



**IT Security Management Standards
for Today's Businesses**

This paper summarises the information presented during the L-SEC event “IT Security Management: Standards for Today’s Businesses”, which took place on January 20, 2006. Dr Marijke De Soete, Vice-Chair of ISO/IEC JTC 1/SC27 IT Security techniques chaired the seminar, which featured the following presentations:

- **International Standardisation of IT Security**
Dr Marijke De Soete, Manager, Sec4Biz/Philips Applied Technologies
- **IS 17799 2nd Edition: Main Changes, Comparison to BS7799**
Mr Christophe Sténuît, Manager, Ogeris
- **What is Up with Certification?**
Mr Christophe Sténuît, Manager, Ogeris
- **IS 13335 Management of Communication Technology Security and Risk Management**
Mr Jean-Luc Allard, Manager, MISIS
- **ISO/IEC 18028 Network Security**
Mr Marc Sel, Director, PWC
- **ISO/IEC 18044 Incident Management**
Mr Alain De Greve, IT Security Project Manager
- **Information Security Governance and the CobIT Framework for Process Implementation**
Mr Georges Ataya, President, ISACA Belux
- **Importance of the ISO Security Standards for the Security Professional**
Mr Bart Moerman, Security Officer, Isabel
- **Case Study: ISO 17799 Framework Implementation at ING Bank**
Mrs Veronique De Bie, SWE/OPS & IT/BIS Information Risk Managements,
Information Security Manager, ING Bank

The event concluded with a panel discussion on the practical use of standardisation and on certification in Belgium.

This paper is offered for information purposes only. L-SEC makes no representation or warranty, express or implied, of its accuracy or completeness. L-SEC assumes no liability for the use of or reliance on this information in this paper, or any of the referenced materials.



Table of Content

Standardisation	4
Benefits	4
Structure.....	4
Certification	5
ISO Standards.....	6
ISO/IEC JTC 1 SC27, IT Security Techniques Subcommittee	6
ISO/IEC17799.....	6
ISO27000 ISMS Series.....	7
ISO/IEC13335.....	7
ISO/IEC 18028.....	7
ISO/IEC TR 18044.....	8
ISSA	9
CobiT	10
Information Security Governance.....	10
Framework.....	10
CobiT Products	10
CobiT Security Baseline	10
Case Study: ING	11
Conclusion.....	12
Acronyms glossary.....	13



Standardisation

The L-Sec seminar provided an overview of the most important information security management standards, focussing on the benefits these standards bring to organisations' information security and to business in general.

Benefits

Information security plays a more important role than ever. Standards can offer companies operating in this increasingly internationalised business environment a muchneeded framework of reference. Standards offer benchmarks for the assessment of current situations and guidelines for drawing up an adequate action plan for risk management.

Structure

To stay in tune with the changing business world, standards are regularly updated and improved through iterative review cycles, both before their first publication, as well as during later revision cycles.

ISO standards in particular go through a six-stage process that may span several months before they are published. When a new ISO standard evolves from an existing standard, e.g. a national standard, the ISO Fast Track is followed. ISO standards are reviewed at least every five years, but if defects are identified, there will be earlier revisions.

There are several types of standardisation bodies, each with their own scope and structure. International bodies, like ISO, ITU-T and ETSI rely on formal processes, which imply that approval of new and revised standards may be lengthy process. Currently, however, these bodies' processes are being streamlined and speed up, partly as a result of digitisation of the process. Organisations like IETF have less formalised processes in place. The large numbers of participants and the transparency of the process sometimes impact the speed of decision making in these organisations. Industry groups and consortia focus on specific technologies and applications, and this specific scope implies they are able to issue workable standards at a fairly rapid pace. One potential drawback here is the lack of maintenance after standards have been published. The glossary on page 113 lists organisations active in the field of standardisation.



Certification

Certification is carried out by Certification Bodies. In order to become an accredited certification body, organisations have to demonstrate they comply with the requirements outlined in standards concerning accreditation, like ISO/IEC Guide 62 (General requirements for bodies operating assessment and certification/registration of quality systems), EN 45012 (the European Norm mirroring ISO/IEC Guide 62) and EA 7/03 (the guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems issues by the European Co-operation for Accreditation). The Belgian national accreditation body is BELAC. BELAC accredits national certification bodies like CEBEC, Vinçotte, the Belgian Construction Certification Association (BCCA) and IQA.

These certification organisations will certify that products, staff or processes comply with requirements set out in specific standards. Some examples:

- ISO 15408, the so-called Common Criteria is used as the basis for certifying security products.
- The International Information Systems Security Certification Consortium, (ISC)², has established the CISSP credential (Certified Information Systems Security Professional), which is accredited under the ISO/IEC 17024 standard for certifying persons.
- For processes, ISMS certification (Information Security Management Systems) shows that an organisation has an information security management system in place that complies with the requirements set out in ISO 27001.

For organisations, an ISO certification process itself typically contains three phases. The first one is a preparatory phase in which the organisation prepares for assessment. In the second phase, an accredited certification body conducts an audit to determine if the requirements have been met. This audit is carried out by qualified auditors. When the audit results are positive, the organisation receives a certificate. The organisation can then use the certificate number and ISO symbol for external communication and this for a period of three years. Within this period, qualified auditors will carry out surveillance audits. After three years, the organisation needs to be re-audited for continuation of the certification.

To consumers, certification signals that companies are trustworthy, as they have sound quality controls in place, and measure up to the standards. For service providers, certification offers credibility and recognition, a competitive edge and, first and foremost, a motivation for continuous process improvement. For legislators, certification allows for easier compliance checks, as it offers a conformity guarantee in view of specific regulations.



ISO Standards

ISO, established in 1947, is a worldwide federation of national standards bodies. The organisation spans 146 countries, each country delegating one member. BIN-IBN, the Belgian Institute for Normalisation (www.ibn.be) is the Belgian ISO member. ISO has been established to promote the development of standards to facilitate international exchange and cooperation. ISO is organised in technical bodies (2.952 in total), technical committees (TCs) and subcommittees (SCs) and working groups (WGs). ISO's work results in international agreements that are published as International Standards (IS).

ISO/IEC JTC 1 SC27, IT Security Techniques Subcommittee

The ISO/IEC JTC 1 SC27 subcommittee works on standardization of generic IT security services and techniques, including

- Identification of generic requirements for IT system security services, development of security techniques and mechanisms (cryptographic and non-cryptographic),
- Development of security guidelines,
- Development of management support documentation and standards,
- Development of criteria for IT security evaluation and certification of IT systems, components, and products.

ISO/IEC JTC 1 SC27 is currently organised into three working groups (WG). WG1 focuses on Security Guidelines, WG2 on Cryptography and Security Mechanisms, and WG3 works on Security Evaluation. The subcommittee's organisation structure is evolving. The creation of two new working groups is currently under discussion, one focusing on Security Controls and Services (WG4), and one on Privacy, identity and Biometric Security. Once the new structure is established, the focus of WG 1 will be on an international ISMS requirements specification standard, that will help organisations set up and maintain effective information security management systems. The potential addition of these new working groups reflects the committee's focus on new technologies and issues, like biometrics, privacy, identity management, which are the subjects of new studies and projects that will later develop into standards.

In order to ensure involvement, broad consensus, efficient use of resources and widespread usability and recognition, SC27 sets up liaisons with organisations such as ISSA and ISSEA, and ITU-T and ETSI.

Several of the ISO/IEC JTC 1 SC27 standards have been discussed in detail during the L-SEC event. An overview:

ISO/IEC17799

In 1992, the Industry Code of Practice for Information Security Management was published by DTI in the UK. This code of practice developed into BS 7799-1 in 1995. A revised version of this standard appeared in 1999. ISO 17799 was published in 2000, as a result of a fast track approval process of BS 7799.

In 2001, a first revision cycle of ISO 17799 started. The revision resulted in ISO/IEC17799, 2nd edition, published in November 2005. In this second edition, sections have been improved and additions have been made to cover new threats, to better reflect current practices and to cover new technologies. Reworked parts include the section on Human Resources security, which now also contains information on roles and responsibilities and on measures to be taken after termination of contracts. Comparable improvements have been made to other sections, like the section on Incident Management. At the same time, terminology use has been streamlined and controls have been reorganised.

ISO27000 ISMS Series

To bring more unity in the naming of the information security-related standards, a new family of standards has been established. The 27000 family will incorporate the ISMS standards.

- ISO 27000, a newly proposed project, will list the Principles and the Vocabulary used in the 27000 series.
- ISO 27001 will detail ISMS requirements, based on BS7799 Part 2:2002. It can be used as a basis for ISMS certification. Other standards in the family provide additional support, advice and information concerning the requirements outlined in ISO27001.
- ISO 27002 (ISMS Security techniques) will replace ISO/IEC 17799, 2nd edition, from April 2007 onwards, providing a code of practice for information security management.

Other standards that currently are being developed are

- ISO 27003 ISMS Implementation Guidelines, which will include details on the PDCA process model (Plan – Do – Check – Act),
- ISO 27004 (ISMS Metrics and Measurements) and
- ISO 27005 (ISMS Risk Management). The Management of ICT Security guidelines that will be part of this last standard will be a continuation of those listed in ISO/IEC 13335, described above.

ISO/IEC13335

The origin of ISO/IEC13335, which will provide the contents for the future ISO/IEC 27005, is in the Guidelines for the Management of IT security (GMITS), which were published in five parts between 1996 and 2001:

- In 1996, GMITS Part 1 was published, providing Concepts and Models of IT Security.
- In 1997, GMITS Part 2 followed, with information on Managing and Planning IT Security.
- GMITS Part 3, Techniques for the Management of IT Security, was published in 1998.
- GMITS Part 4, the Selection of Safeguards appeared in 1999.
- In 2001, GMITS Part 5, Management Guidance of Network Security completed the series.

In 2000, TR ISO/IEC 13335-1 was revised, and re-named MICTS, Management of ICT Security, which became an ISO/IEC standard. The structure of the former guidelines changed as well.

MICTS, Part 1 includes the former GMITS-1 and GMITS-2. As the title Concepts and Models for Managing and Planning ICT Security shows, this part focuses on concepts, objectives, strategies and policies and on the organisational aspects of ICT security, including ICT security management functions.

MICTS Part 2, the former GMITS2, GMITS3 and GMITS 4, focuses on Information Security Risk Management. Part 2 is currently a working draft.

The last set of guidelines, GMITS 5, was moved to ISO/ICT 18028, Network Security.

ISO/IEC 18028

There is a wide variety of safeguards from which IT security professionals can choose to secure their IT networks. The selection of the right safeguard determines network exposure (risks), the price/quality ratio of the network, and the flexibility to adjust to changing circumstances in a secure way. ISO 18028 provides a repository of threats, safeguards and mappings, providing organisations with common sense guidance for network security.

ISO/IEC 18028-1 provides a process approach to network security management. It offers a risk-based framework, focussing on the selection of safeguards, the types of connections, their characteristics and trust as well as potential risks. It offers guidelines for the implementation and monitoring of network security.

ISO/IEC 18028-2 proposes reference architecture. It is based on three components: security dimensions (services like access, control and authentication, but also privacy), security layers (infrastructure security layer, the services security layer and the applications security layers, like ftp, mail and http) and finally, security planes (management security plane, control security plane (signalling) and the end-user security plane).

ISO/IEC 18028-3 describes techniques for security gateways, like packet filtering, security gateway components, like switches and routers, as well as security gateway architectures (like single and multi-staging gateways). It also provides guidelines for selection and configuration of gateways and gateway components.

ISO/IEC 18028-4 describes types of and techniques for remote access connections (communication servers, LAN resources, etc). It contains guidelines for selection and configuration.

ISO/IEC 18028-5 contains an overview of VPNs and VPN security objectives and requirements. It lists guidelines for the selection and the implementation of secure VPNs (including monitoring).

ISO/IEC TR 18044

Within the ISO 27000 family, this technical report on Information Security Incident Management is part of the so-called Toolbox of Techniques. The initial draft was proposed, in 2001, and the final text was published in 2004.

TR 18044 supports incident handling controls described in ISO/IEC 17799, and provides templates and technical advice for implementing an incident handling scheme.

It also focuses also on the roles of information security managers and information system managers, the benefits of a good ISIM approach, like enhanced security and improved ROI. It includes a discussion of examples of incidents and their possible causes. TR 18044 also details the planning phase and documentation requirements for the introduction of a structured information security incident management approach, and it describes the information security management process, with information on the short- and long-term actions required. It outlines that response should always be based on previously developed, documented and accepted procedures and processes. The proposed approach for implementing adequate security incident management is based on the PDCA process model, the Plan-Do-Check-Act cycle that is at the heart of the ISO approach.



ISSA

The Information Systems Security Association (ISSA™) is an international, not-for-profit security professionals' association. The organisation sets out to be The Global Voice of Information Security. It is ISSA's mission to be "the premier authority in information security, providing international leadership, forum for sharing best practices and mentoring security professionals world-wide" (<http://www.issa.org>). The organisation wants to promote sound management and technical IT security practices by facilitating interaction and education. The organisation's key areas of interest are:

1. Executive/Board Governance: The key issues that executive management and boards of directors must know to establish and maintain information security as a necessary function of their business.
2. Industry Self-Governance, Standards and Best Practices: A set of agreed-to guidelines that the security community places on itself as a collective group, establishing criteria that should be met by all industry professionals.
3. Government and Legal Issues: Issues that must be first understood, then addressed by government and legal organizations to create national and international security policies and establish legal framework.
4. Education and Awareness: Information and advice for security professionals and end-users describing their role and responsibility to help improve Internet security on a global scale.
5. Technical Issues: Concerns of professionals that deal specifically with daily security tactics, such as product development, systems integration, networking and security administration.

In April 2005, ISSA applied for a liaison with JTC 1/SC 27, in the field of Information Security Management Systems (ISMS), Working Group 1. The collaboration agreement is currently being developed. Once this agreement has been established, ISSA chapters will contribute to the ISO standards through the national ISO bodies.

Currently, ISSA organises more than three events a year on the topic of ISO17799, which shows the organisation's interest and commitment in this area.



CobiT

In December 2005, the IT Governance Institute (ITGI) published version 4.0 of Control Objectives for Information and related Technology (CobiT). CobiT provides good practices that are based on the consensus of experts, with the objective of helping organisations optimise IT investments, ensure service delivery and provide a measure against which to judge when things do go wrong. CobiT offers a framework in which activities are presented in a manageable and logical structure. It is strongly focused on control and less on execution.

Information Security Governance

Information security governance consists of the leadership, organisational structures and processes that ensure that the enterprise's information is safeguarded. It is the responsibility of the board of directors and executive management. To be efficient, information security governance must be an integral and transparent part of enterprise governance, and fit in with the IT governance framework.

Information security governance protects organisations against the growing risk of liability claims. It also offers increased business operations predictability and stability, providing assurance concerning sound decision making processes, effective risk management and incident response practices. It allows organisations to optimise allocations of security resources and provides accountability for safeguarding information during critical business activities such as mergers and acquisitions, business process recovery, and regulatory response.

The security governance framework also instils customers' trust, adds to the organisation's reputation. Moreover, it helps organisations curb costs as risk factors causing interruption of business process are eliminated.

Framework

A governance framework or control system is a comprehensive security strategy that is explicitly linked with IT and organizational objectives. The CobiT framework supports IT governance in organisation, as it is a framework allows companies to ensure that IT is aligned with the business objectives and maximises benefits that IT resources are used efficiently and that risks are managed adequately. The framework also allows for performance measurement.

CobiT Products

The CobiT products have been structured to suit the needs of three distinct groups: executive management and boards (Board Briefing on IT Governance, 2nd Edition), business and IT management (Management Guidelines) and governance, assurance, control and security professionals. For this last group, there are several components.

One of these is the CobiT Framework, which details how CobiT organises IT governance objectives and best practices by IT domains and processes, and how these are linked to business requirements. Control Objectives provides generic best practice management objectives for all IT activities. Another one is CobiT Quickstart, for fast adoption of the most important CobiT elements, which provides a baseline of control for the smaller organisation and a first step for larger enterprises. CobiT Security Baseline, described in some more detail below, focuses on essential steps for implementing information security within the enterprise. The full list of products is represented in the CobiT Publications section of the ISACA website (<http://www.isaca.org>).

CobiT Security Baseline

CobiT Security Baseline is aimed at home users and users in small to medium sized enterprises, but also at executives and board members of larger organizations. It includes an easy to understand introduction to information security, threats and vulnerabilities. The baseline itself provides 39 control objectives, and 22 processes. It includes several Survival Kits, each aimed at a specific audience (home users,

professional users, managers and executives, senior executives and board of directors and trustees).

Case Study: ING

With about 114,000 employees in more than 50 countries, ING holds a position in the top 20 of financial institutions world-wide, and in the top 10 of financial institutions in Europe. As in many other organisations, the approach to information security evolved over the years from an event-driven approach, focussing on technology risks to a wider, structured information risk-driven approach, in which 'risk' spans both technology and information-related business risks.

The foundations of this approach were laid in 1999 when strategic decisions concerning information risk management were taken. In 2000, ING carried out a gap analysis, which was later followed by a compliance program directed at tackling the weaknesses that had been identified. In a next phase, action plans were drafted. The organisation also started developing activities concerning Sarbanes Oxley compliance.

The initial gap analysis was based on ISO controls. For each control, the current status was described and the level of compliance was assessed. Then an inventory was made of main issues, both at group level and at business unit level. Among the challenges were a lack of security awareness, both of management and of staff, issues with security governance and security structure and the lack of a global approach and interpretation.

As a result of the gap analysis, operational policies, standards and guidelines were created, as well as an information risk management organisation structure at group level. At business unit level, a security structure was set up, along with implementation projects dealing with issues that came up in the gap analysis.

Security policies were established based on ISO controls. 35 policies and standards formed the basis for 700 statements, which were translated into 2000 questions. Together, these formed a complete set of controls and measures for information security assessment. The final compliance level was based on the resulting security metrics and on deviation statements (risk acceptance).

In a next phase, an action plan was established and put into practice, with actions addressing key areas identified in the former stages, like increasing staff awareness and execution of IT control projects.

The next steps in the organisation's risk management efforts are related to operational risk management and compliance with regulations like Basel II and Sarbanes Oxley. Here too, standards like ISO and frameworks like CobiT as well as the ITIL IT Infrastructure Library are used as a basis.

The case study clearly shows how organisations can leverage the work done by standardisation bodies that offer reliable and objective guidance for assessing and reducing risk, establishing the required level of control and, equally important, capturing management interest and commitment to information security.



Conclusion

The variety of standards presented during the event provides companies and organisations with several sets of guidelines for good IT security. Rather than a competitive field, these standards make up a full range of complementary references that companies can use to improve visibility, streamline IT security approaches and comply with regulations. In addition, standards and standardisation efforts in general can function as powerful awareness raisers, bringing security to the attention of the board, as well as making it a concern for all parties involved.

—

Acronyms glossary

Overview of organisations referred to by the speakers:

ANSI X9F	American National Standards Institute	http://www.ansi.org
BCCA	Belgian Construction Certification Association	http://www.bcca.be
BELAC	Belgian Accreditation Structure	http://belac.fgov.be
BELCERT	Belgian accreditation of bodies operating certification of products, quality systems or persons	http://belac.fgov.be/belcert/home_en.htm
BELTEST	Belgian accreditation of laboratories and inspection bodies	http://belac.fgov.be/beltest/home_en.htm
BIN/IBN	Belgian Institute for Normalization	http://www.ibn.be
BSI	Bundesamt für Sicherheit in der Informationstechnik	http://www.bsi.de
CEBEC	Belgian Certification Body in the field of electrical equipment	http://www.cebex.sgs.com
CNRS	Centre National de Recherches Scientifiques	http://www.cnrs.fr
CERT	Computer Emergency Response Team	http://www.cert.org/
CERTA	Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques	http://www.certa.ssi.gouv.fr
CISSP	Certified Information Systems Security Professional	http://www.isc2.org
Clusif	Club de la Sécurité des Systèmes d'Information Français	https://www.clusif.asso.fr
CST	Communications Security Establishment	http://www.cse-cst.gc.ca
DIN	Deutsches Institut für Normung	http://www.din.de
DQS GmbH	Deutsche Gesellschaft zur Zertifizierung von Managementsystemen	http://www.dqs.de
EA	European co-operation for Accreditation	http://www.european-accreditation.org
ENISA	European Network and Information Security Agency	http://europa.eu.int/agencies/enisa/index_en.htm
EPC	European Payments Council	http://www.europeanpaymentscouncil.org
ECBS	European Committee for Banking Standards	http://www.ecbs.org
ETSI	European Telecommunications Standards Institute	http://www.etsi.org
ETSI SAGE:	Security Algorithms Group of Experts	http://portal.etsi.org/sage
FIRST	Forum of Incident Response and Security Teams	http://www.first.org
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org
IETF	Internet Engineering Task Force	http://www.ietf.org
INAB	Irish National Accreditation Board	http://www.inab.ie
IQA	Institute of Quality Assurance	http://www.iqa.org
ISACA	Information Systems Audit and Control Association	http://www.isaca.org
ISC ²	International Information Systems Security Certification Consortium	https://www.isc2.org
ISF	Information Security Forum	http://www.securityforum.org
ISO	International Organisation for Standardisation	http://www.iso.org
ISSA	Information Systems Security Association	http://www.issa.org
ISSEA	International Systems Security Engineering Association	http://www.issea.org
ITGI	IT Governance Institute	http://www.itgi.org
ITU-T	International Telecommunication Union	http://www.itu.int/ITU-T/
JIPDEC	Japan Information Processing Development Corporation	http://www.jipdec.jp
NIST	National Institute of Standards & Technology	http://www.nist.gov
BKO/OBE	Belgian Calibration Organisation	http://belac.fgov.be/OBE/home_en.htm#A
SANS	SysAdmin, Audit, Network, Security Institute	http://www.sans.org
SAS	Swiss Accreditation Service	http://www.sas.ch
UKAS	United Kingdom Accreditation Service	http://www.ukas.com