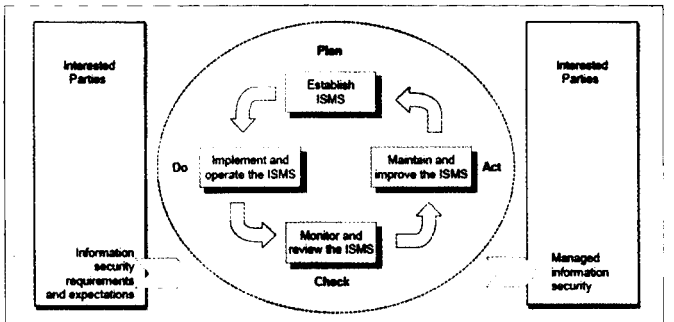
The growing accreditation of IT security tools and processes

Vincent Villers
Marc Sel

For a long time, Information Security has had many technical standards but has been lacking a minimal consensus in the area of management and responsibilities. The BSI (British Standards Institute) put forward their 7799 standards, which were well accepted and evolved into the ISO (International Standards Organisation) world.

Fundamental to the ISMS (Information Security Management System) standard is the typical management organisation model 'Plan-Do-Check-Act':

as well as how to establish, manage and monitor the ISMS. It continues by addressing ISMS responsibilities, as well as audit and management review aspects.



PDCA model applied to ISMS processes

ISO 27001 is commonly used as a term to refer to a family of interrelated standards:

- 27000 ISMS fundamentals and vocabulary
- 27001 ISMS requirements (absorbing parts of ISO 13335)
- 27002 Code of practice (based on the BSI 7799)
- 27003 ISMS implementation guidelines
- 27004 Information security management measurements
- 27005 ISMS risk management (absorbing parts of ISO 13335)

Structure of ISO 27001

The main standard document ISO 27001 addresses requirements for the Information Security Management System,

The ISO 27001 certification process

In many countries, certification bodies have been established under the umbrella of accreditation bodies. For example, one of the authors, Marc Sel, is accredited Lead Auditor for PwC's Certification Body 'PwCC B.V.' which is on a peer level with the BSI, TÜV and KEMA (1). PwCC B.V. is in turn accredited by the Dutch Accreditation Body ('Raad voor Accreditatie').

The International Register of ISMS accredited certificates lists those certificates that have been awarded to organisations that have gone through an accredited certification process in line with the ISMS standard BS 7799 Part 2:2002 and ISO/IEC 27001:2005 (i.e. the revised version of BS 7799 Part 2:2002).

This register has been produced in cooperation with the international network of certification bodies and is managed and maintained by the ISMS International User Group (IUG). It is updated on a regular basis in co-operation with the certification bodies. The entries in this register have been supplied by those certification bodies that have carried out the ISMS certification.

The increasing interest in ISO 27001 certification

In November 2008, almost 5.000 ISMS certificates have been issued (4.987 to be precise)2. The top five countries with the highest number of certificates today are Japan, India, the UK, Taiwan and China. They are followed by Germany and the USA.

The best advice to follow is to centralise core IT services in larger data centres. For example, the data centres of PwC Yemen, UK, Hong Kong, China, and USA have been secured by ourselves and accredited by the BSI against ISO 27001:2005. This gives us a strong background when helping customers prepare for such certification or improve their security posture.

In Luxembourg, only one company is registered as being accredited against the standard so far. However, considering the current trend of financial institutions to focus on their core business by considering outsourcing of several functions, coupled with the increasing need to embed trust in business relationship, all conditions are fulfilled to lead to a growing interest for this certification. Indeed, unlike current perception of other standards, the ISO 27001:2005 relies upon clear requirements and implementation guidelines and its implementation is becoming an optimal approach to tackling regulatory requirements for IT controls.

Finally, rather than individually answering each request for compliance, it is advised to look at the requirements holistically, and build a framework that allows demonstrating compliance against a broad set of regulations, re-using the same set of well-defined controls. The implementation of such a control framework makes demonstrating compliance significantly less expensive.

The authors are respectively a partner at PwC Luxembourg and a director at PwC Belgium

(1) BSI British Standards is the National Standards Body of the UK, TÜV Rheinland Group is a leading provider of technical services worldwide, KEMA is a commercial enterprise, specializing in high-grade business and technical consultancy, inspections and measurement, testing and certification.

The status of the official ISO 27001 certificates is available at **www.iso27001certificates.com.**