cases, the reliability of the business will increase both for the customers and for the stakeholders. For all these reasons, itrust consulting will support organisations to apply the new standard by offering trainings and implementation expertise, and internal and external auditors.

The announced trainings in Luxembourg with exam by LSTI are:

hts High Tech Security | itrust consulting

Lead Auditor
1-5/07/2013 – LUXEMBOURG
Lead Implementer
18-22/11/2013 – LUXEMBOURG
More info and registration on www.itrust.lu

HSC Formations

Lead Implementor
10-14/06/2013 - LUXEMBOURG