



The ISO 27000 series for IT Security Management

Dr. Marijke De Soete
Security4Biz
Vice Chair ISO/IEC JTC 1/SC 27 “IT Security Techniques”

L-Sec Seminar
February 12th 2008
Brussels



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

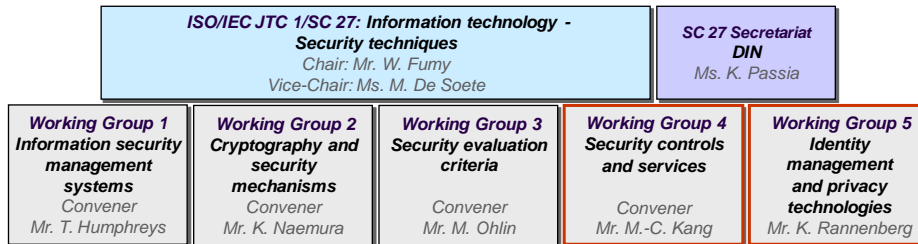


ISO/IEC JTC 1/SC 27 “IT Security Techniques” Scope & Organization

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



3



Membership of SC 27

Brazil	Belgium	France	Netherlands	Sweden	USSR
Canada	Denmark	Germany	Norway	Switzerland	China
USA	Finland	Italy	Spain	UK	Japan

founding P-Members (in 1990)

			South Africa	Kenya		Cyprus
Russian Federation						Kazakhstan
Korea		Ukraine	Malaysia	Austria	New Zealand	Uruguay
Australia	Poland	Czech Republic	India	Luxembourg	Singapore	Sri Lanka
1994	1996	1999	2001	2002	2003	2005-07

additional P-Members (total: 35)

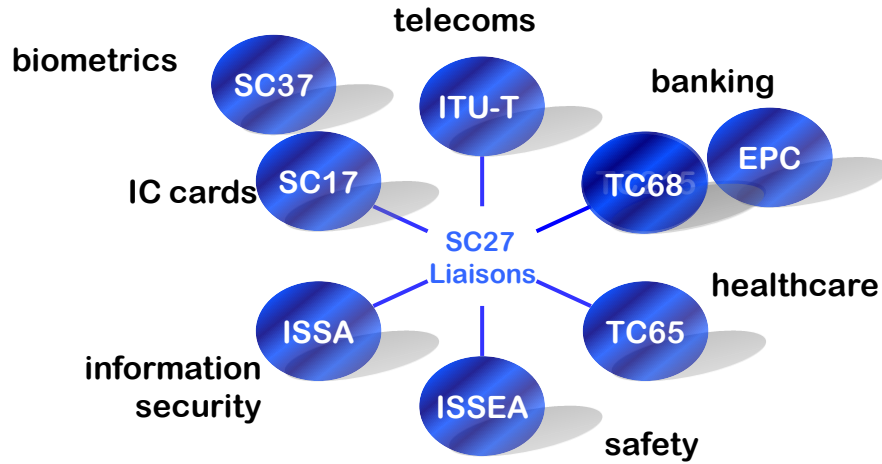
O-members (total: 13)

- Argentina, Hong Kong, Indonesia, [Belarus](#), Estonia, Hungary, Ireland, Israel, Lithuania, Serbia and Montenegro, Romania, Slovakia, Turkey

4



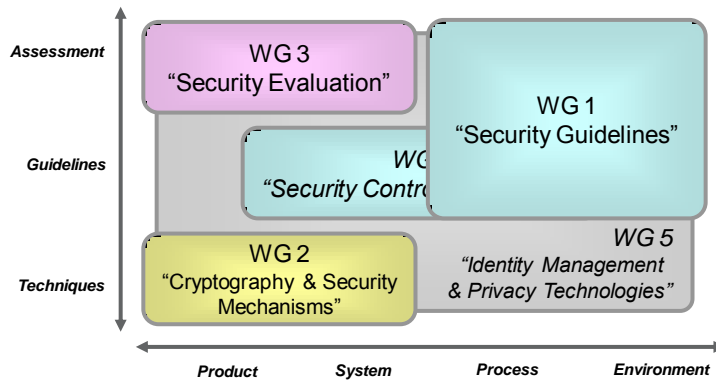
Selected Liaisons



5



SC 27 – Evolving Structure

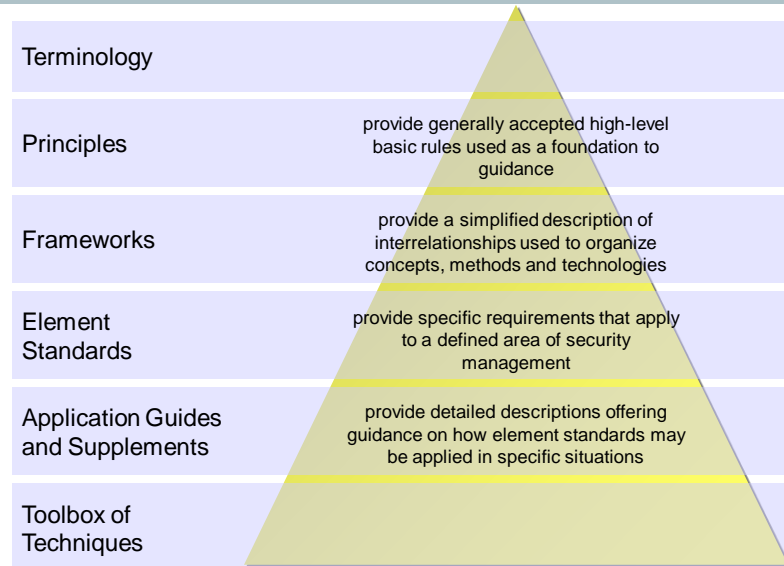


WGs in *italics* are new

6



Hierarchical Security Management Model (SC 27 View)



7



Information Security Management Systems

ISO/IEC JTC 1 SC27/ WG 1 covers the development of Information Security Management System (ISMS) standards and guidelines.

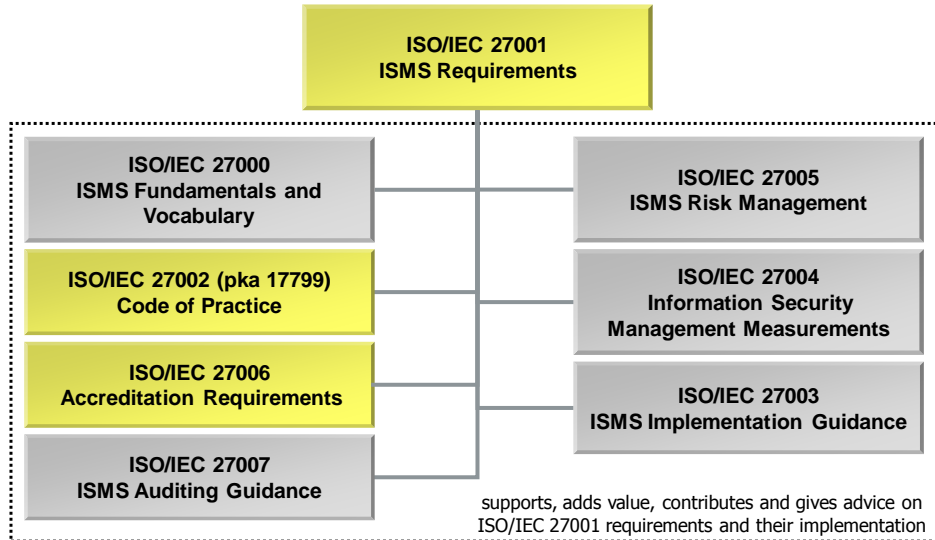
Development and maintenance of the ISO/IEC 27000 ISMS standards family

- 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]*

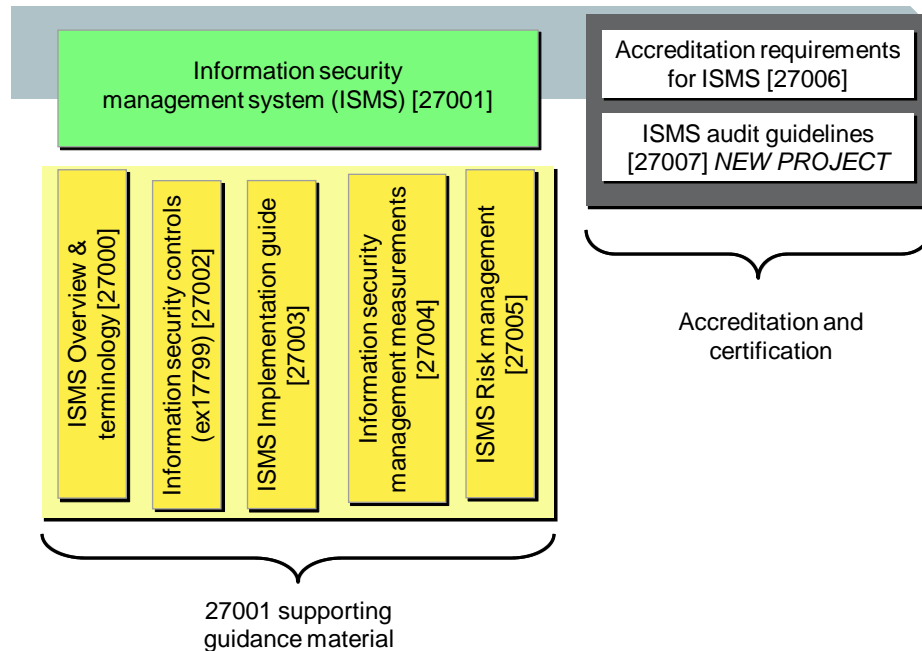
8



ISO/IEC 27000 – ISMS series of Standards



9



10

IS 27001 ISMS Requirements (1)

- 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

11

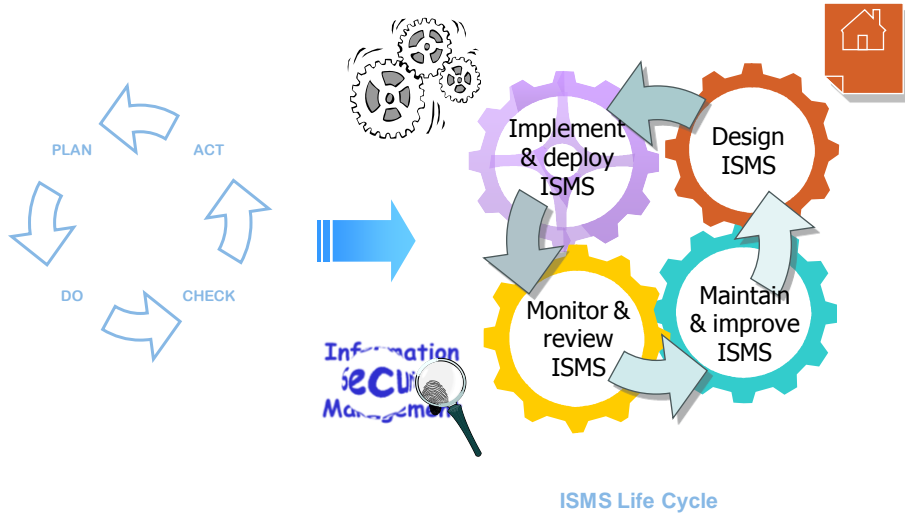
IS 27001 ISMS Requirements (2)

- Benchmark for measuring internal security
- Building customer confidence & trust
- Business Enabler
- Marketing & market presence
- Compliance with legislation

- Auditable specification (internal and external ISMS auditing)

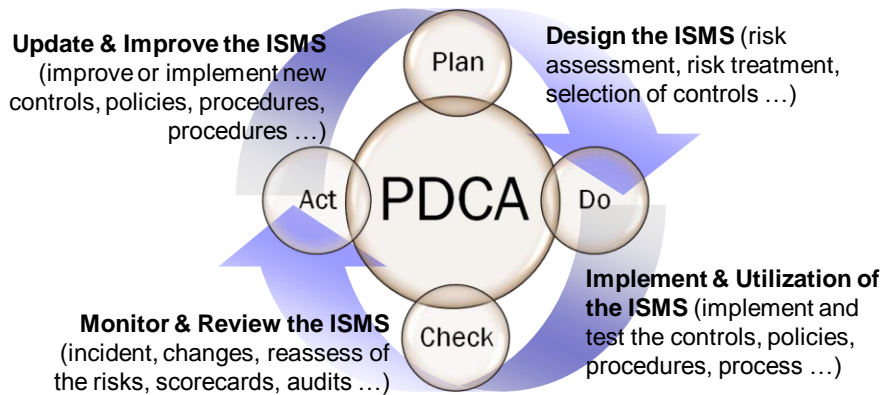
12

PDCA ISMS Model



13

Information Security Management System (ISMS) Process Model



Implement risk management processes to achieve an effective ISMS through a continual improvement process

14
14

IS 27002 Code of Practice (1)



- 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

15

IS 27002 Selection of Controls



16

IS 27003 ISMS Implementation

- 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)

17

IS 27004 ISM measurements



- 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

18

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

19

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

20

IS 27007 ISMS Audit Guidelines – **New project**

- 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

21

IS 27000 Principles and Vocabulary

- Includes a reference model for the 27000 series
- Current status third CD

22

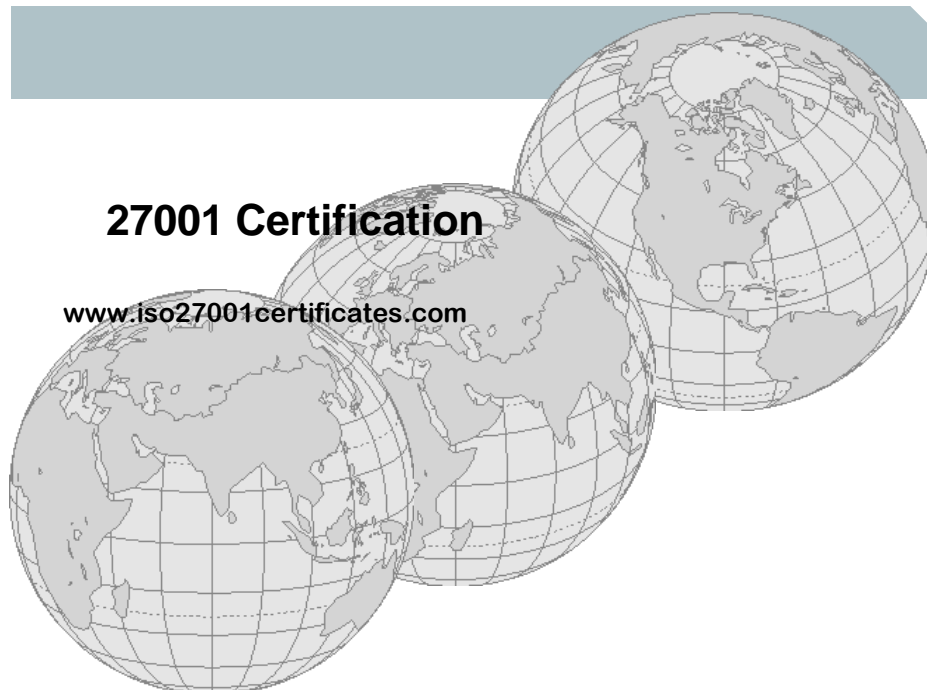
27001 Certification

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)

23



24

27001 Certification

The screenshot displays the 'International Register of ISMS Certificates' website. The main content area is titled 'Certificate Search page' and shows 'Results of Your Certificate Query'. Below this is a table with the following data:

Name of the Organization	Country	Certificate Number	Certification Body	Standard
JA&I System Co., Ltd.	Japan	021-1	JICQA	BS 7799-
JAAD Co., Ltd.	Japan	U 01703 (IS 98440)	BSI-J	BS 7799-
JABeam Consulting Ltd.	Japan	U 01486 (IS 95275)	BSI-J	BS 7799-
Accès Co., Ltd.	Japan	U 00754 (IS 79202)	BSI-J	BS 7799-
Accutechs Co., Ltd.	Japan	U 01637 (IS 95617)	BSI-J	BS 7799-
Act Co Ltd	Japan	U 00504 (IS 78611)	BSI-J	BS 7799-
ADECCO LTD	Japan	KDS-1	JICQA	BS 7799-
Administrative System Kyushu Co., Ltd.	Japan	U 01043 (IS 87613)	BSI-J	BS 7799-
ADOC INTERNATIONAL Co., Ltd.	Japan	IC05.0127 (005.0127)	JACO-IS	BS 7799-
AEON Co., Ltd.	Japan	U 01603 (IS 96310)	BSI-J	BS 7799-
AEON Credit Service Co., Ltd.	Japan	JQA-IMD178	JQA	BS 7799-

Below the table, there is a link: 'Some certified organizations have also given the scope of their ISMS - click here to search for all ISMS scopes:' followed by a 'Send Query' button.

25



26



Security Controls and Services (*new* WG 4) – Scope

ICT Readiness for BC, DR, & ER	NP; possibly include ISO/IEC 24762, Vulnerability Mgmt, IDS, & Incident Response related standards
Cyber Security	Anti-Spyware, Anti-SPAM, Anti-Phishing, NP 27032
Network Security	ISO/IEC 18028 revision
Application Security	NP 27034
TTP Services Security	includes outsourcing and offshoring security
Forensic Investigation	future NP

27

ISO/IEC 18044

Information security incident handling management

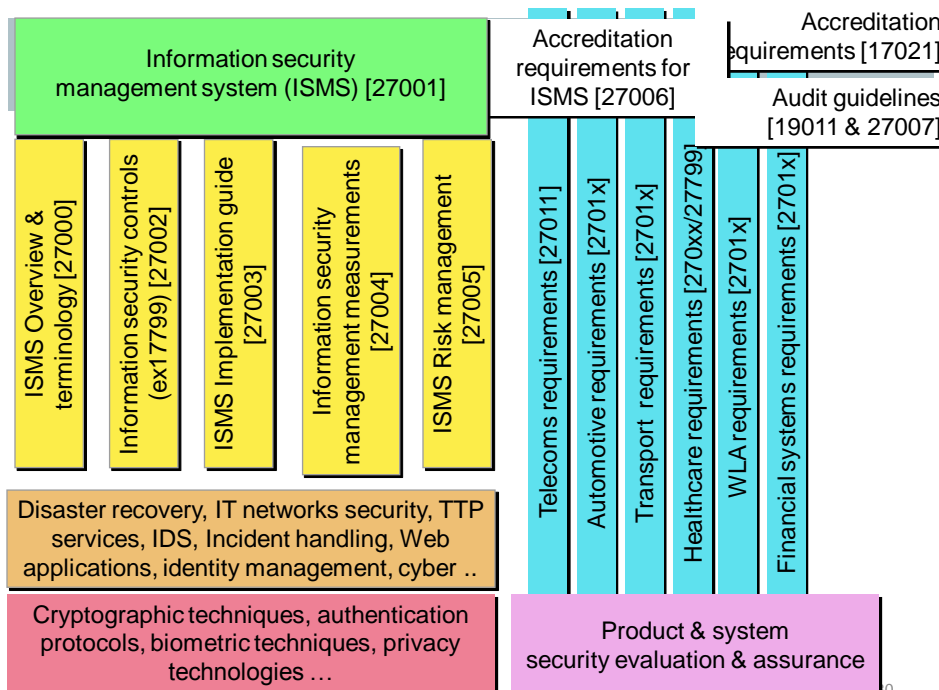
- Supports incident handling controls in ISO/IEC 27002
- Provides templates and more technical advice on how to implement incident handling schemes
- Published 2005

28

Disaster Recovery Services

- Working draft was based on the Singapore Standard SS 507 Standard for disaster recovery service providers
- To be published

29



30



Study Periods & New Projects

New Projects include:

- ISO/IEC FDIS 27011 (= ITU-T X.1051): *Information security management guidelines for telecommunications*
- NP 27031: *ICT readiness for business continuity*
- NP 27032: *Guidelines for cyber security*
- NP 27034: *Guidelines for application security*

Study Periods include

- *Sector-specific ISMS standards for the automotive industry*
- *Sector-specific ISMS standards for e-governments*

31



SC 27 – Summary

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
- SC 27 Chairman: Walter.Fumy@siemens.com
- SC 27 Vice Chair: marijke.desoete@pandora.be

32



Thank You

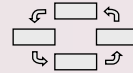
marijke.desoete@pandora.be



Towards a Benelux ISMS User Group

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



35

International take-up of IS 2700x

Businesses in Europe, the Americas and Asia-Pacific are using and applying the IS 2700x family

- Telecoms
- Finance and insurance
- Third party services
- Manufacturing
- IT industry
- Automotive
- Government
- SMEs

36

ISMS International User Group

Established in 1997 (www.17799.com)

Promotes the use of the standards IS 2700x family

Sharing of user experiences

Produces periodical Journal

Promotes Global events, workshops and seminars

Several national Chapters

- Australia, Brazil, Canada, Germany, Hong Kong, Italy, Japan, Korea, Norway, Poland, Singapore, Sweden, UK, USA,....