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

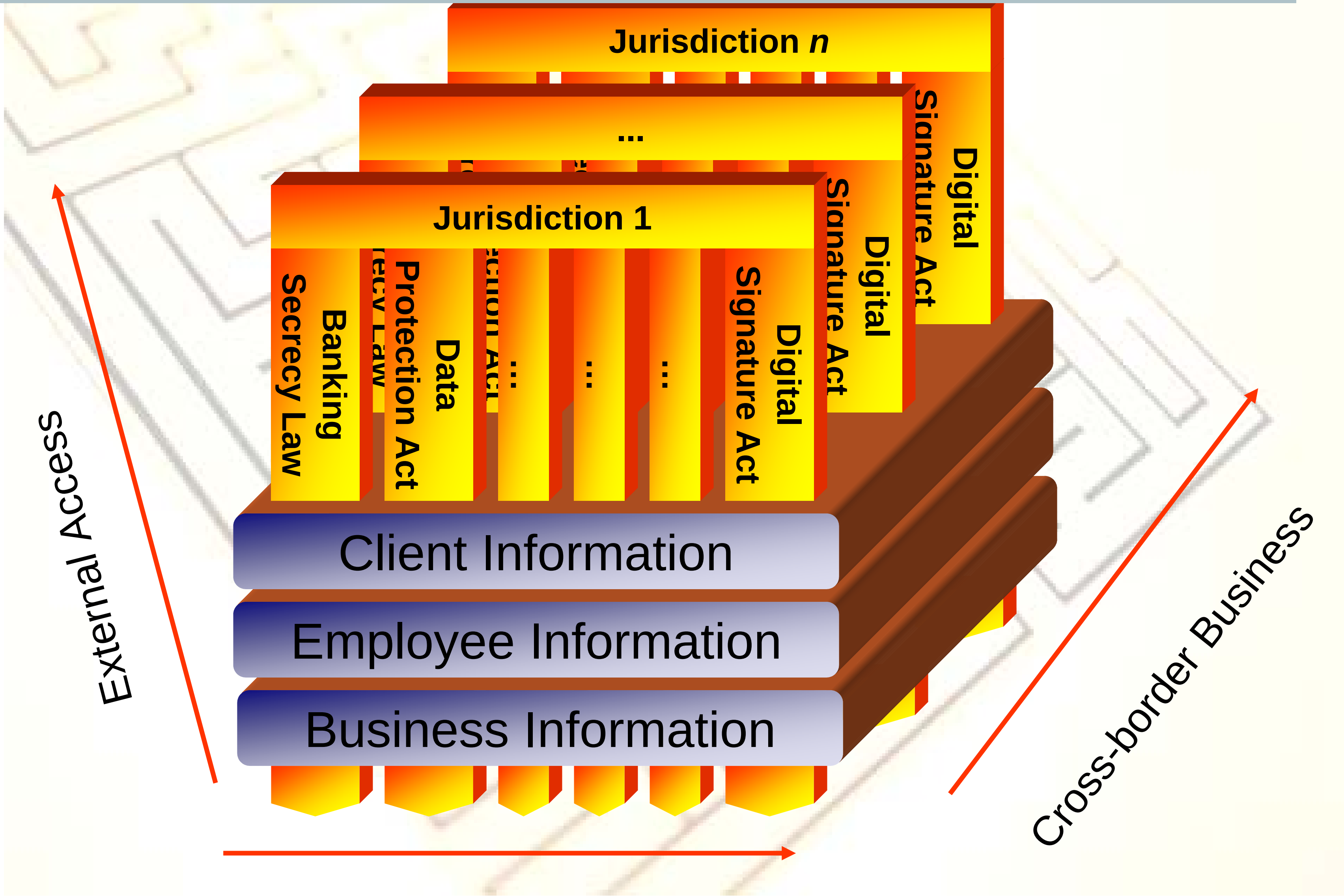
because of

- 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**

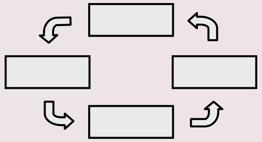
Legal & Regulatory Framework



Business Criticality

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

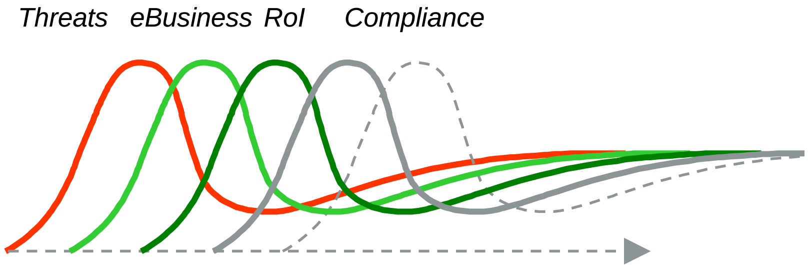
- interoperability, open interfaces
- reduction of development time and costs
- state-of-the-art concepts and techniques
- open the market for SMEs
- transparent & democratic international consensus-oriented process

Potential problems

- standardization process takes too long
- techniques continue to develop
- IPRs (patents) versus standardization
- key players not always interested
- boring subject (?)

ISO 9796, ISO 9797, ISO 9798, ISO 9979, ISO 10116, ISO 10118, ISO 10770, ISO 13355, ISO 13888, ISO 14888, ISO 15408, ISO 15946, ISO 18032, ISO 18033, ISO 18034, ISO 18043, ISO 18045, ISO 18046, ...

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

- IP Security Protocol, Transport Layer Security, Public-Key Infrastructure (X.509), S/MIME Mail Security,...

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, ...

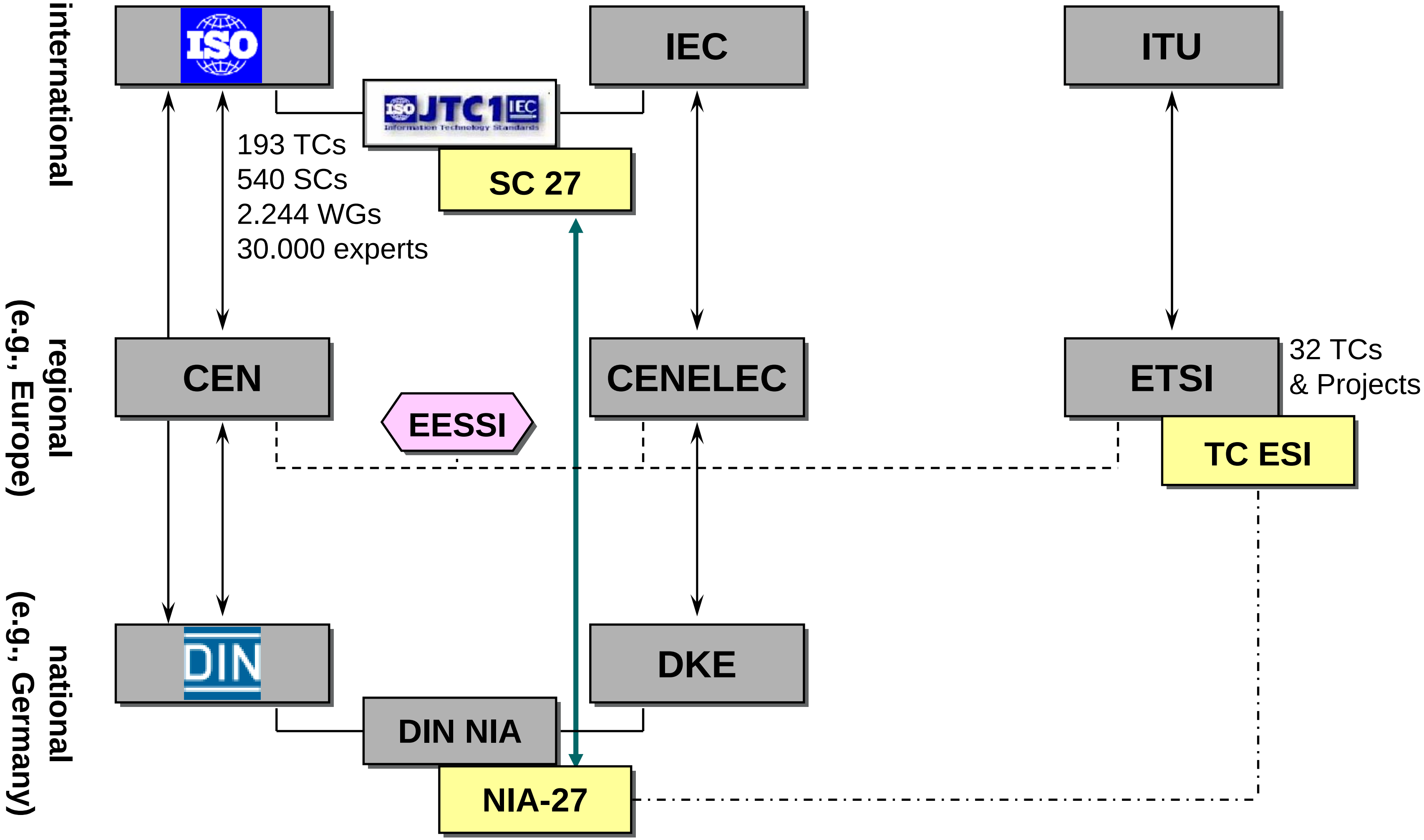
ETSI

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

IEEE 802.11: (Wireless) LANs

- 802.11i, 802.1X, ...

Interconnections

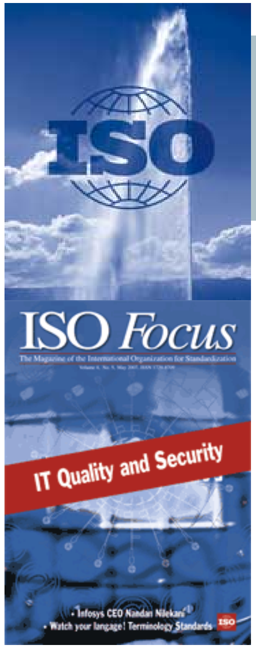


Liaisons

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


ISO
ISO Focus
The Magazine of the International Organization for Standardization
IT Quality and Security
• Infosys CEO Nandan Nilekani
• Watch your language! Terminology Standards
ISO

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)

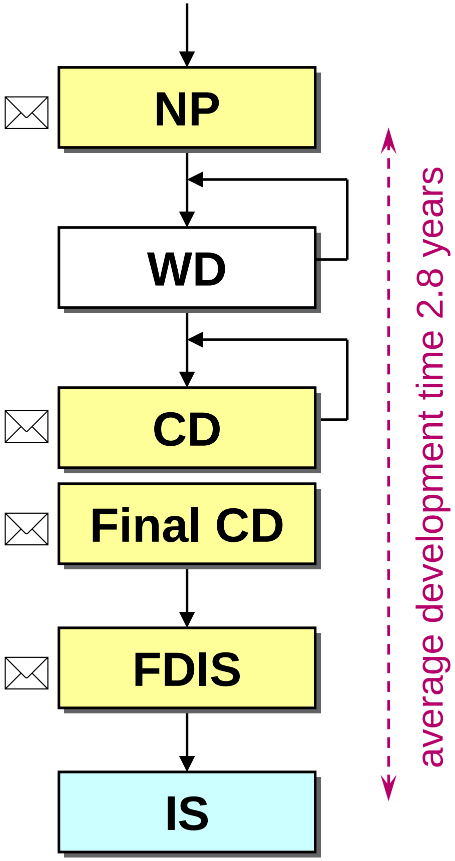
ISO's work results in international agreements which are published as International Standards (IS)

- 16.455 standards and standards-type documents
- 1.388 (68.146 pages) published in 2006

ISO –
Standardization Process

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**

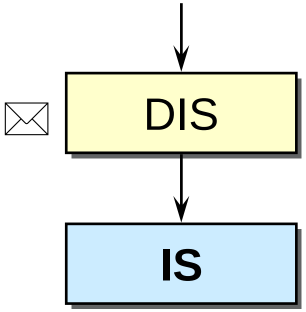
ISO/IEC JTC 1 – *Fast Track Process*

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



A Standard
is a Standard is a Standard ...

	Membership	Voting	Publications
ISO www.iso.ch	National Bodies	one vote per participating NB	in general not available for free
IETF www.ietf.org	individuals (anyone can join)	“rough consensus and running code”	available for free
ETSI www.etsi.org	organizations	weighted voting	available for free (since 1999)
ANSI www.ansi.org	organizations	one vote per member	in general not available for free
NIST www.nist.gov	Government agency, not a membership organization		available for free

ISO/IEC JTC 1 “Information Technology” – *Security Related Sub-committees*

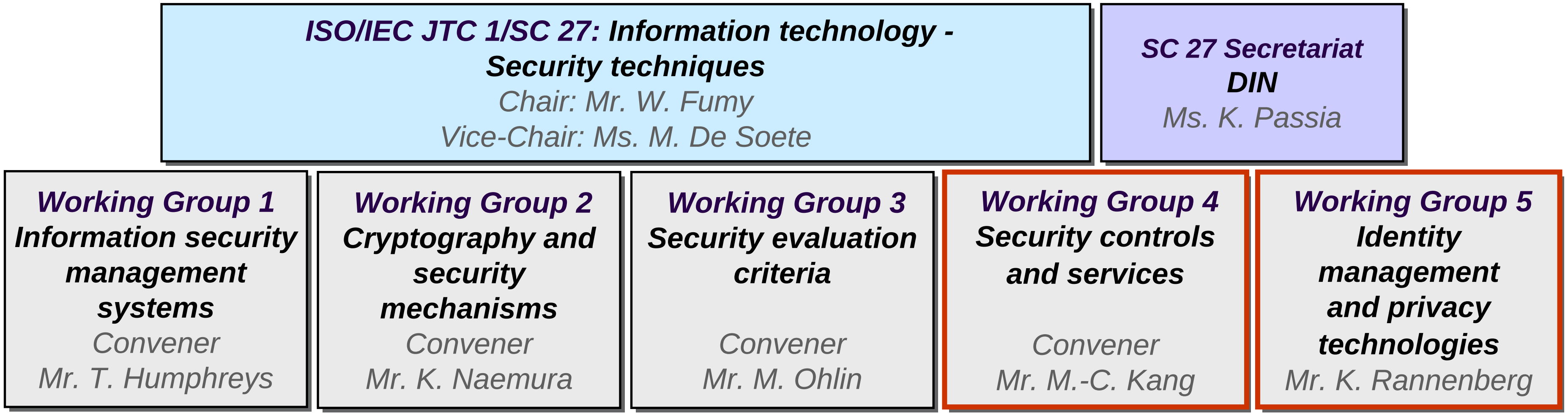
- SC 6 Telecommunications and information exchange between systems
- SC 7 Software and system engineering
- **SC 17 Cards and personal identification**
- SC 25 Interconnection of information technology equipment
- **SC 27 Information technology security techniques**
- SC 29 Coding of audio, picture, 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



*ISO/IEC JTC 1/SC 27: **Information technology - Security techniques***
Chair: Mr. W. Fumy
Vice-Chair: Ms. M. De Soete

SC 27 Secretariat
DIN
Ms. K. Passia

Working Group 1
Information security management systems
Convener
Mr. T. Humphreys

Working Group 2
Cryptography and security mechanisms
Convener
Mr. K. Naemura

Working Group 3
Security evaluation criteria
Convener
Mr. M. Ohlin

Working Group 4
Security controls and services
Convener
Mr. M.-C. Kang

Working Group 5
Identity management and privacy technologies
Mr. K. Rannenberg

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)

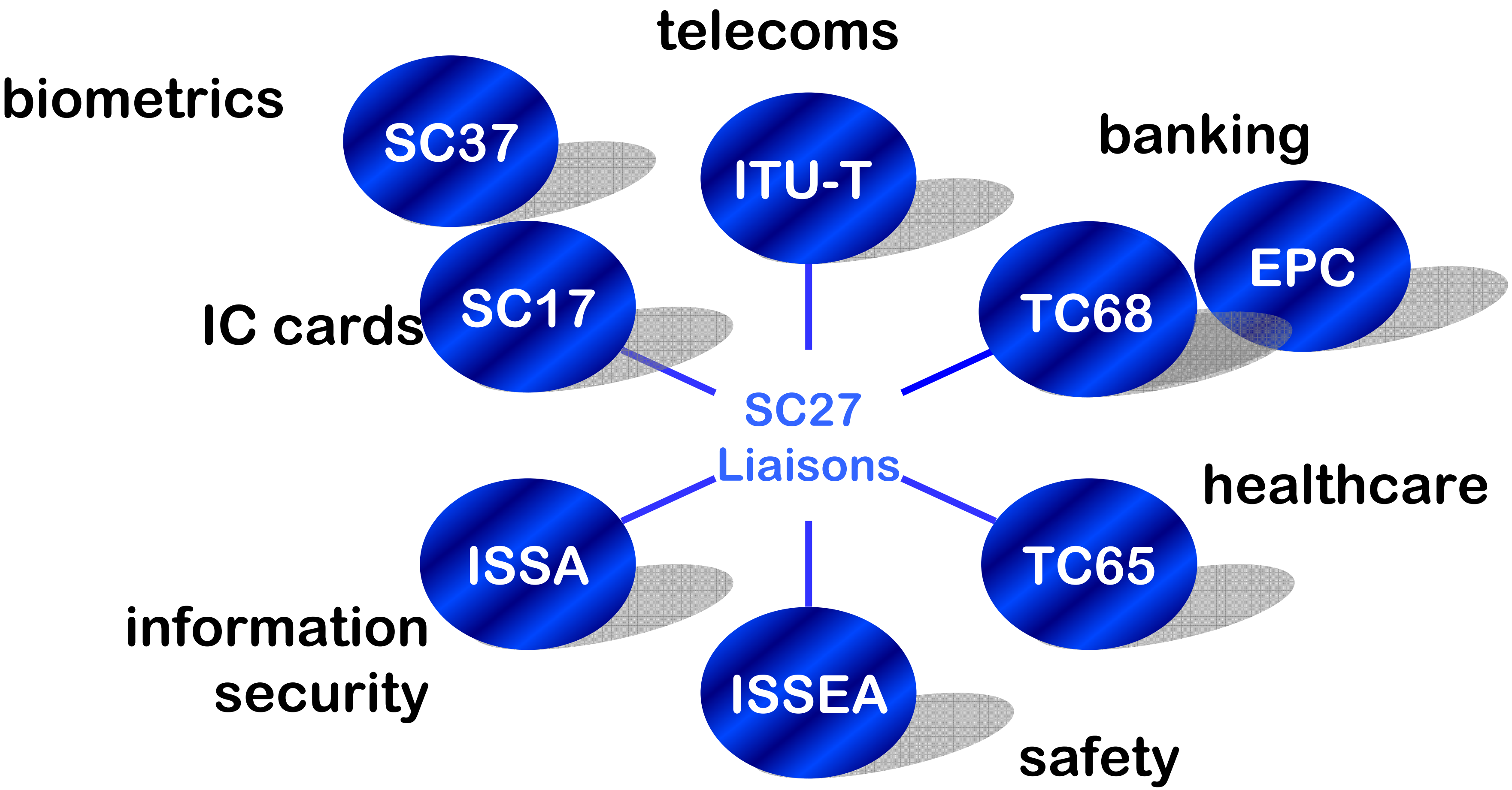
						Cyprus
Russian Federation			South Africa	Kenya		Kazakhstan
Korea		Ukraine	Malaysia	Austria	New Zealand	Uruguay
Australia	Poland	Czech Republic	India	Luxembourg	Singapore	Sri Lanka
1994	*1996*	*1999*	*2001*	*2002*	*2003*	*2005-07*

additional P-Members (total: 35)

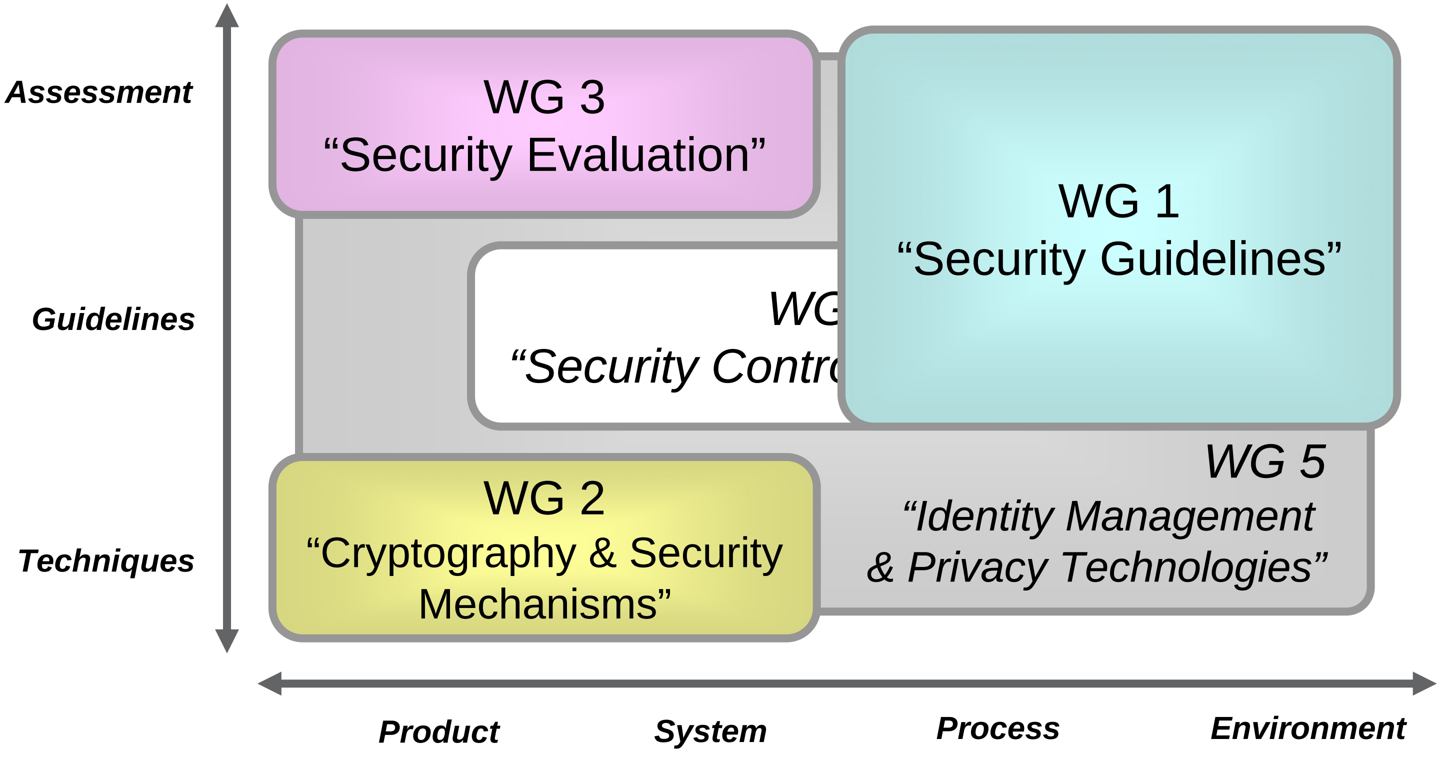
O-members (total: 13)

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

Selected Liaisons

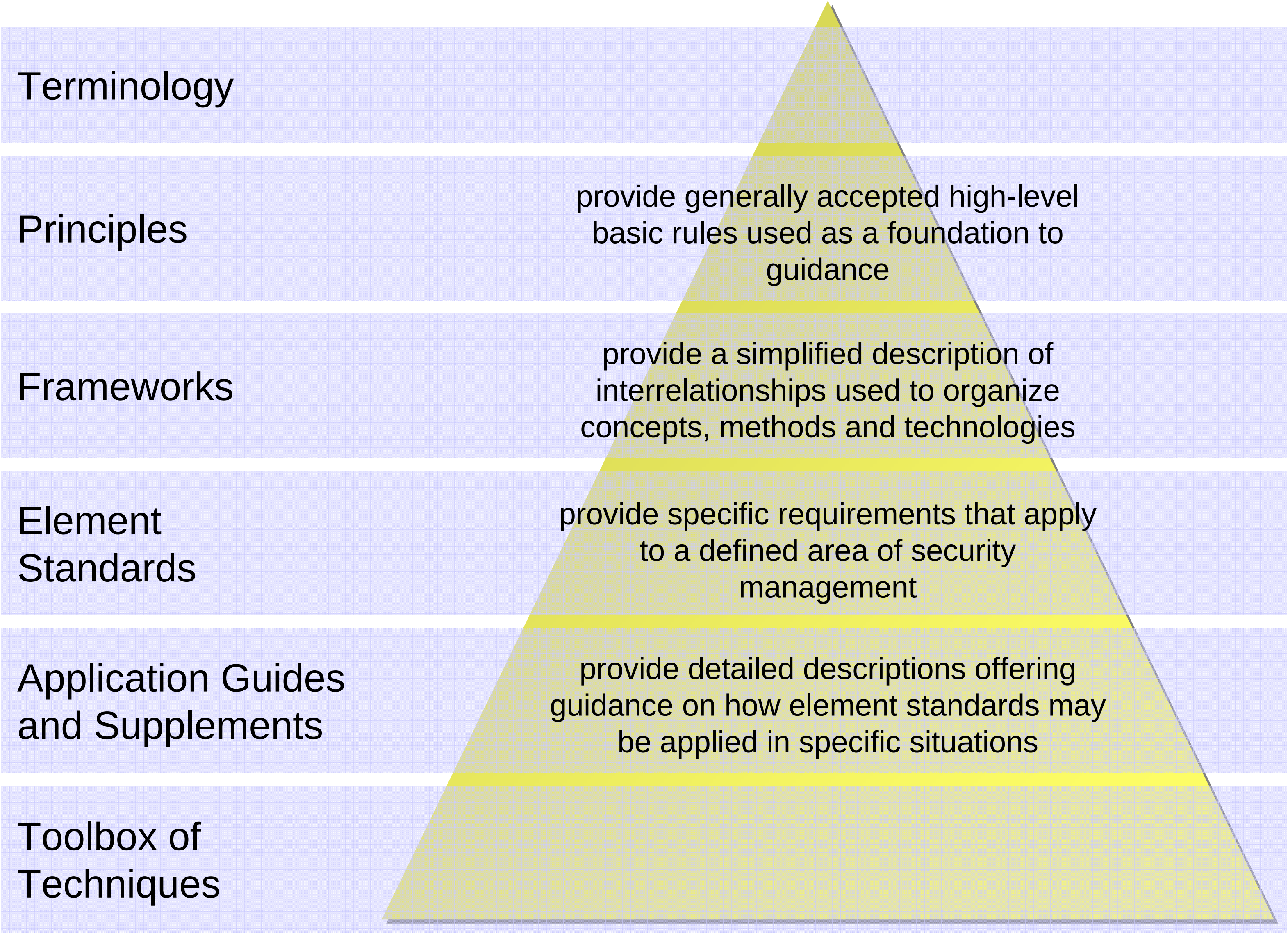


SC 27 –
Evolving Structure



WGs in ***italics*** *are new*

Hierarchical Security Management Model
(SC 27 View)



Terminology

Principles

provide generally accepted high-level basic rules used as a foundation to guidance

Frameworks

provide a simplified description of interrelationships used to organize concepts, methods and technologies

Element Standards

provide specific requirements that apply to a defined area of security management

Application Guides and Supplements

provide detailed descriptions offering guidance on how element standards may be applied in specific situations

Toolbox of Techniques

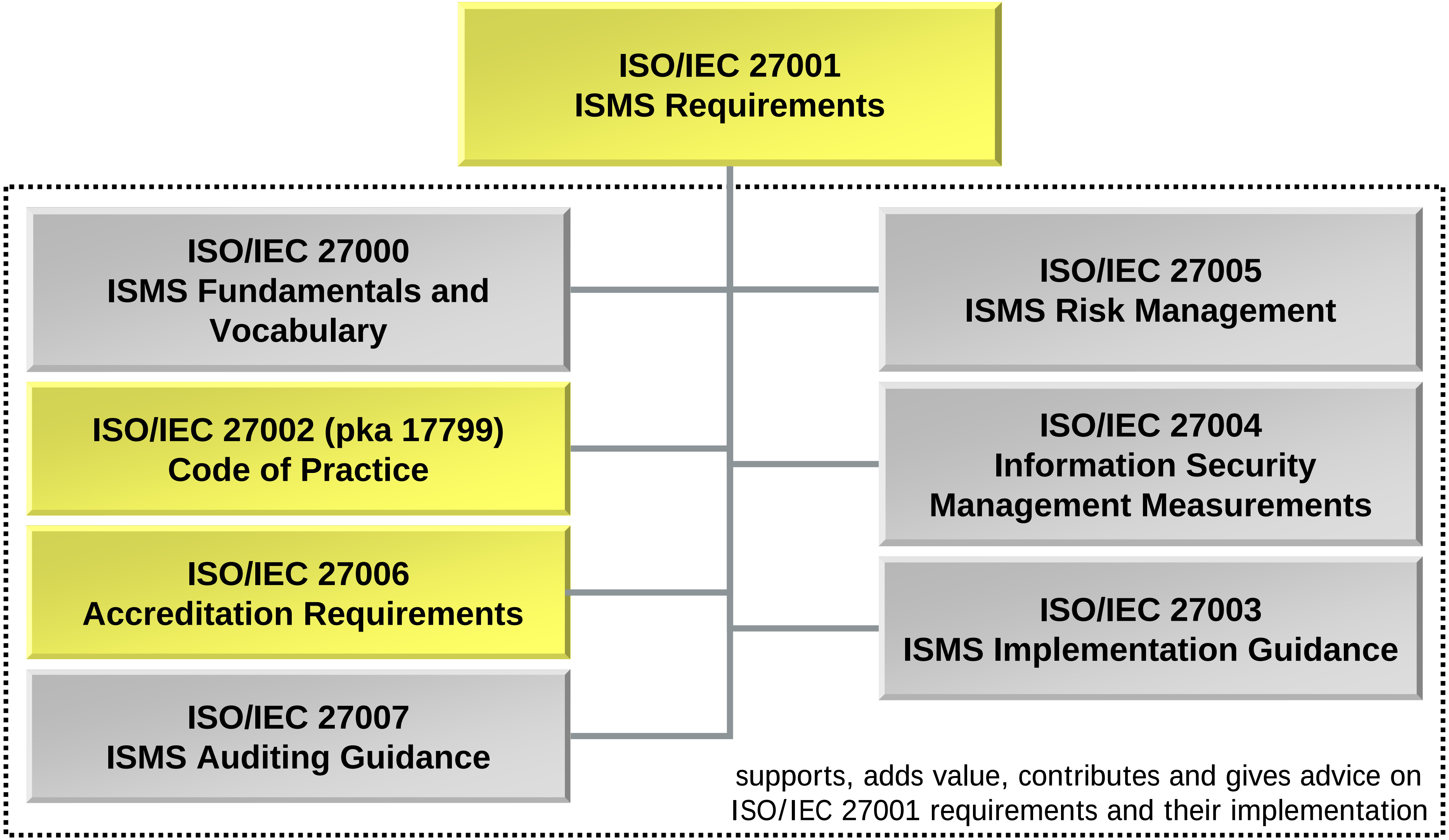
Information Security Management Systems

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]*

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

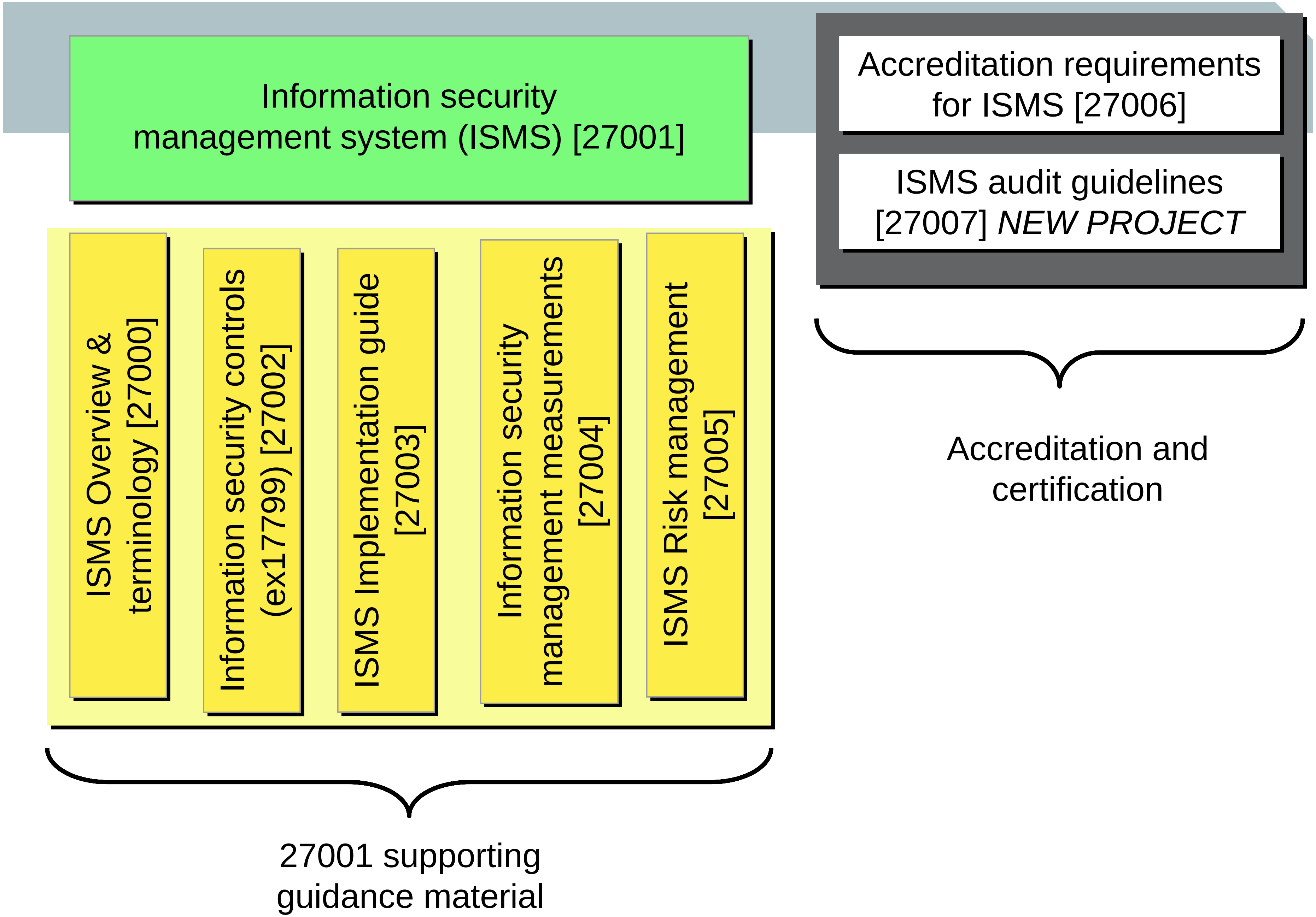
ISO/IEC 27007
ISMS Auditing Guidance

ISO/IEC 27005
ISMS Risk Management

ISO/IEC 27004
Information Security Management Measurements

ISO/IEC 27003
ISMS Implementation Guidance

supports, adds value, contributes and gives advice on ISO/IEC 27001 requirements and their implementation



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]

27001 supporting guidance material

Accreditation requirements for ISMS [27006]

ISMS audit guidelines [27007] *NEW PROJECT*

Accreditation and certification

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

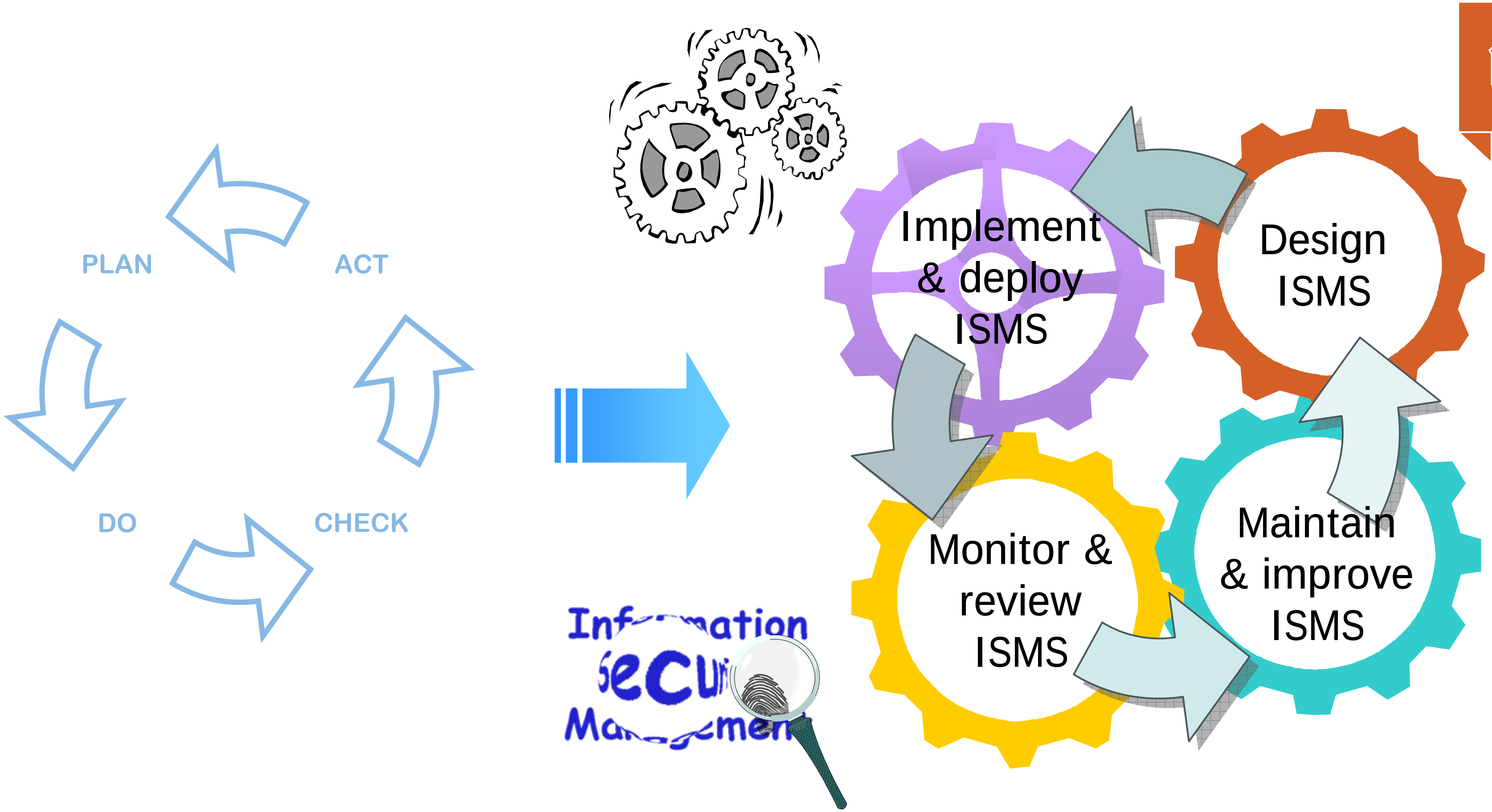
- Replaces BS 7799 Part 2

IS 27001 ISMS Requirements (2)

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

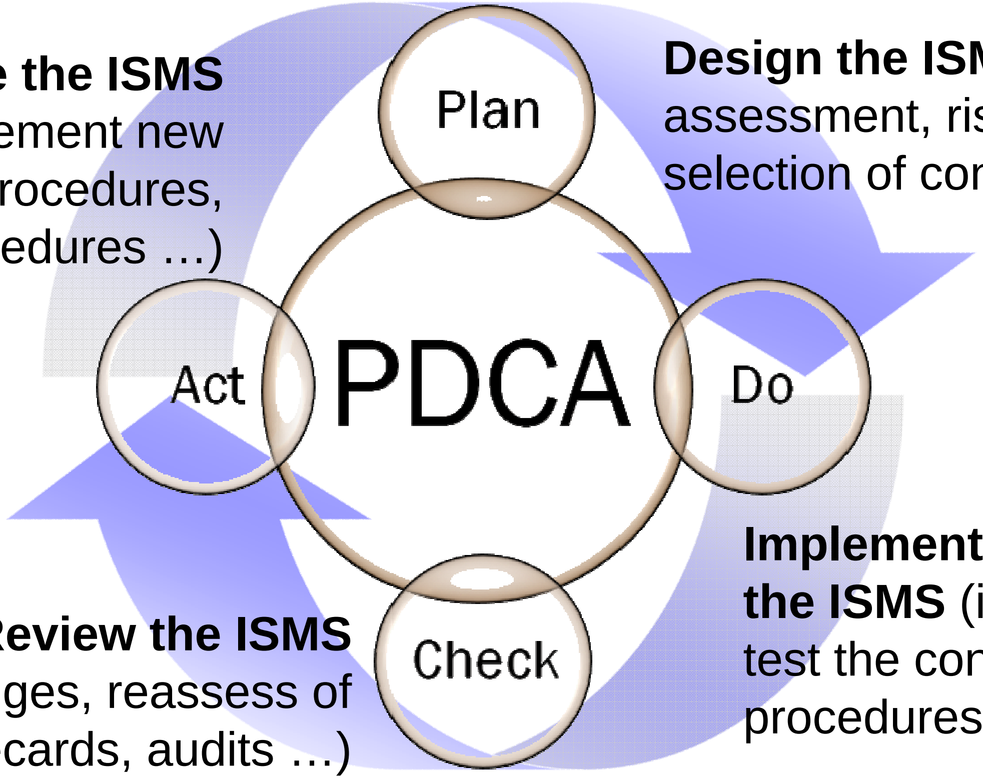
- Auditable specification (internal and external ISMS auditing)

PDCA ISMS Model



ISMS Life Cycle

Information Security Management System (ISMS) Process Model



Design the ISMS (risk assessment, risk treatment, selection of controls …)

Implement & Utilization of the ISMS (implement and test the controls, policies, procedures, process …)

Monitor & Review the ISMS (incident, changes, reassess of the risks, scorecards, audits …)

Update & Improve the ISMS (improve or implement new controls, policies, procedures, procedures …)

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

IS 27002 Code of Practice (1)

Best practice for information security
17799... TO PLAY IT SAFE!
NOW, YOU CHOOSE YOUR PIN CODE!
Zk 2004

- 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

INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

INTERNATIONAL STANDARD

ISO/IEC 17799

First edition
2000-##-##

Information technology — Code of practice for information security management

Technologies de l'information — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 17799:2000(E)

© ISO/IEC 2000

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

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)

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

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

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

IS 27000 Principles and Vocabulary

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

27001 Certification

Large, medium & small business enterprises

In every commercial & industry sector

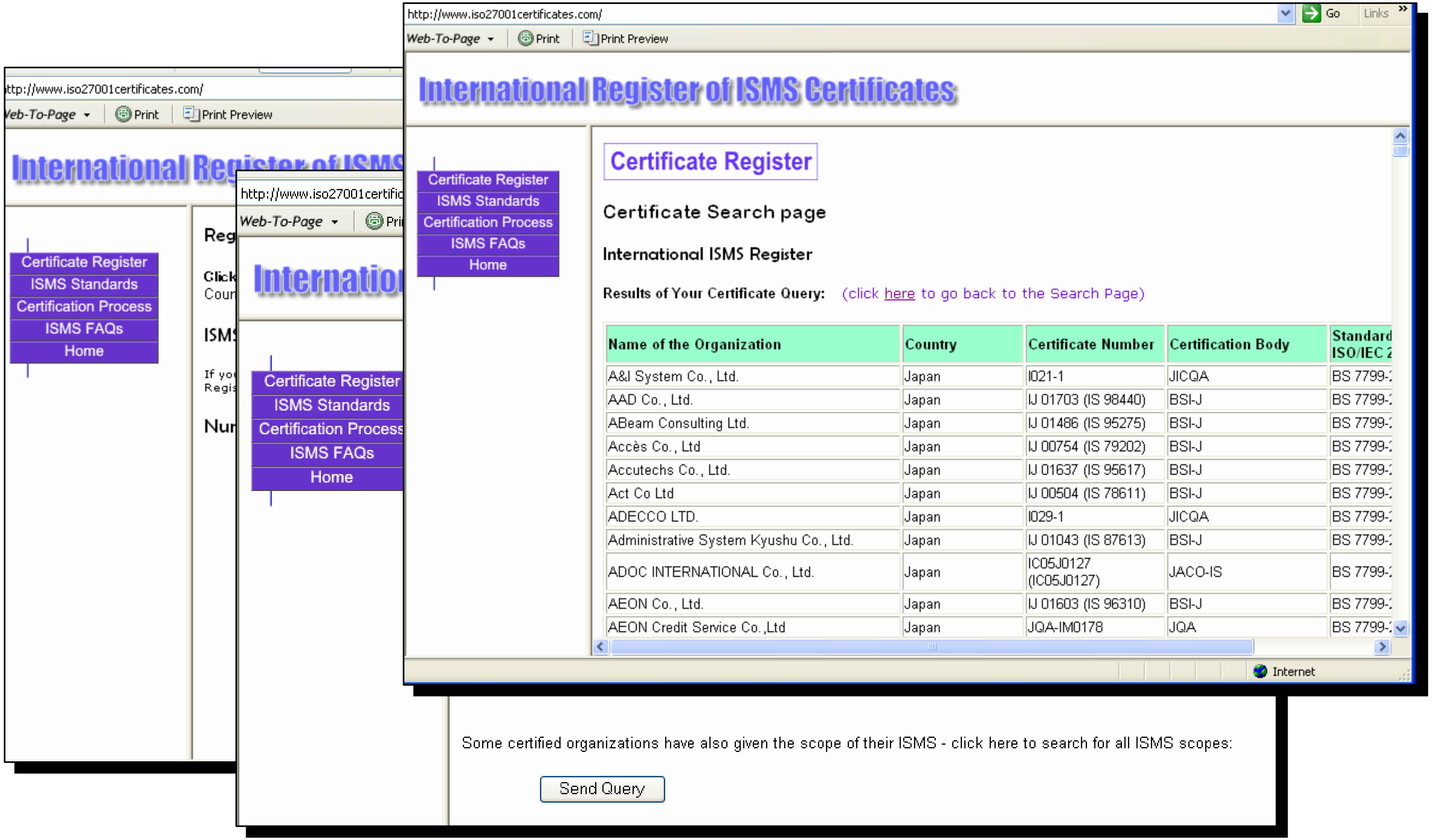
- Banks, financial institutions, insurance
- Telecoms companies, network service providers
- Petroleum, electricity, gas & water companies
- IT manufactures
- Retail organisations
- Publishing companies
- Government departments

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

27001 Certification

www.iso27001certificates.com

27001 Certification



International Register of ISMS Certificates

Certificate Register

Certificate Search page

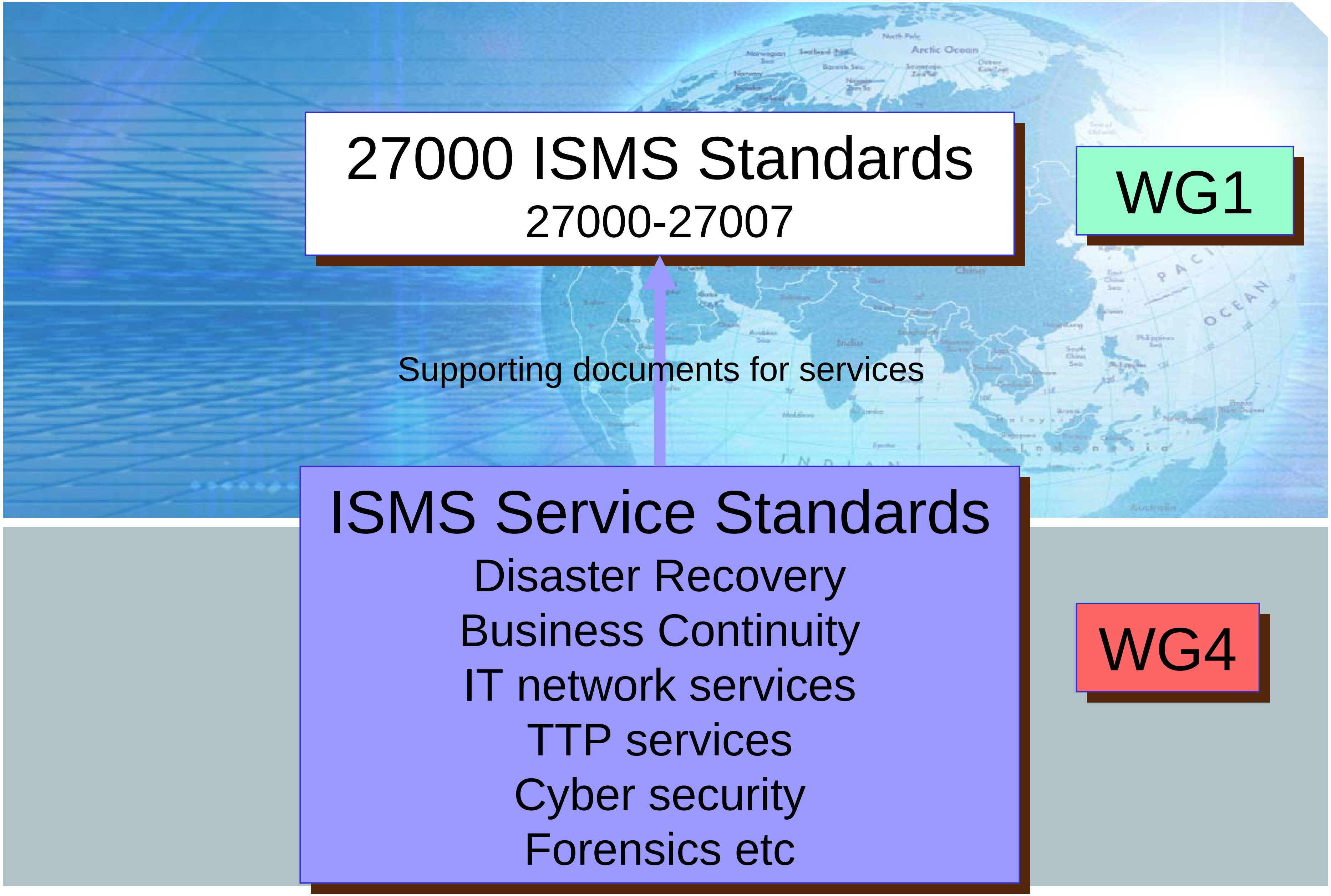
International ISMS Register

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

Name of the Organization	Country	Certificate Number	Certification Body	Standard ISO/IEC 2
A&I System Co., Ltd.	Japan	I021-1	JICQA	BS 7799-2
AAD Co., Ltd.	Japan	IJ 01703 (IS 98440)	BSI-J	BS 7799-2
ABeam Consulting Ltd.	Japan	IJ 01486 (IS 95275)	BSI-J	BS 7799-2
Accès Co., Ltd	Japan	IJ 00754 (IS 79202)	BSI-J	BS 7799-2
Accutechs Co., Ltd.	Japan	IJ 01637 (IS 95617)	BSI-J	BS 7799-2
Act Co Ltd	Japan	IJ 00504 (IS 78611)	BSI-J	BS 7799-2
ADECCO LTD.	Japan	I029-1	JICQA	BS 7799-2
Administrative System Kyushu Co., Ltd.	Japan	IJ 01043 (IS 87613)	BSI-J	BS 7799-2
ADOC INTERNATIONAL Co., Ltd.	Japan	IC05J0127 (IC05J0127)	JACO-IS	BS 7799-2
AEON Co., Ltd.	Japan	IJ 01603 (IS 96310)	BSI-J	BS 7799-2
AEON Credit Service Co.,Ltd	Japan	JQA-IM0178	JQA	BS 7799-2

Some certified organizations have also given the scope of their ISMS - click here to search for all ISMS scopes:

Send Query



27000 ISMS Standards
27000-27007

WG1

Supporting documents for services

ISMS Service Standards
Disaster Recovery
Business Continuity
IT network services
TTP services
Cyber security
Forensics etc

WG4

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

ISO/IEC 18044

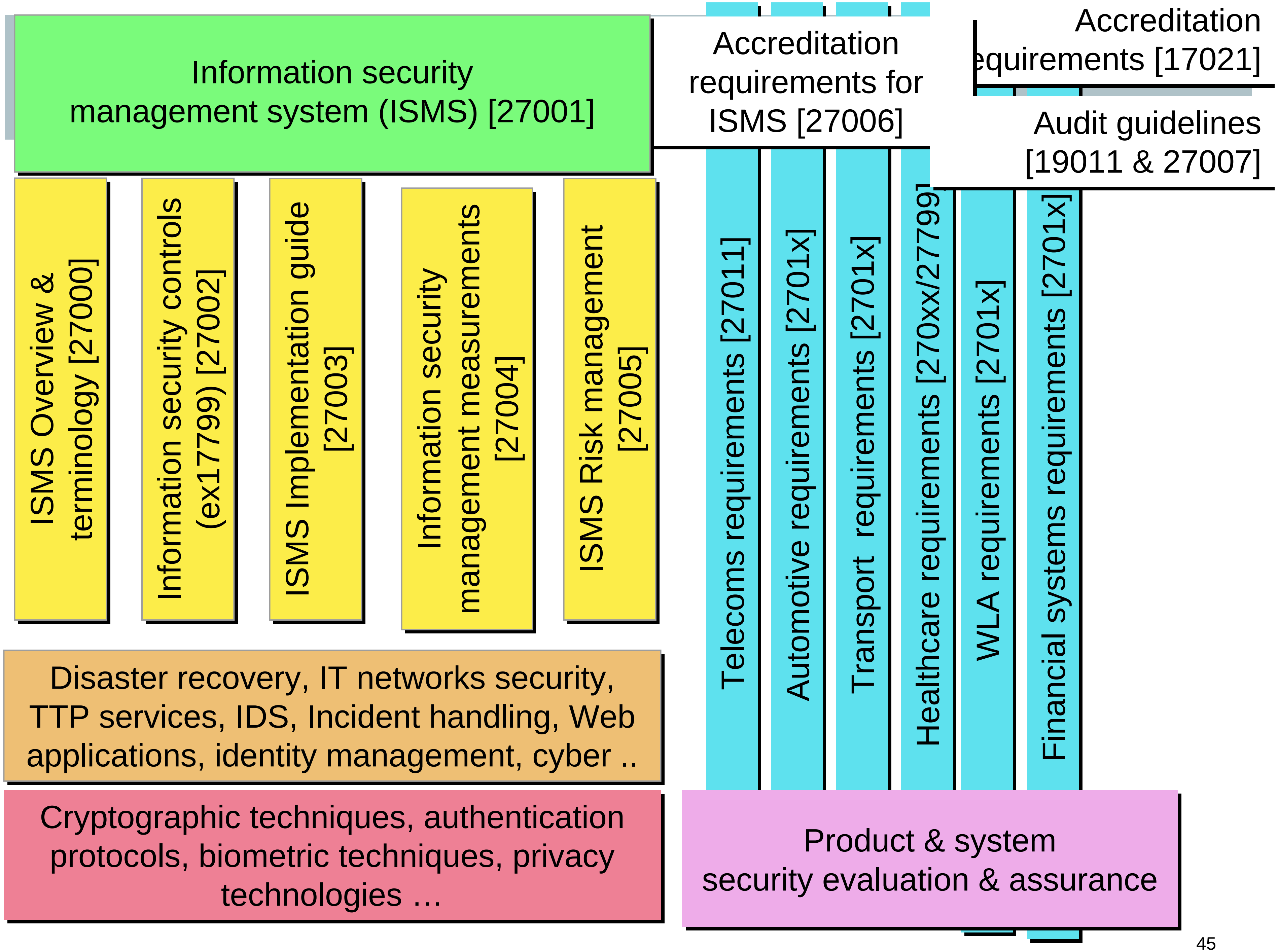
Information security incident handling management

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

ISO/IEC 24762

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]

Accreditation requirements for ISMS [27006]

Accreditation equirements [17021]

Audit guidelines [19011 & 27007]

ISMS Overview & terminology [27000]

Information security controls (ex17799) [27002]

ISMS Implementation guide [27003]

Information security management measurements [27004]

ISMS Risk management [27005]

Telecoms requirements [27011]

Automotive requirements [2701x]

Transport requirements [2701x]

Healthcare requirements [270xx/27799

WLA requirements [2701x]

Financial systems requirements [2701x]

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

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

Product & system security evaluation & assurance

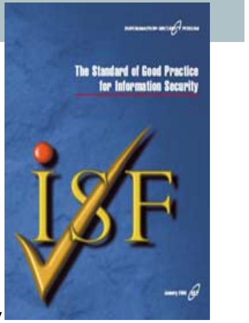
Hierarchical Security Management Model
(SC 27 View)

Terminology		ISO Guide 73	SC 27 SD 6 Updated and harmonized	
Principles		Information Security Management Implementation Guidance (NP 27003)		
Frameworks		Information Security Mgt Framework	MICTS-1: Models and concepts	
Element Standards	ISMS Requirements (NP 27001)	Code of Practice for ISM (IS 17799 / ITU-T X.1051)	MICTS-2: Risk management	ISM Metrics & Measurements (NP 27004)
Application Guides and Supplements	IS 19011 Auditing	Financial ISMS Guide (TC 68)	T-ISMS: Telecom ISMS Guide (ITU-T X.1051)	Healthcare ISMS Guide (TC 215)
Toolbox of Techniques	Info Security Incident Management (TR 18044)	IT Intrusion Detection Framework (TR 15947)	IT Network Security (IS 18028 / ITU-T X.???)	Guidelines for TTP Services (IS 14516 / ITU-T X.842)

Recent SC 27 Publications – *WG 1 & WG 4*

- ISO/IEC 18028: IT network security –
  - Part 1: Network security management, 2006.
  - Part 2: Network security architecture, 2006.
  - Part 3: Securing communications between networks using security gateways, 2006.
  - Part 4: Securing remote access, 2005.
  - Part 5: Securing communications across networks using Virtual Private Networks, 2006.
- ISO/IEC 18043: Selection, deployment and operations of intrusion detection systems (IDS), 2006.
- ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems, 2007.

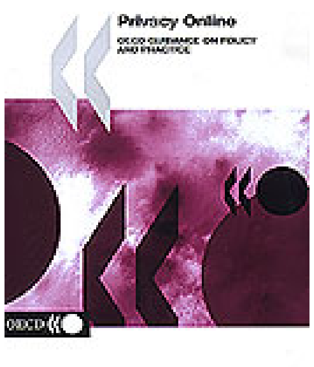
Information Security Management Guidelines – Overview



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)

Guidelines - ISF

INFORMATION SECURITY FORUM

Non-profit association

Widely recognised as being a dominant force in Information Security

Incepted 1989

INFORMATION SECURITY FORUM
The Standard of Good Practice for Information Security
ISF

Engineering, manufacturing & mining	43
Financial services and insurance	90
Transport	11
Chemicals, healthcare, pharmaceuticals	28
Te	
Ut	
Su	
Re	

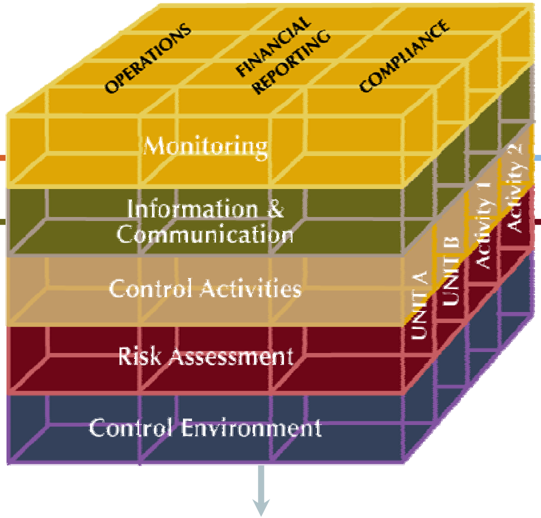
256

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

Guidelines - COSO

Monitoring

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

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.

Control Environment

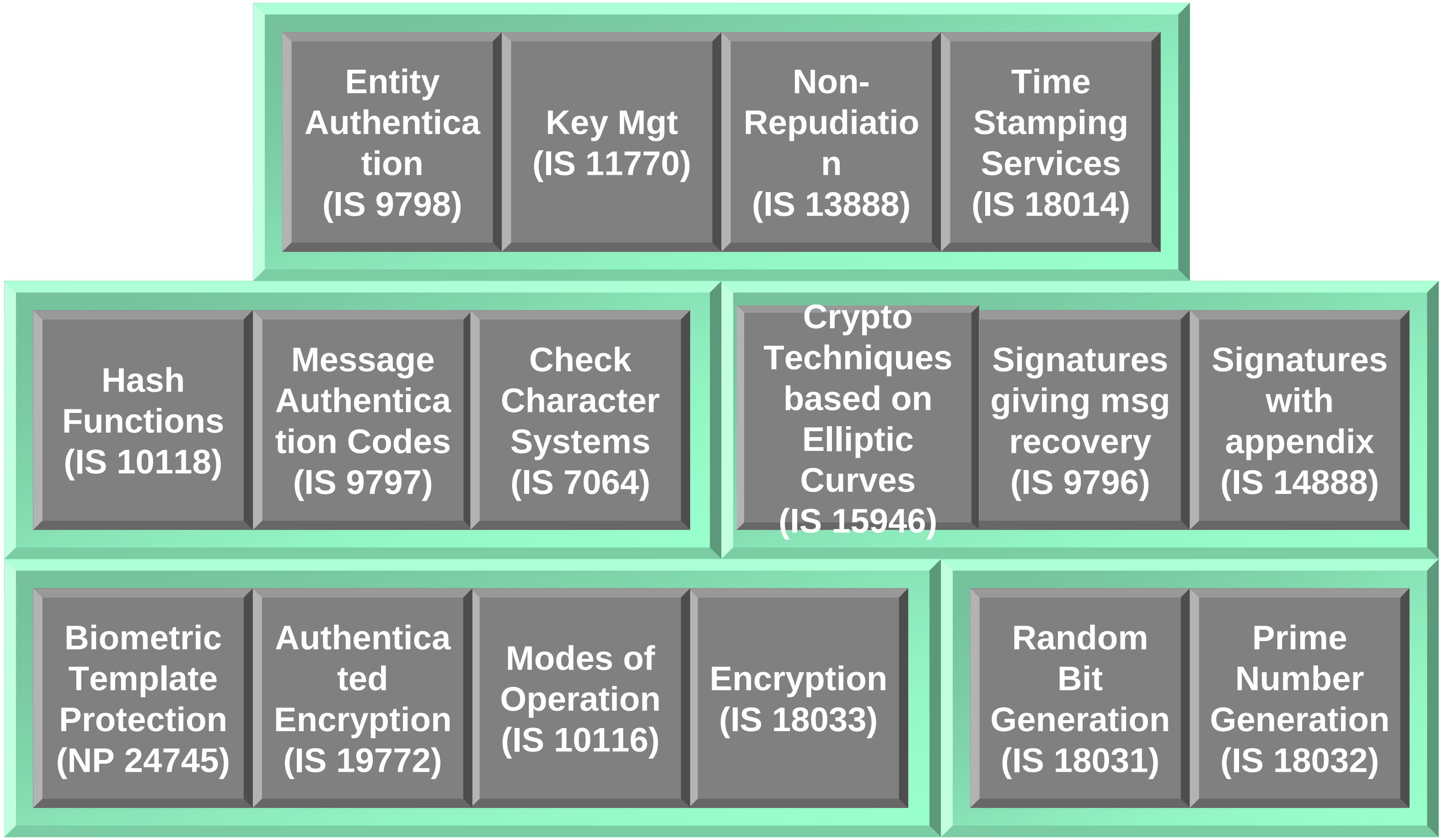
- Sets tone of organization-influencing control consciousness of its people.
- Factors include integrity, ethical values, competence, authority, responsibility.
- Foundation for all other components of control.

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.

All five components must be in place for a control to be effective.

SC 27 Standards – Cryptographic Techniques



Entity Authentication (IS 9798)

Key Mgt (IS 11770)

Non-Repudiation (IS 13888)

Time Stamping Services (IS 18014)

Hash Functions (IS 10118)

Message Authentication Codes (IS 9797)

Check Character Systems (IS 7064)

Crypto Techniques based on Elliptic Curves (IS 15946)

Signatures giving msg recovery (IS 9796)

Signatures with appendix (IS 14888)

Biometric Template Protection (NP 24745)

Authenticated Encryption (IS 19772)

Modes of Operation (IS 10116)

Encryption (IS 18033)

Random Bit Generation (IS 18031)

Prime Number Generation (IS 18032)

Recent SC 27 Publications – *WG 2*

- ISO/IEC 9796: Digital signatures giving message recovery –
  - Part 3: Discrete logarithm based mechanisms, 2nd edition 2006.

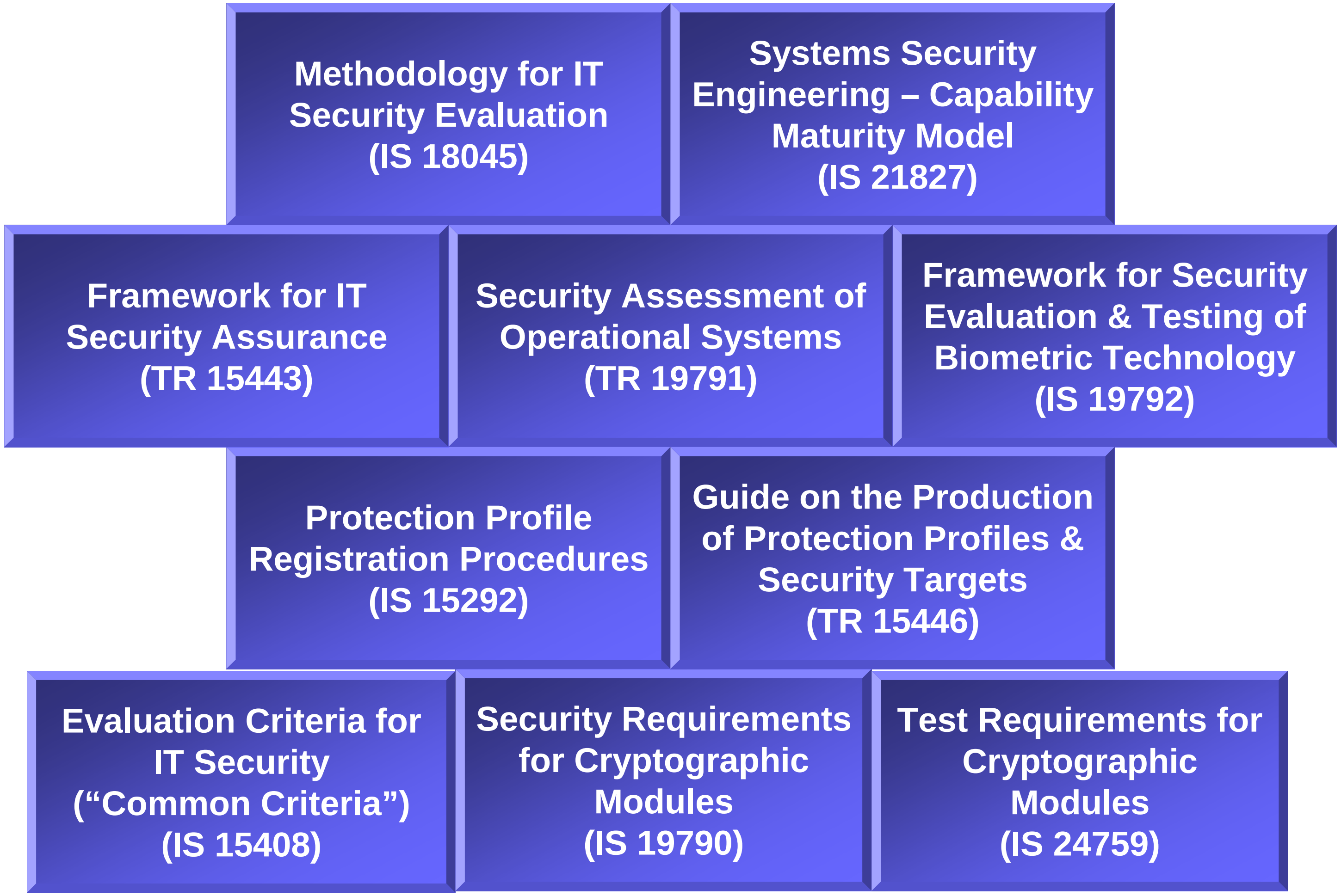
- ISO/IEC 10116: Modes of operation for an n-bit block cipher algorithm, 3rd edition 2006.

- ISO/IEC 11770: Key management –
  - Part 4: Mechanisms based on weak secrets, 2006.

- ISO/IEC 14888: Digital signatures with appendix –
  - Part 3: Discrete logarithm based mechanisms, 2006.

- ISO/IEC 18033: Encryption algorithms –
  - Part 1: General, 2005.
  - Part 2: Asymmetric ciphers, 2006.
  - Part 3: Block ciphers, 2005.
  - Part 4: Stream ciphers, 2005.

SC 27 Standards – Security Evaluation



Methodology for IT Security Evaluation (IS 18045)

Systems Security Engineering – Capability Maturity Model (IS 21827)

Framework for IT Security Assurance (TR 15443)

Security Assessment of Operational Systems (TR 19791)

Framework for Security Evaluation & Testing of Biometric Technology (IS 19792)

Protection Profile Registration Procedures (IS 15292)

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

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

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 –
  - Part 1: Introduction and general model, 2nd edition 2005.
  - Part 2: Security functional requirements, 2nd edition 2005.
  - Part 3: Security assurance requirements, 2nd edition 2005.
- ISO/IEC TR 15443: A framework for IT security assurance –
  - Part 3: Analysis of assurance methods, 2007.
- ISO/IEC 19790: Security requirements for cryptographic modules, 2006.
- ISO/IEC TR 19791: Security assessment of operational systems, 2006.
- ISO/IEC 21827: Systems Security Engineering - Capability Maturity Model (SSE-CMM)

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.

Study Periods & New Projects

<u>New Projects include</u>:

- 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*

<u>Study Periods include</u>

- *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 – *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

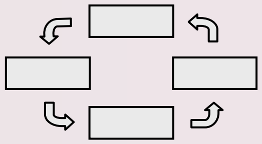
- SC 27 web-page: scope, organization, work items, etc. http://www.jtc1sc27.din.de/en
- SD7: Catalogue of SC 27 Projects & Standards
- SC 27 Secretariat: Krystyna.Passia@din.de

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

Security 4 Biz