International Standardisation on IT Security

Dr. Marijke De Soete

Security4Biz
Vice Chair ISO/IEC JTC 1/SC 27 “IT Security Techniques”

Course Secure Application Development
Faculty Club Leuven
March 7th 2008
Corporate Security Governance

Security has become a fundamental component of an internal control system enabling the effective conduct and achievement of an organisation's business mission has evolved from an “exclusivity” within the IT department of a company with

- limited budget & resources
- very fragmented “reactive” approach
- lack of management buy-in towards
an inherent part of the Corporate Governance and Strategy with

- increased budget and resources
- increased awareness

- integrated “pro-active” approach
- executive & senior management control because of

- increased and new corporate responsibilities
- re-assurance of shareholders and other stakeholders (monitoring, response strategy)
- legal repercussions and damage to corporate image in case of non-compliance
Legal and Regulatory Requirements-Overview

- **EU directives**
  - Protection of personal data (95/46)
  - Privacy and electronic communications (2002/58)
  - Electronic signature (99/93)
  - Money laundering (91/308+amendments)
  - Electronic commerce (2000/31)
  - Auditing (78/660, 83/349, 84/253 +rec. 2001/256)

- **Basel Committee**
  - Risk management principles for electronic banking (July 2003)
  - Management and supervision of Cross-Border Electronic Banking Activities (July 2003)
  - The compliance function in banks (Oct 2003)
  - Basel II (June 2004)
  - Outsourcing in financial services (Aug 2004)

- **Sarbanes-Oxley**
- **Corporate governance codes & principles**
- **Gramm-Leach-Bliley Act**
- **HIPAA**
Data Protection Act
Business Information
Employee Information
Client Information
Banking Secrecy Law
Jurisdiction 1
Jurisdiction n
Digital Signature Act
Cross-border Business
External Access
Business Criticality
Legal & Regulatory Framework
Security-What is it about?

- Security is a continuous process, not a state
- Regulatory requirements will likely further increase over time
- Compliance is making IT security and forms the basis to pass a security audit for being in business
- Enterprises should make IT security an integral part of the overall business policy / corporate governance and establish a security-aware culture. This requires
  - senior management commitment
  - implementation of an ISMS (Information Security Management System)
  - employee training

- Business value of information security can be calculated on the basis of
  - risk reduction
  - reduced cost of doing business
  - return on investment via improved business opportunities
  - role in assisting enterprises to achieve and sustain a compliance environment
Standards –
Benefits and Problems

Benefits
- interoperability, open interfaces
- reduction of development time and costs
- state-of-the-art concepts and techniques
- open the market for SMEs
- transparent & democratic international consensus-oriented process

Potential problems
- standardization process takes too long
- techniques continue to develop
- IPRs (patents) versus standardization
- key players not always interested
- boring subject (?)
Standards – Return on Investment

- Benefits for cooperations
  - Risk reduction
  - Reduced cost of doing business
  - Return on investment via improved business opportunities
  - Role in assisting enterprises to achieve and sustain a compliance environment

- Economic benefits
  - The economic benefits of standardization are estimated to account for around 1% of gross domestic product (GDP)*.
  - The economic benefits of standardization are estimated to account for around 16 billion € per year for Germany**.
  - „Every investment in international standardization pays off twenty-five-fold“.

*) result of a joint study carried out by the German, Austrian and Swiss associations for standardization.

**) result of a study carried out by TU Dresden.
Defining Security Standards –
Many Players exist

- International standards bodies (e.g., ISO, ITU-T, ETSI) have formal processes
  - Procedures and processes take time
  - Progress in streamlining the time for standards approvals

- IETF processes are less formal
  - Number of participants, transparency of the processes have sometimes slowed down the work

- Industry groups and consortia focus on specific technologies and applications
  - Focus has allowed work products to be produced rapidly, although limited in scope
  - Maintenance?

⇒ Experience has shown there is a role for each organization to play in continued security standards development
Major Players – Cryptographic Mechanisms

ISO/IEC JTC 1/SC 27: Information technology - Security techniques
- standardization of generic IT security services and techniques

ETSI SAGE: Security Experts Group
- creates reports (which may contain confidential specifications) in the area of cryptographic algorithms and protocols specific to public/private telecommunications networks

IEEE P1363: Standard Specifications for Public-Key Cryptography

NIST: National Institute of Standards and Technology
- issues standards and guidelines as Federal Information Processing Standards (FIPS) for use by the US government

ANSI X9F: Data & Information Security
- standards for the financial services industry
Major Players –
*Security Protocols & Services*

IETF: Internet Engineering Task Force

ITU-T: International Telecommunication Union
- X.509 (Public-key certificates), H.235 (Security and encryption for H-Series multimedia terminals), X.841, X.842, X.843, ...

ETSI
- GSM, 3GPP, TETRA, TIPHON, SPAN, TISPAN, ...

IEEE 802.11: (Wireless) LANs
- 802.11i, 802.1X, ...
Interconnections

- **International**
  - ISO
  - IEC
  - ITU
  - 193 TCs
  - 540 SCs
  - 2,244 WGs
  - 30,000 experts

- **Regional** (e.g., Europe)
  - CEN
  - CENELEC
  - EESSI

- **National** (e.g., Germany)
  - DIN
  - DKE
  - DIN NIA
  - NIA-27

- **ETSI**
  - 32 TCs & Projects

- **TC ESI**

---

**Note:**
- DIN NIA
- NIA-27
- SC 27
Liaisons

Liaisons are partnership collaborations in the course of developing standards.

Main goals

- to ensure maximum participation and collaboration among all relevant parties
  - broad consensus
  - globally applicable standards
- to optimize the use of resources
  - cost effectiveness
  - encourage the adoption of existing work whenever possible
  - ability to support the ever growing standardization demand
- to improve the outreach of deliverables
  - extended usability in additional contexts
  - improved overall recognition of specific standardization work
International Organization for Standardization (ISO)

Worldwide federation of national standards bodies from 158 countries, one from each country, established in 1947 (www.iso.org)

Mission

- to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity.

3.041 technical bodies
  - 193 technical committees (TCs)
  - 540 subcommittees (SCs)
  - 2.244 working groups (WGs)

ISO's work results in international agreements which are published as International Standards (IS)
  - 16.455 standards and standards-type documents
  - 1.388 (68.146 pages) published in 2006
Maturity level / state of standardization

- **Study Period / New Project (NP)**
  - 2 month NP letter ballot*)
- **Working Draft (WD)**
- **Committee Draft (CD/FCD)**
  - 3 month CD ballot(s)
  - 4 month FCD ballot
- **Draft International Standard (DIS/FDIS)**
  - 2 month FDIS ballot
  - no more comments at this stage
- **International Standard (IS)**
  - review every 5 years
  - or after 'defect report'

*) one vote per P-member

average development time 2.8 years
ISO/IEC JTC 1 –
Fast Track Process

Motivation

- to allow an existing standard from any source (e.g., a National Standard) to become an International Standard

Process

- Submission by a JTC 1 member organization or a recognized PAS submitter (PAS = Publicly Available Specification)
- 6 month NB ballot (as DIS)
  - at least two thirds of the P-members voting need to approve
  - not more than one-quarter of the votes may be negative
- Ballot Resolution
  - assignment of the project to a SC
  - appointment of Project Editor
  - establishment of a ballot resolution group
- Publication
<table>
<thead>
<tr>
<th>Organization</th>
<th>Membership</th>
<th>Voting</th>
<th>Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO</td>
<td>National Bodies</td>
<td>one vote per participating NB</td>
<td>in general not available for free</td>
</tr>
<tr>
<td>IETF</td>
<td>individuals (anyone can join)</td>
<td>“rough consensus and running code”</td>
<td>available for free</td>
</tr>
<tr>
<td>ETSI</td>
<td>organizations</td>
<td>weighted voting</td>
<td>available for free (since 1999)</td>
</tr>
<tr>
<td>ANSI</td>
<td>organizations</td>
<td>one vote per member</td>
<td>in general not available for free</td>
</tr>
<tr>
<td>NIST</td>
<td>Government agency, not a membership organization</td>
<td></td>
<td>available for free</td>
</tr>
</tbody>
</table>
ISO/IEC JTC 1 “Information Technology” – Security Related Sub-committees

- SC 6  Telecommunications and information exchange between systems
- SC 7  Software and system engineering
- **SC 17 Cards and personal identification**
- SC 25  Interconnection of information technology equipment

**SC 27 Information technology security techniques**

- SC 29  Coding of audio, picture, multimedia and hypermedia information
- SC 31  Automatic identification and data capture techniques
- SC 32  Data management and interchange
- SC 36  Information technology for learning, education and training
- **SC 37 Biometrics**
ISO/IEC JTC 1/SC 27 “IT Security Techniques”
Scope & Organization

Standardization of generic methods, techniques and guidelines for information, IT and communication security. This includes the following areas:

- requirements capture methodology;
- security techniques and mechanisms, including procedures for the registration of security components;
- management of information, IT and communication security;
- management support documentation, including terminology;
- conformance assessments and security evaluation criteria standards.

SC27 engages in active liaison and collaboration with appropriate bodies to ensure proper development and application of SC27 standards and technical reports in relevant areas.
**Membership of SC 27**

<table>
<thead>
<tr>
<th>Brazil</th>
<th>Belgium</th>
<th>France</th>
<th>Netherlands</th>
<th>Sweden</th>
<th><strong>DG8</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Denmark</td>
<td>Germany</td>
<td>Norway</td>
<td>Switzerland</td>
<td>China</td>
</tr>
<tr>
<td>USA</td>
<td>Finland</td>
<td>Italy</td>
<td>Spain</td>
<td>UK</td>
<td>Japan</td>
</tr>
</tbody>
</table>

*Founding P-Members (in 1990)*

<table>
<thead>
<tr>
<th>Russian Federation</th>
<th>South Africa</th>
<th>Kenya</th>
<th>Cyprus</th>
<th>Kazakhstan</th>
<th>Korea</th>
<th>Ukraine</th>
<th>Malaysia</th>
<th>Austria</th>
<th>New Zealand</th>
<th>South Africa</th>
<th>Kenya</th>
<th>Cyprus</th>
<th>Kazakhstan</th>
<th>Korea</th>
<th>Ukraine</th>
<th>Malaysia</th>
<th>Austria</th>
<th>New Zealand</th>
<th>South Africa</th>
<th>Kenya</th>
<th>Cyprus</th>
<th>Kazakhstan</th>
<th>Korea</th>
<th>Ukraine</th>
<th>Malaysia</th>
<th>Austria</th>
<th>New Zealand</th>
</tr>
</thead>
</table>

*Additional P-Members (total: 35)*

**O-members** (total: 13)

- Argentina, Hong Kong, Indonesia, **Belarus**, Estonia, Hungary, Ireland, Israel, Lithuania, Serbia and Montenegro, Romania, Slovakia, Turkey
Selected Liaisons

- SC37
- SC17
- ITU-T
- TC65
- ISSA
- ISSEA
- TC68
- EPC

Categories:
- Telecoms
- Banking
- Healthcare
- Safety
- Biometrics
- IC cards
- Information security
- EPC
SC 27 – Evolving Structure

WG 1
“Security Guidelines”

WG 2
“Cryptography & Security Mechanisms”

WG 3
“Security Evaluation”

WG 4
“Security Controls & Services”

WG 5
“Identity Management & Privacy Technologies”

WGs in italics are new
## Hierarchical Security Management Model (SC 27 View)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology</td>
<td></td>
</tr>
<tr>
<td>Principles</td>
<td>provide generally accepted high-level basic rules used as a foundation to guidance</td>
</tr>
<tr>
<td>Frameworks</td>
<td>provide a simplified description of interrelationships used to organize concepts, methods and technologies</td>
</tr>
<tr>
<td>Element Standards</td>
<td>provide specific requirements that apply to a defined area of security management</td>
</tr>
<tr>
<td>Application Guides and Supplements</td>
<td>provide detailed descriptions offering guidance on how element standards may be applied in specific situations</td>
</tr>
<tr>
<td>Toolbox of Techniques</td>
<td></td>
</tr>
</tbody>
</table>

- Identification of requirements for future ISMS standards and guidelines
- Liaison and collaboration with those organizations and committees dealing with specific requirements and guidelines for ISMS, e.g.:
  - ITU-T (Telecoms)
  - TC 215 (Healthcare)
  - TC 68 (Financial Services)
  - TC 204 (Transportation) [in process]
  - World Lottery Association (Gambling) [in process]
ISO/IEC 27000 – ISMS series of Standards

ISO/IEC 27001
ISMS Requirements

ISO/IEC 27000
ISMS Fundamentals and Vocabulary

ISO/IEC 27002 (pka 17799)
Code of Practice

ISO/IEC 27006
Accreditation Requirements

ISO/IEC 27007
ISMS Auditing Guidance

ISO/IEC 27004
Information Security Management Measurements

ISO/IEC 27005
ISMS Risk Management

ISO/IEC 27003
ISMS Implementation Guidance

supports, adds value, contributes and gives advice on ISO/IEC 27001 requirements and their implementation
Published 15th Oct 2005

A specification for 3rd party certifications

Risk management approach
  - risk assessment
  - risk treatment
  - management decision making

Continuous improvement model

Replaces BS 7799 Part 2
Benchmark for measuring internal security

Building customer confidence & trust

Business Enabler

Marketing & market presence

Compliance with legislation

Auditable specification (internal and external ISMS auditing)
PDCA ISMS Model

ISMS Life Cycle

- **Plan**
  - Design ISMS

- **Do**
  - Implement & deploy ISMS

- **Check**
  - Monitor & review ISMS

- **Act**
  - Maintain & improve ISMS
Implement risk management processes to achieve an effective ISMS through a continual improvement process.
Code of Practice for Information Security Management

The new number given to IS 17799 mid 2007

Published 15th June 2005

Management, policy, procedural, physical and technical controls

Controls are selected according to the risk management process specified in 27001

It is a catalogue of best practices, suggesting a holistic set of controls and hence NOT a certification or auditable standard
IS 27002 Selection of Controls
Objective: provide implementation guidance to support the ISMS requirements standard 27001

Detailed advice and guidance regarding the PDCA processes e.g.

- ISMS Scope and policy
- Identification of assets
- Implementation on selected controls
- Monitoring and review
- Continuous improvement

Current status Working Draft (WD)
Objective to develop an Information security management measurements standard aimed at addressing how to measure the EFFECTIVENESS of ISMS implementations (processes and controls)

- Performance targets, benchmarking …
- What, how and when to measure?
- Performance, benchmarking, monitoring and review of the ISMS effectiveness to help with business decision making and improvements to the ISMS
- Current status third CD
IS 27005 Risk Management

- Guidance on ISMS risk management to support the risk assessment, treatment and management, and the selection of controls requirements defined in 27001
- Detailed guidance for ISMS implementers, risk managers, security officers …
- Current status final CD
IS 27006 Accreditation Requirements

- ISMS Accreditation Requirements
- Requirements for bodies providing audit and certification of information security management systems
- Specific ISMS requirements to complement the generic requirements in ISO 17021-1
- Replaces EA 7/03
- Published February 2007
Specific ISMS guidance to complement ISO 19011

Dealing with guidance for auditors on subjects such as

- Establishing ISMS audit trails
- Auditing forensics
- ISMS scopes
- Measurements
IS 27000 Principles and Vocabulary

- Includes a reference model for the 27000 series
- Current status third CD
Large, medium & small business enterprises
In every commercial & industry sector

- Banks, financial institutions, insurance
- Telecoms companies, network service providers
- Petroleum, electricity, gas & water companies
- IT manufactures
- Retail organisations
- Publishing companies
- Government departments

(e.g., see www.certificationeurope.com)
27001 Certification

International Register of ISMS Certificates

Certificate Register

Certificate Search page

International ISMS Register

Results of Your Certificate Query: (click here to go back to the Search Page)

<table>
<thead>
<tr>
<th>Name of the Organization</th>
<th>Country</th>
<th>Certificate Number</th>
<th>Certification Body</th>
<th>Standard ISO 15002</th>
</tr>
</thead>
<tbody>
<tr>
<td>A&amp;I System Co., Ltd.</td>
<td>Japan</td>
<td>021-1</td>
<td>JICQA</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>AAD Co., Ltd.</td>
<td>Japan</td>
<td>U01075 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>ABK Consulting Ltd.</td>
<td>Japan</td>
<td>U01048 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>Access Co., Ltd.</td>
<td>Japan</td>
<td>U00756 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>Acuvate Co., Ltd.</td>
<td>Japan</td>
<td>U01632 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>Act Co Ltd</td>
<td>Japan</td>
<td>U01654 (IS 9811)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>ADECO LTD.</td>
<td>Japan</td>
<td>020-1</td>
<td>JICQA</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>Administrative System Kyushu Co., Ltd.</td>
<td>Japan</td>
<td>U01043 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>ADOC INTERNATIONAL Co., Ltd.</td>
<td>Japan</td>
<td>0038127 (IS 9001)</td>
<td>JACO-2S</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>AEON Co., Ltd.</td>
<td>Japan</td>
<td>U01605 (IS 9001)</td>
<td>BSI-J</td>
<td>BS 7799-1</td>
</tr>
<tr>
<td>AEON Credit Service Co. Ltd.</td>
<td>Japan</td>
<td>D000-MT018</td>
<td>JQA</td>
<td>BS 7799-1</td>
</tr>
</tbody>
</table>

Some certified organizations have also given the scope of their ISMS - click here to search for all ISMS scopes.
ISMS Service Standards
Disaster Recovery
Business Continuity
IT network services
TTP services
Cyber security
Forensics etc

Supporting documents for services

27000 ISMS Standards
27000-27007
### Security Controls and Services *(new WG 4)* – Scope

<table>
<thead>
<tr>
<th>Category</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Readiness for BC, DR, &amp; ER</td>
<td>NP; possibly include ISO/IEC 24762, Vulnerability Mgmt, IDS, &amp; Incident Response related standards</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>Anti-Spyware, Anti-SPAM, Anti-Phishing, NP 27032</td>
</tr>
<tr>
<td>Network Security</td>
<td>ISO/IEC 18028 revision</td>
</tr>
<tr>
<td>Application Security</td>
<td>NP 27034</td>
</tr>
<tr>
<td>TTP Services Security</td>
<td>includes outsourcing and offshoring security</td>
</tr>
<tr>
<td>Forensic Investigation</td>
<td>future NP</td>
</tr>
</tbody>
</table>
ISO/IEC 18044

Information security incident handling management

- Supports incident handling controls in ISO/IEC 27002
- Provides templates and more technical advice on how to implement incident handling schemes
- Published 2005
Disaster Recovery Services

- Working draft was based on the Singapore Standard SS 507 Standard for disaster recovery service providers
- To be published
Information security management system (ISMS) [27001]

ISMS Overview & terminology [27000]
Information security controls (ex17799) [27002]
ISMS Implementation guide [27003]
Information security management measurements [27004]
ISMS Risk management [27005]

Accreditation requirements for ISMS [27006]

Telecoms requirements [27011]
Automotive requirements [2701x]
Transport requirements [2701x]
Healthcare requirements [270xx/27799]
WLA requirements [2701x]
Financial systems requirements [2701x]

Product & system security evaluation & assurance

Disaster recovery, IT networks security, TTP services, IDS, Incident handling, Web applications, identity management, cyber ...

Cryptographic techniques, authentication protocols, biometric techniques, privacy technologies …

Accreditation requirements [17021]
Audit guidelines [19011 & 27007]
Hierarchical Security Management Model
(SC 27 View)

<table>
<thead>
<tr>
<th>Terminology</th>
<th>ISO Guide 73</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles</td>
<td>Information Security Management Implementation Guidance (NP 27003)</td>
</tr>
<tr>
<td>Frameworks</td>
<td>MICTS-1: Models and concepts</td>
</tr>
<tr>
<td>Element Standards</td>
<td>ISMS Requirements (NP 27001)</td>
</tr>
<tr>
<td></td>
<td>Code of Practice for ISM (IS 17799 / ITU-T X.1051)</td>
</tr>
<tr>
<td></td>
<td>MICTS-2: Risk management</td>
</tr>
<tr>
<td>Application Guides and Supplements</td>
<td>IS 19011 Auditing</td>
</tr>
<tr>
<td></td>
<td>Financial ISMS Guide (TC 68)</td>
</tr>
<tr>
<td></td>
<td>T-ISMS: Telecom ISMS Guide (ITU-T X.1051)</td>
</tr>
<tr>
<td></td>
<td>Healthcare ISMS Guide (TC 215)</td>
</tr>
<tr>
<td>Toolbox of Techniques</td>
<td>Info Security Incident Management (TR 18044)</td>
</tr>
<tr>
<td></td>
<td>IT Intrusion Detection Framework (TR 15947)</td>
</tr>
<tr>
<td></td>
<td>IT Network Security (IS 18028 / ITU-T X.???)</td>
</tr>
<tr>
<td></td>
<td>Guidelines for TTP Services (IS 14516 / ITU-T X.842)</td>
</tr>
</tbody>
</table>
Recent SC 27 Publications –
WG 1 & WG 4

- ISO/IEC 18028: IT network security –


Information Security Management Guidelines – Overview

**ISF (Information Security Forum)**

**COSO** – Committee of Sponsoring Organizations of the Treadway Commission (Internal control framework– Enterprise risk management framework)

**IT Governance Institute** (Information Security governance)  
(www.ITgovernance.org) – Cobit

**OECD**

**FFIEC** (Federal Financial Institutions Examination Council)
Non-profit association
Widely recognised as being a dominant force in Information Security
Incepted 1989

<table>
<thead>
<tr>
<th>Industry</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering, manufacturing &amp; mining</td>
<td>43</td>
</tr>
<tr>
<td>Financial services and insurance</td>
<td>90</td>
</tr>
<tr>
<td>Transport</td>
<td>11</td>
</tr>
<tr>
<td>Chemicals, healthcare, pharmaceuticals</td>
<td>28</td>
</tr>
<tr>
<td>Telecommunications and post</td>
<td>26</td>
</tr>
<tr>
<td>Utilities and government</td>
<td>21</td>
</tr>
<tr>
<td>Suppliers of consultancy and services</td>
<td>30</td>
</tr>
<tr>
<td>Retail and lottery</td>
<td>7</td>
</tr>
</tbody>
</table>

TOTAL: 256

E-mail: info@securityforum.org
Web: www.securityforum.org
The Standard of Good Practice (complimentary download): www.isfsecuritystandard.com
Guidelines - COSO

**Control Environment**
- Sets tone of organization-influencing control consciousness of its people.
- Factors include integrity, ethical values, competence, authority, responsibility.
- Foundation for all other components of control.

**Information and Communication**
- Pertinent information identified, captured and communicated in a timely manner.
- Access to internal and externally generated information.
- Flow of information that allows for successful control actions from instructions on responsibilities to summary of findings for management action.

**Monitoring**
- Assessment of a control system’s performance over time.
- Combination of ongoing and separate evaluation.
- Management and supervisory activities.
- Internal audit activities.

**Risk Assessment**
- Risk assessment is the identification and analysis of relevant risks to achieving the entity’s objectives-forming the basis for determining control activities.

**Control Activities**
- Policies/procedures that ensure management directives are carried out.
- Range of activities including approvals, authorizations, verifications, recommendations, performance reviews, asset security and segregation of duties.

All five components must be in place for a control to be effective.
Recent SC 27 Publications – WG 2

- ISO/IEC 9796: Digital signatures giving message recovery –


- ISO/IEC 11770: Key management –

- ISO/IEC 14888: Digital signatures with appendix –

- ISO/IEC 18033: Encryption algorithms –
  - Part 3: Block ciphers, 2005.
SC 27 Standards – Security Evaluation

Methodology for IT Security Evaluation (IS 18045)

Framework for IT Security Assurance (TR 15443)

Protection Profile Registration Procedures (IS 15292)

Evaluation Criteria for IT Security (“Common Criteria”) (IS 15408)

Systems Security Engineering – Capability Maturity Model (IS 21827)

Security Assessment of Operational Systems (TR 19791)

Guide on the Production of Protection Profiles & Security Targets (TR 15446)

Security Requirements for Cryptographic Modules (IS 19790)

Test Requirements for Cryptographic Modules (IS 24759)
Recent SC 27 Publications –
WG 3

- ISO/IEC 15408: Evaluation criteria for IT security –

- ISO/IEC TR 15443: A framework for IT security assurance –


Identity Management & Privacy Technologies (*new* WG5) – Scope

Scope covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data. This includes:

- Current projects
  - A framework for Identity Management (ISO/IEC WD 24760)
  - Biometric template protection (ISO/IEC WD 24745)
  - Authentication context for biometrics (ISO/IEC CD 24761)
  - A privacy framework (ISO/IEC WD 29100)
  - A privacy reference architecture (NP 29101)
  - Authentication assurance (ISO/IEC WD 29115)

- Identification of requirements for and development of future standards and guidelines in these areas.
New Projects include:
- ISO/IEC CD 27011 (= ITU-T X.1051): Information security management guidelines for telecommunications
- NP 29128: Verification of cryptographic protocols
- NP 27031: ICT readiness for business continuity
- NP 27032: Guidelines for cybersecurity
- NP 27034: Guidelines for application security

Study Periods include
- Sector-specific ISMS standards for the automotive industry
- Sector-specific ISMS standards for e-governments
- Object identifiers and ASN.1 syntax
- Light-weight encryption
- Three party entity authentication
- Signcryption
- Merge of ISO/IEC 9796 and ISO/IEC 14888
SC 27 is responsible for
  - ~ 90 projects, including ~ 45 active projects
Between 1990 and today, SC 27 has published
  - 60+ International Standards (IS) and Technical Reports (TR)

Next Meetings
  - April 2008 Kyoto (Japan) WGs & Plenary
  - October 2008 Lemesos (Cyprus) WGs

More Information & Contact
  - SC 27 web-page: scope, organization, work items, etc.  
    http://www.jtc1sc27.din.de/en
  - SD7: Catalogue of SC 27 Projects & Standards
  - SC 27 Secretariat: Krystyna.Passia@din.de
ISO TC 215 “Health Informatics” –
Selected Security Activities

- ISO 17090: Health informatics - Public key infrastructure
  - Part 1: Framework and overview, 2002
  - Part 2: Certificate profile, 2002
  - Part 3: Policy management of certification authority, 2002
- ISO 20301: Health informatics - Health cards - General characteristics, 2006
- ISO 21549: Health informatics - Patient health card
  - Part 1: General structure, 2004
  - Part 2: Common objects, 2004
  - Part 3: Limited clinical data, 2004
  - Part 4: Extended clinical data, 2006
  - Part 7: Medication data, 2007
- ISO TS 22600: Health informatics - Privilege management and access control
  - Part 1: Overview and policy management, 2006
  - Part 2: Formal models, 2006
- ISO/DIS 27799 Health informatics –
  Information security management in health using ISO/IEC 17799
Conclusion

- The good news about (security) standards is … … there are so many to choose from ….

- Given the limited availability of resources for the development of security standards, we must avoid duplication of effort and make use of effective cooperation and collaboration.

- Standards development does not always take sufficient account of coordination and of stakeholder needs and views:
  - ISO Strategic Advisory Group on Security (SAG-S)
  - Network and Information Security Steering Group (NISSG)
  - ICT Security Standards Roadmap

- **Warning**: ISMS Model (“Plan-Do-Check-Act”) applies to standardization as well.
Thank You

marijke.desoete@pandora.be