Organisers:

CYBERPORT 數碼港

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

Expert Opinions from International Standards Developers

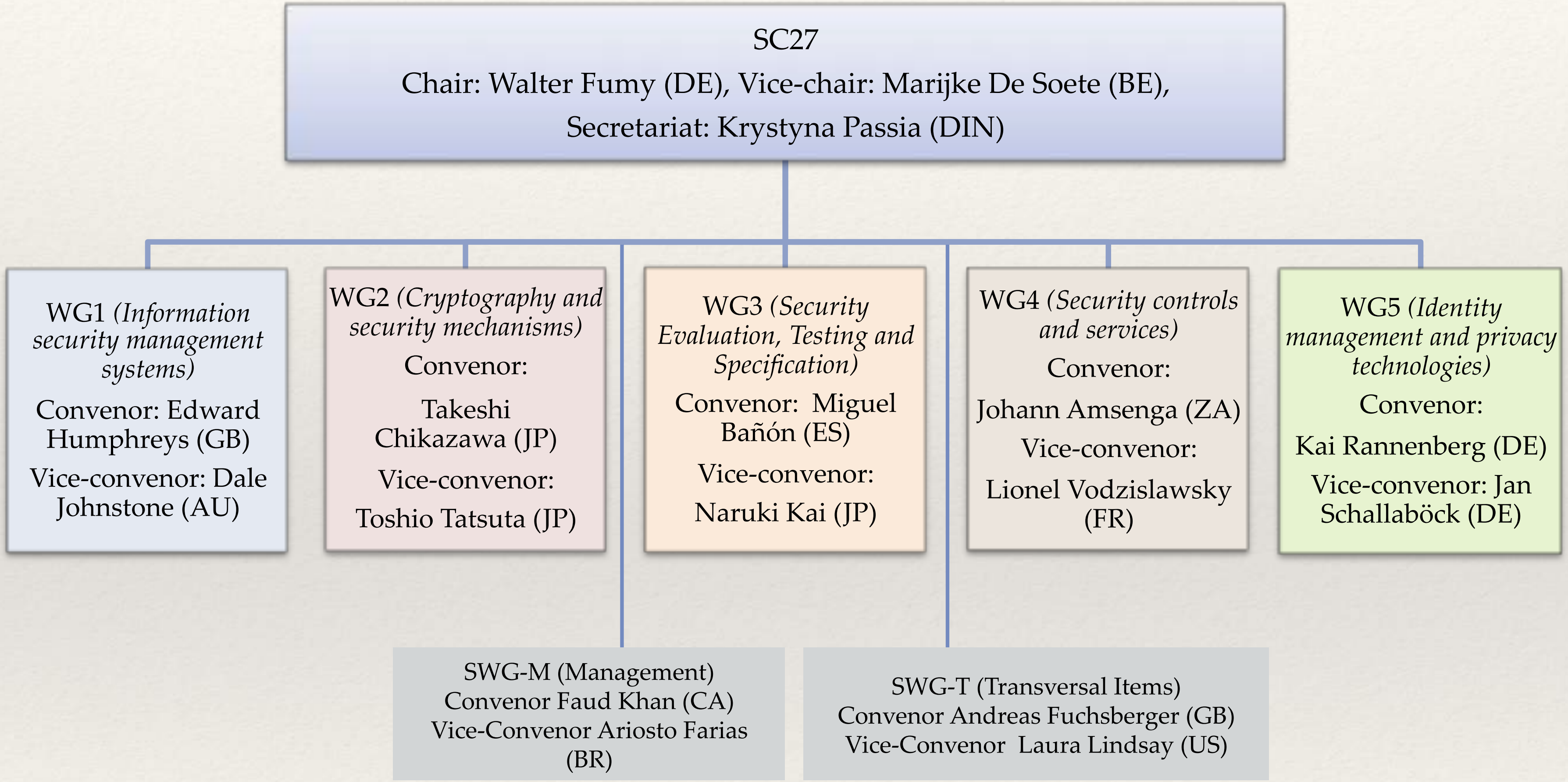
International Conference on
Information Security Standards
11 April 2014 (Fri), Cyberport

SC27 Hong Kong Business Workshop - 11th April 2014

27001 Family of ISMS Standards (with comments on Risk, the Big Picture and κυβερ)

Edward (Ted) Humphreys

ISO/IEC JTC 1/SC 27



SC27
Chair: Walter Fumy (DE), Vice-chair: Marijke De Soete (BE),
Secretariat: Krystyna Passia (DIN)

WG1 *(Information security management systems)*
Convenor: Edward Humphreys (GB)
Vice-convenor: Dale Johnstone (AU)

WG2 *(Cryptography and security mechanisms)*
Convenor:
Takeshi Chikazawa (JP)
Vice-convenor:
Toshio Tatsuta (JP)

WG3 *(Security Evaluation, Testing and Specification)*
Convenor: Miguel Bañón (ES)
Vice-convenor:
Naruki Kai (JP)

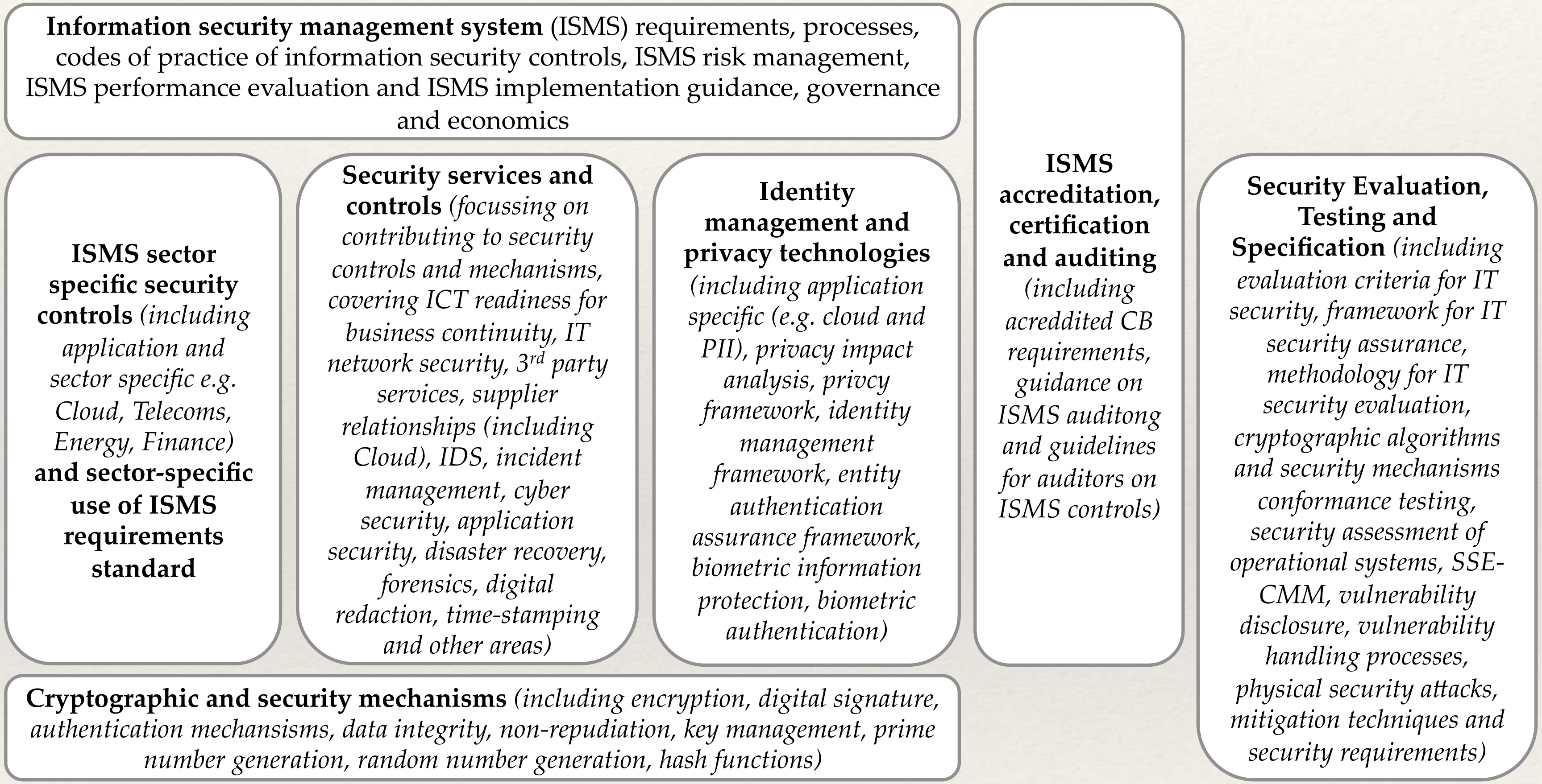
WG4 *(Security controls and services)*
Convenor:
Johann Amsenga (ZA)
Vice-convenor:
Lionel Vodzislawsky (FR)

WG5 *(Identity management and privacy technologies)*
Convenor:
Kai Rannenberg (DE)
Vice-convenor: Jan Schallaböck (DE)

SWG-M (Management)
Convenor Faud Khan (CA)
Vice-Convenor Ariosto Farias (BR)

SWG-T (Transversal Items)
Convenor Andreas Fuchsberger (GB)
Vice-Convenor Laura Lindsay (US)

ISMS Oriented View of SC27



Information security management system (ISMS) requirements, processes, codes of practice of information security controls, ISMS risk management, ISMS performance evaluation and ISMS implementation guidance, governance and economics

ISMS sector specific security controls *(including application and sector specific e.g. Cloud, Telecoms, Energy, Finance)* **and sector-specific use of ISMS requirements standard**

Security services and controls *(focussing on contributing to security controls and mechanisms, covering ICT readiness for business continuity, IT network security, 3rd party services, supplier relationships (including Cloud), IDS, incident management, cyber security, application security, disaster recovery, forensics, digital redaction, time-stamping and other areas)*

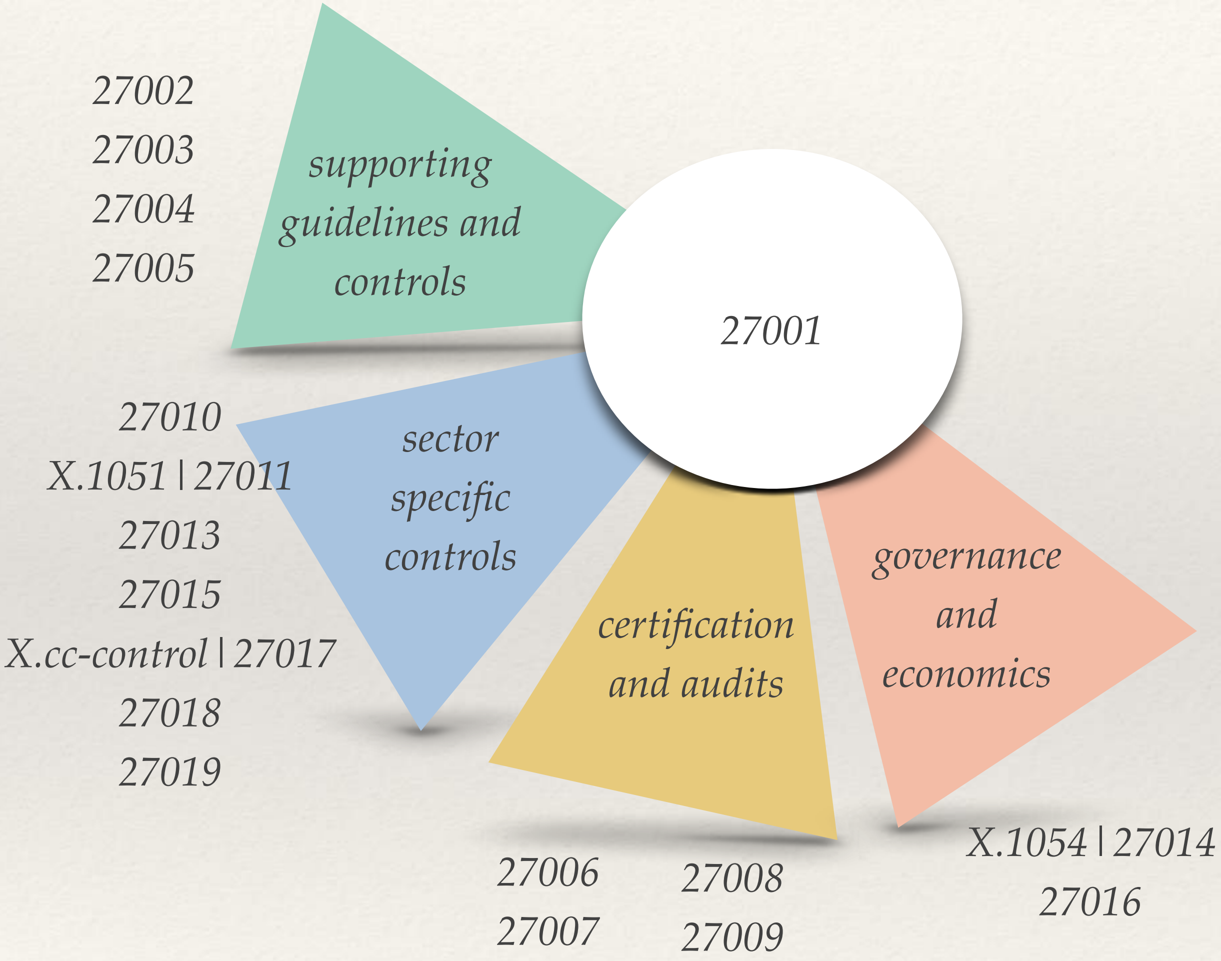
Identity management and privacy technologies *(including application specific (e.g. cloud and PII), privacy impact analysis, privcy framework, identity management framework, entity authentication assurance framework, biometric information protection, biometric authentication)*

ISMS accreditation, certification and auditing *(including acreddited CB requirements, guidance on ISMS auditong and guidelines for auditors on ISMS controls)*

Security Evaluation, Testing and Specification *(including evaluation criteria for IT security, framework for IT security assurance, methodology for IT security evaluation, cryptographic algorithms and security mechanisms conformance testing, security assessment of operational systems, SSE-CMM, vulnerability disclosure, vulnerability handling processes, physical security attacks, mitigation techniques and security requirements)*

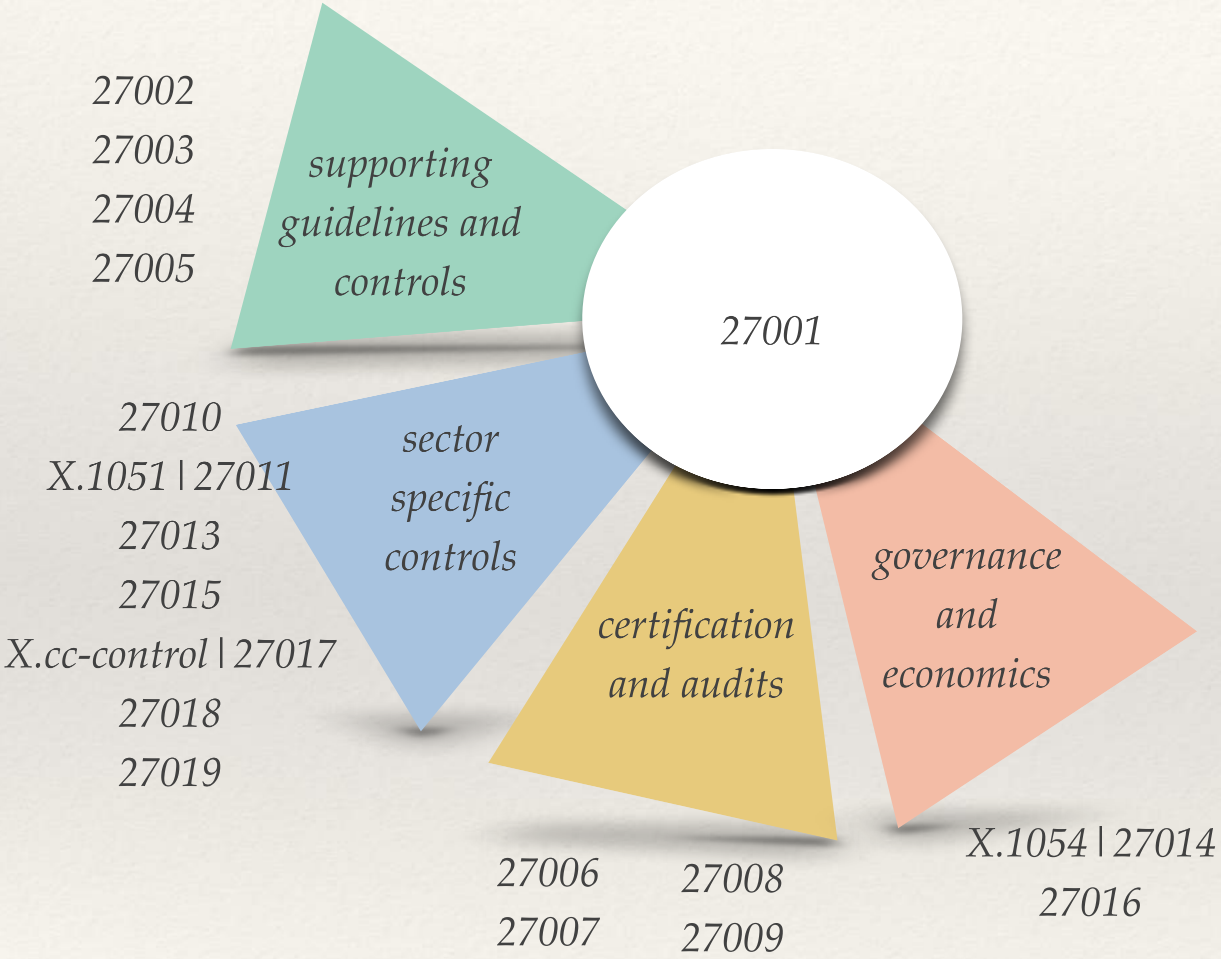
Cryptographic and security mechanisms *(including encryption, digital signature, authentication mechansisms, data integrity, non-repudiation, key management, prime number generation, random number generation, hash functions)*

ISMS Family



SUPPORTING GUIDELINES AND CONTROLS		
27002	Code of practice for information security controls	2nd ed. 2013
27003	Information security management systems — Guidance	1 *under revision (3rd WD)*
27004	Information security management systems — Monitoring, measurement, analysis and evaluation	1 *under revision (3rd WD)*
27005	Information security risk management	2nd ed. 2011 *under revision (2nd WD)*

ISMS Family



27001

27002
27003
27004
27005

supporting guidelines and controls

27010
X.1051 | 27011
27013
27015
X.cc-control | 27017
27018
27019

sector specific controls

certification and audits

27006
27007

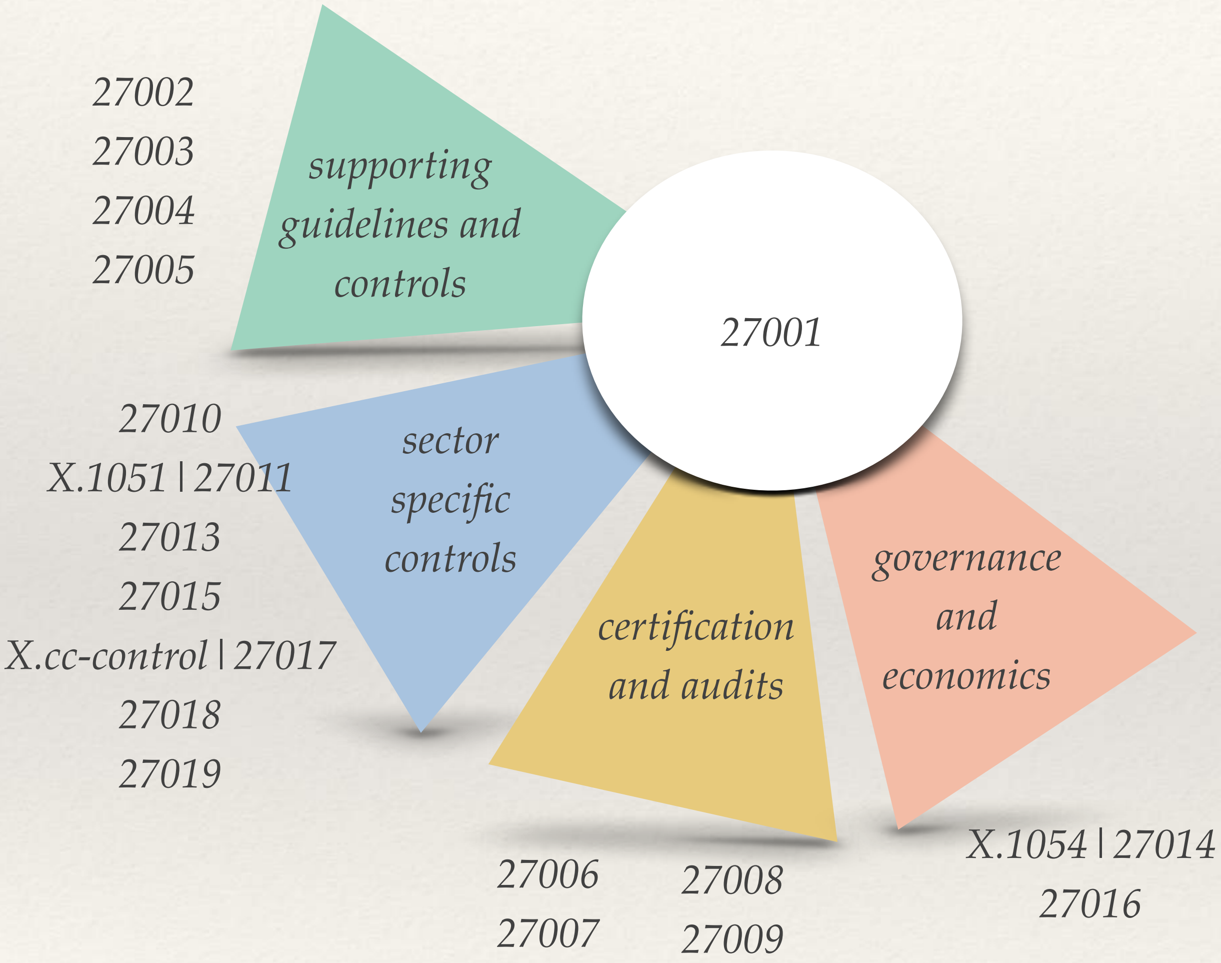
27008
27009

governance and economics

X.1054 | 27014
27016

SECTOR SPECIFIC CONTROLS		
27010	Information security management for inter-sector and inter-organisational communications	1
X.1051 | 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	1 *under revision (1st CD)*
27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	1 under revision (1st CD)
27015	Information security management guidelines for financial services	1

ISMS Family



27001

supporting guidelines and controls

27002
27003
27004
27005

sector specific controls

27010
X.1051 | 27011
27013
27015
X.cc-control | 27017
27018
27019

certification and audits

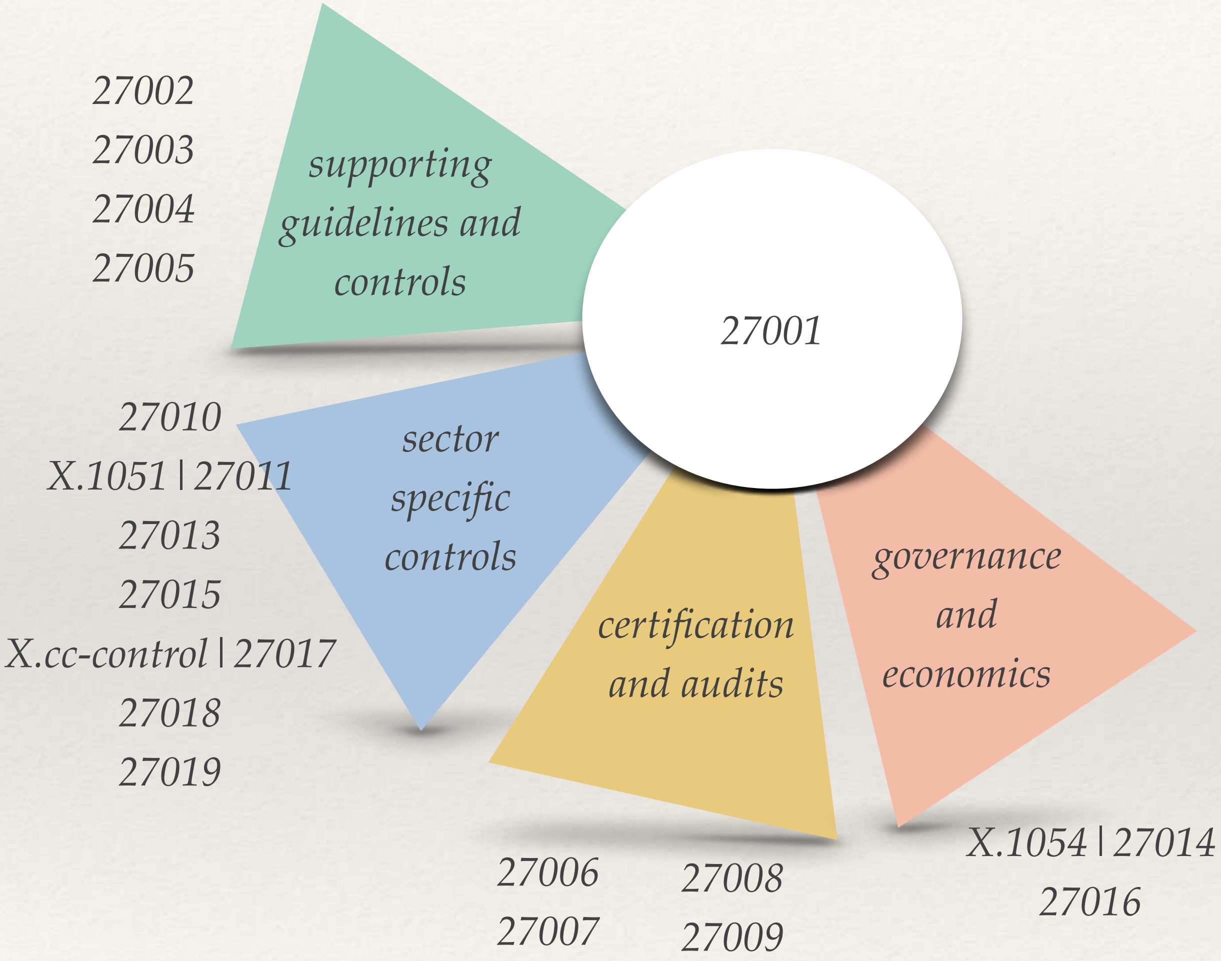
27006
27007
27008
27009

governance and economics

X.1054 | 27014
27016

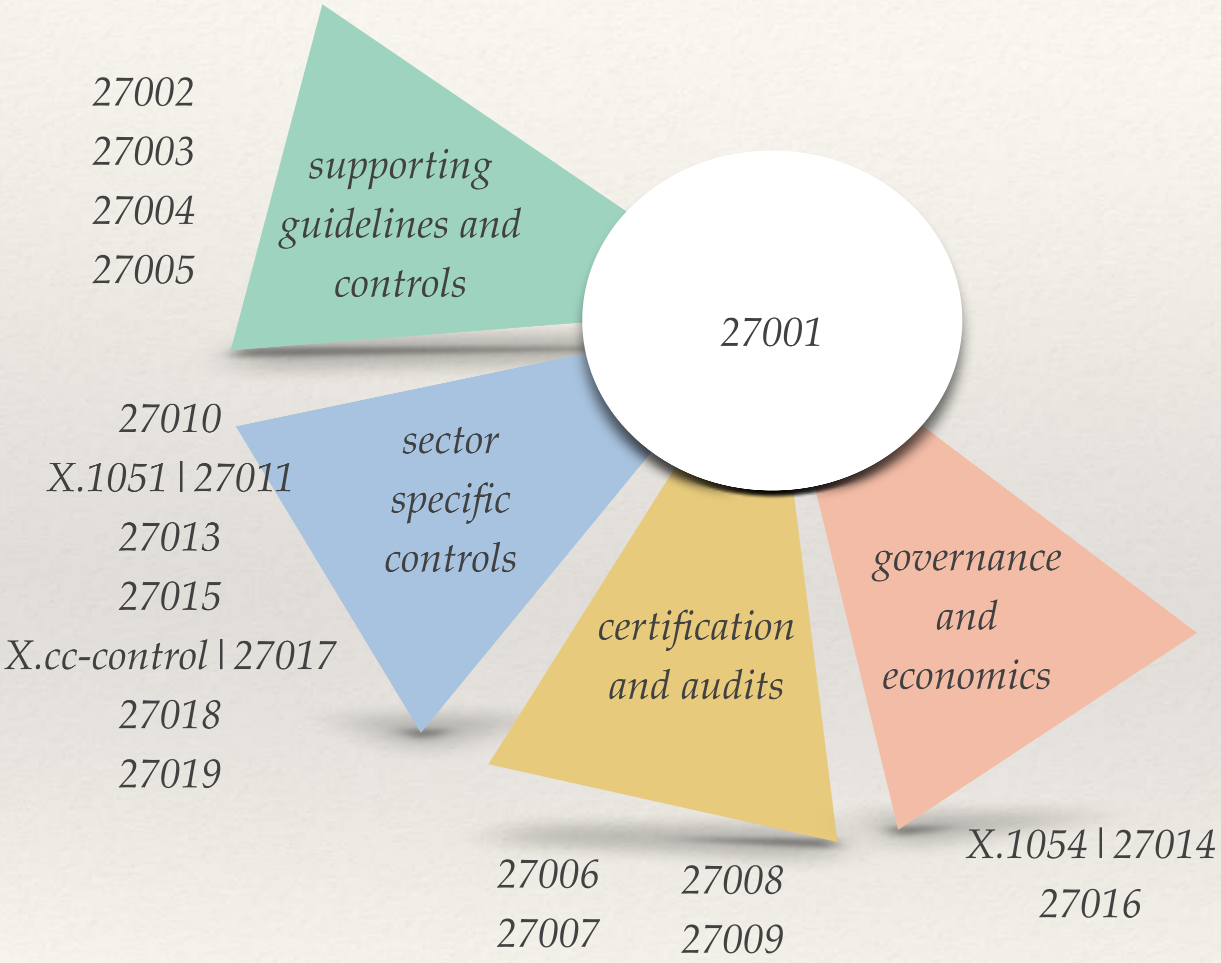
SECTOR SPECIFIC CONTROLS		
X.cc-control |27017	Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	2nd CD
27018	Code of practice for PII protection in public clouds acting as PII processors	DIS 2013
27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	1

ISMS Family



CERTIFICATION AND AUDITS		
27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	2nd ed. 2011 *under revision (2nd CD)*
27007	Guidelines for information security management systems	1
27008	Guidelines for auditors on ISMS controls	1
27009	Sector-specific application of ISO/IEC 27001 – Requirements	1st CD

ISMS Family



27002
27003
27004
27005

supporting guidelines and controls

27001

27010
X.1051 | 27011
27013
27015
X.cc-control | 27017
27018
27019

sector specific controls

certification and audits

27006
27007

27008
27009

governance and economics

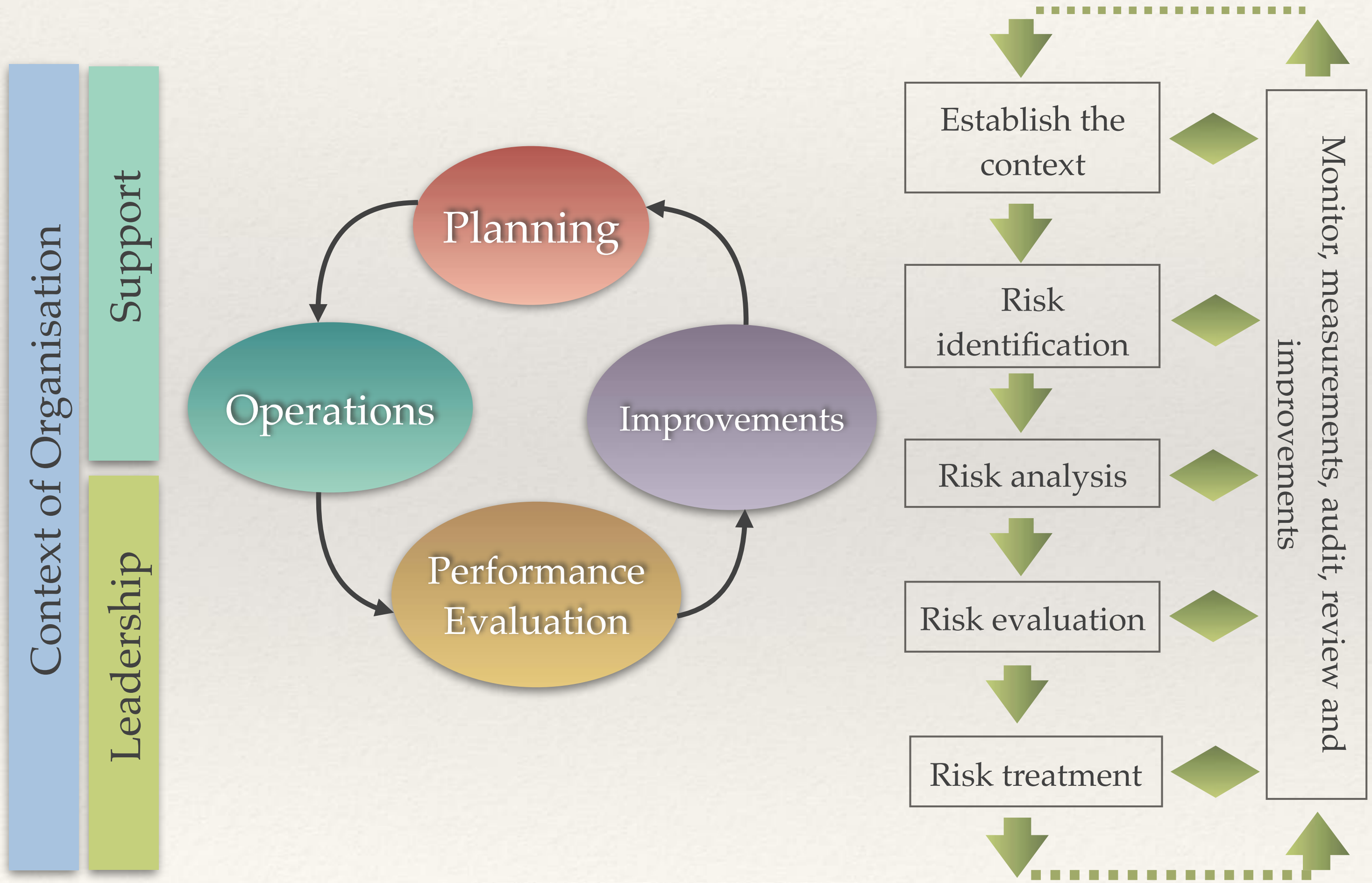
X.1054 | 27014
27016

GOVERNANCE AND ECONOMICS		
X.1054 | 27014	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	1st ed. 2011
27016	Information security - organisation economics	1 2011

ISO/IEC 27001:2013

(2nd edition published Oct 2013)

focus is on - Effective management of information security through - Risk management - Performance evaluation - Continual improvement



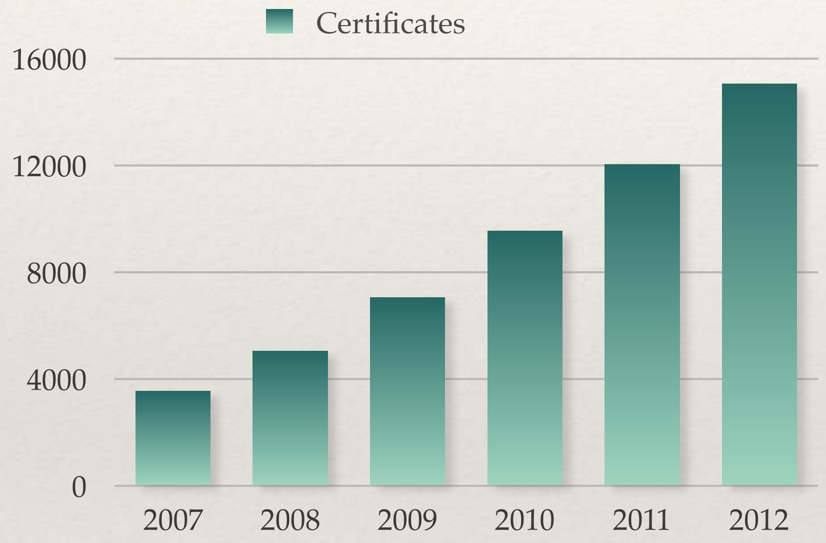
ANNEX A

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident handling
- Information security aspects of business continuity
- Compliance

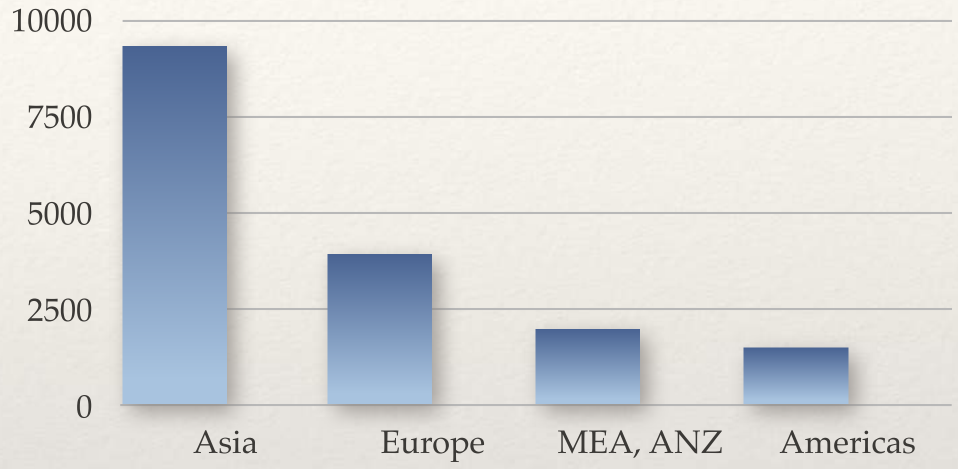
ISMS Processes

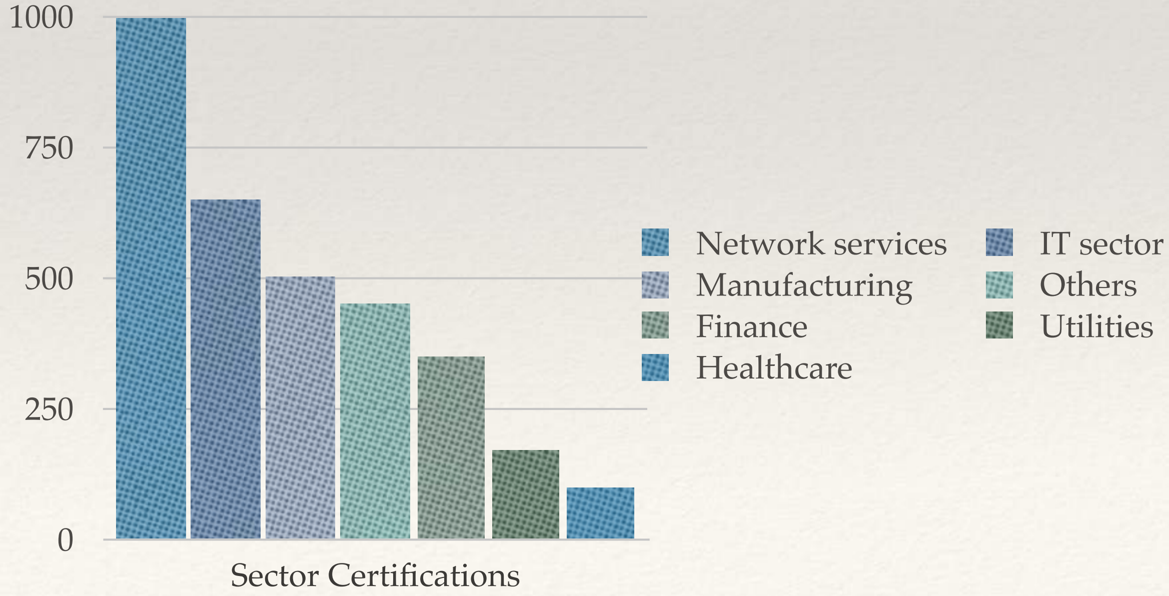
ISMS Controls

ISO/IEC 27001 - Certification



Certifications per Region





ISO/IEC 27001
2005-2013 Transition Arrangements

The International Accreditation Forum (IAF) at its General Assembly meeting on October 24th and 25th 2013 made the following statement:

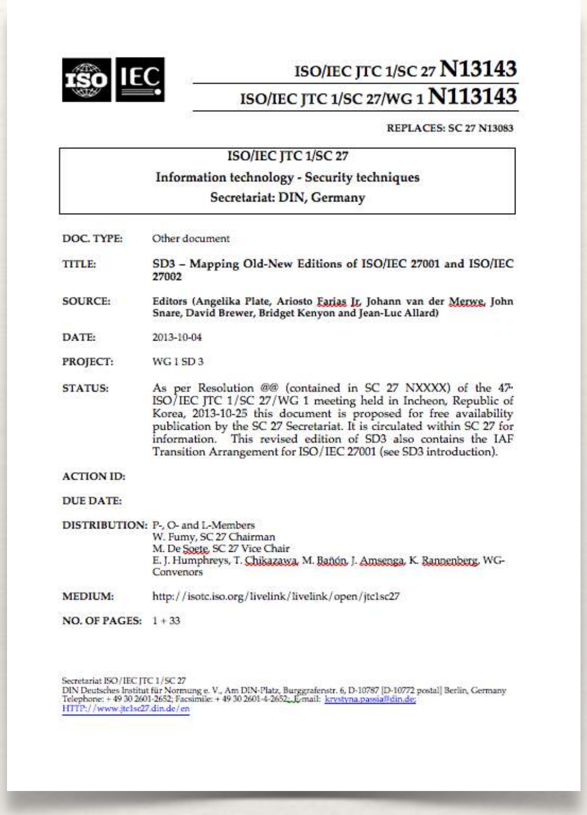
- The General Assembly, acting on the recommendation of the Technical Committee, resolved to endorse ISO/IEC 27001:2013 as a normative document.
- The General Assembly further agreed that the deadline for conformance to ISO/IEC 27001:2013 will be two years from the date of publication.
- One year after publication of ISO/IEC 27001:2013, all new accredited certifications issued shall be to ISO/IEC 27001:2013.

Note: As the date of publication was 1 October 2013, the deadline for Certification Bodies to conform will be 1 October 2015.

ISO/IEC 27001
2005-2013 Transition Maps (SD3)

Mapping 27001 and 27002 2005 editions to the 2013 editions

HTTP://www.jtc1sc27.din.de/en



ISO/IEC JTC 1/SC 27 **N13143**

ISO/IEC JTC 1/SC 27/WG 1 **N113143**

REPLACES: SC 27 N13083

ISO/IEC JTC 1/SC 27
Information technology - Security techniques
Secretariat: DIN, Germany

DOC. TYPE:	Other document
TITLE:	**SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002**
SOURCE:	**Editors (Angelika Plate, Ariosto Farias Jr, Johann van der Merwe, John Snare, David Brewer, Bridget Kenyon and Jean-Luc Allard)**
DATE:	2013-10-04
PROJECT:	WG 1 SD 3
STATUS:	As per Resolution @@ (contained in SC 27 NXXXX) of the 47th ISO/IEC JTC 1/SC 27/WG 1 meeting held in Incheon, Republic of Korea, 2013-10-25 this document is proposed for free availability publication by the SC 27 Secretariat. It is circulated within SC 27 for information. This revised edition of SD3 also contains the IAF Transition Arrangement for ISO/IEC 27001 (see SD3 introduction).
ACTION ID:	
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice Chair E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors
MEDIUM:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27
NO. OF PAGES:	1 + 33

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

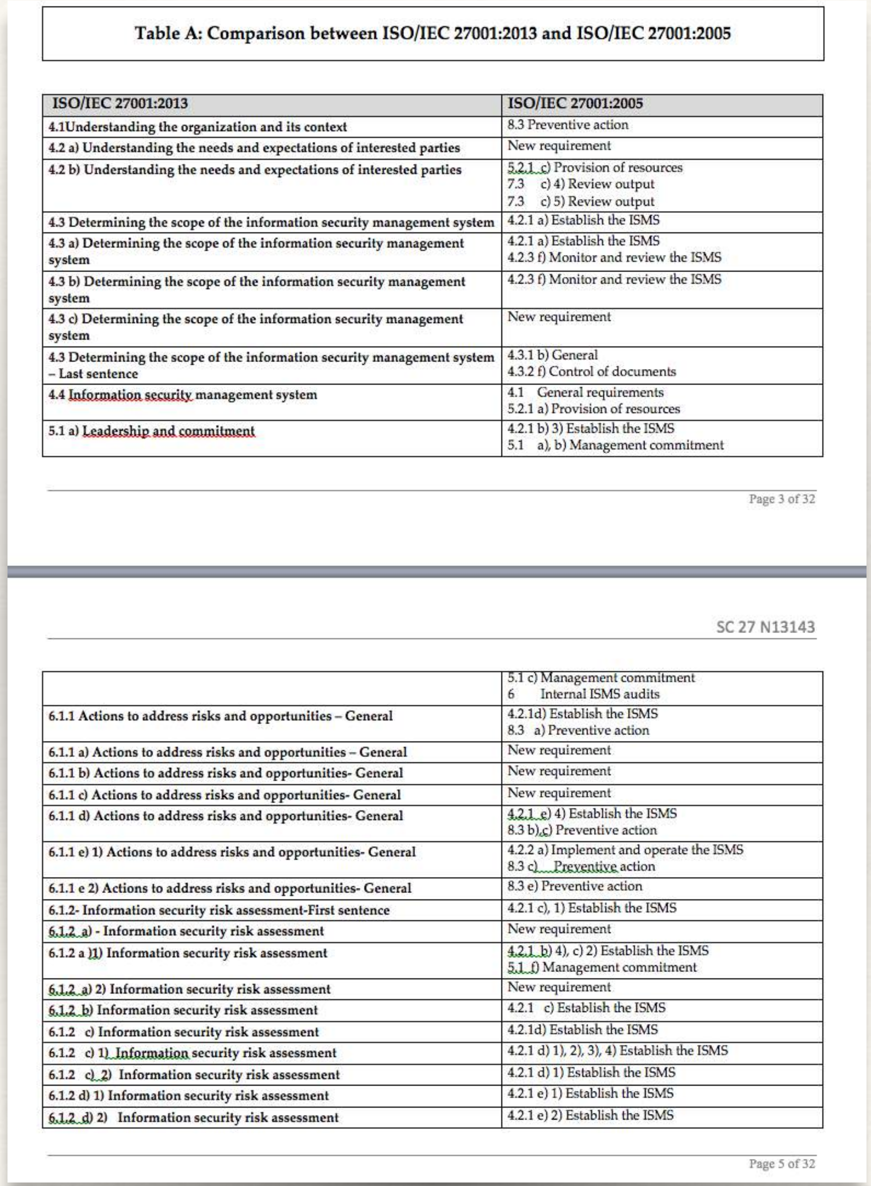


Table A: Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005

ISO/IEC 27001:2013	ISO/IEC 27001:2005
4.1Understanding the organization and its context	8.3 Preventive action
4.2 a) Understanding the needs and expectations of interested parties	New requirement
4.2 b) Understanding the needs and expectations of interested parties	5.2.1 c) Provision of resources 7.3 c) 4) Review output 7.3 c) 5) Review output
4.3 Determining the scope of the information security management system	4.2.1 a) Establish the ISMS
4.3 a) Determining the scope of the information security management system	4.2.1 a) Establish the ISMS 4.2.3 f) Monitor and review the ISMS
4.3 b) Determining the scope of the information security management system	4.2.3 f) Monitor and review the ISMS
4.3 c) Determining the scope of the information security management system	New requirement
4.3 Determining the scope of the information security management system – Last sentence	4.3.1 b) General 4.3.2 f) Control of documents
4.4 Information security management system	4.1 General requirements 5.2.1 a) Provision of resources
5.1 a) Leadership and commitment	4.2.1 b) 3) Establish the ISMS 5.1 a), b) Management commitment

	5.1 c) Management commitment 6 Internal ISMS audits
6.1.1 Actions to address risks and opportunities – General	4.2.1d) Establish the ISMS 8.3 a) Preventive action
6.1.1 a) Actions to address risks and opportunities – General	New requirement
6.1.1 b) Actions to address risks and opportunities- General	New requirement
6.1.1 c) Actions to address risks and opportunities- General	New requirement
6.1.1 d) Actions to address risks and opportunities- General	4.2.1 e) 4) Establish the ISMS 8.3 b),c) Preventive action
6.1.1 e) 1) Actions to address risks and opportunities- General	4.2.2 a) Implement and operate the ISMS 8.3 c) Preventive action
6.1.1 e 2) Actions to address risks and opportunities- General	8.3 e) Preventive action
6.1.2- Information security risk assessment-First sentence	4.2.1 c), 1) Establish the ISMS
6.1.2 a) - Information security risk assessment	New requirement
6.1.2 a)1) Information security risk assessment	4.2.1 b) 4), c) 2) Establish the ISMS 5.1 f) Management commitment
6.1.2 a) 2) Information security risk assessment	New requirement
6.1.2 b) Information security risk assessment	4.2.1 c) Establish the ISMS
6.1.2 c) Information security risk assessment	4.2.1d) Establish the ISMS
6.1.2 c) 1) Information security risk assessment	4.2.1 d) 1), 2), 3), 4) Establish the ISMS
6.1.2 c) 2) Information security risk assessment	4.2.1 d) 1) Establish the ISMS
6.1.2 d) 1) Information security risk assessment	4.2.1 e) 1) Establish the ISMS
6.1.2 d) 2) Information security risk assessment	4.2.1 e) 2) Establish the ISMS

The Future
27001 Risk Management and the Big Picture

- The champions of Digital World technology are
  - Big Data
    - *Exabits of data in a Big playing field*
  - Cloud
    - *Transforming how we live, work and play*
  - IoT (Internet of Things)
    - *Trillions of small things and greater number and variety of devices in talking across a Big universe - the Internet*

Big Data (A security and privacy issue?)

- Government
  - *National Information Infrastructure - Spending, employment, health, society, transport, education, government etc*
- National Infrastructure
  - *Business sectors and government connected to the Internet to form the back-bone of a nation*
- Private sector
  - *data warehousing*
  - *millions of back-end operations, queries from millions of third party sellers/suppliers*
  - *millions of customer transactions*
  - *credit card fraud detection*
- Information security and privacy issue - confidentiality, integrity, availability and PII!!!

- Data that exceeds the capability and processing capacity of standard DBS
  - *data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications.*
- Data that moves fast and is large in size and volume
- There is an exponential growth in the data that business and governments are collectively generating
- It is estimated that the volume of unstructured data (such as videos, photos, documents, texts, Tweets ...) will grow from
  - 2.5 zettabytes (2011) to around 8-9 zettabytes (2015)
  - Data generated in the whole of 1990 is in 2013 being generated in 60 secs.

1 zettabyte (ZB) = 1000 exabytes = 1 billion terabytes = 10^{21} bytes = 1 000 000 000 000 000 000 000 bytes

Cloud

information@risk

- Connecting together ‘smart/intelligent’ things
  - *Devices and networks*
  - *Smart highways, factories, energy systems, hospitals, cities*
- Services
  - *Software, applications, infrastructure and network services (SaaS, AaaS, IaaS and NaaS)*
- On-going uncertainty - *Security and privacy - confidentiality, integrity, availability and PII*

Internet of Things (IoT) (A security and privacy issue?)

- Trillions of small things and devices talking across a Big universe - the Internet
  - Smart buildings
  - Smart energy
  - Smart transport
  - Medical applications
  - Monitoring and sensor systems and devices
  - Industrial control systems
  - Home equipment
- Information security and privacy issue - confidentiality, integrity, availability and PII!!!

Biggest Risks

- Big Data, Cloud and IoT are all prone to risks to the ***security*** and ***privacy*** of ***information***
- Two of the **biggest RISKS** are
    - ***Lack of governance***
        - *inadequate risk management process in place, inadequate audit function*
    - ***Lack of management***
        - *information, people, services and technology*
        - *The ratio of insider to outsider risk is approx. 6:4 and growing (according to stats from EU and USA)*
            - *A management of people problem, process, policy and procedure*
- There is also the other problem **κυβερ-** *(cyber-) (What is cyber and what is the problem?)*

What is **κυβερ-** *(cyber-)*?

… οἷον ***κυβερνήτης*** ἄκρος ἢ ἰατρὸς τά τε ἀδύνατα ἐν τῇ τέχνῃ καὶ τὰ δυνατὰ διαισθάνεται … *(Plato 2.360e-361a, Republic)*

- The ancient Greeks invented the language of ***κυβερ***
    - *Steering a ship and governing a State/Nation - Plato's 'Ship of State'*
    - *The Art (techne - τεχηε - technique) of **Governing, Managing, Navigation***
    - *Ancient Greeks experienced the Art of **κυβερ** first hand in their daily lives over 2000 years ago*

and now Today (2014) we ask the question ***What is Cyber Security?***

*More detailed article "The Art of Cyber - learning from 2500 years of experience of **κυβερ** risks and the role of ISO/IEC 27001" Humphreys, Edward (first edition 2011, revised 2013)*

κυβερ- *(cyber-) and SciFi*

Cyberspace.

A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding. (William Gibson 1948)

Gibson said (2000) "All I knew about the word "cyberspace" when I coined it, was that it seemed like an ***effective buzzword****. It seemed* ***evocative and essentially meaningless****. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page."*

Closing Remark

ISO/IEC 27001 is a management system standard that embraces all the elements of good governance - risk management, system of controls and an audit function (internal) all of which are Mandatory - so we could rename 27001 as a standard defining the

- *Art (techne - τεχηε) of Information Security Management and Governance*
- *And so in the sense of the ancient Greeks use of the word **κυβερνήτης** (cybernetes - to govern, manage, steer) it truly becomes a cyber-security standard*

… οἶον ***κυβερνήτης*** ἄκρος ἢ ἰατρὸς τά τε ἀδύνατα ἐν τῇ τέχνῃ καὶ τὰ δυνατὰ διαισθάνεται … *(Plato 2.360e-361a, Republic)*

*More detailed article "The Art of Cyber - learning from 2500 years of experience of **κυβερ** risks and the role of ISO/IEC 27001" Humphreys, Edward (first edition 2011, revised 2013)*

Thanks for Listening

Edward (Ted) Humphreys

edwardj7@msn.com