ISO/IEC JTC 1/SC 27

Prof Edward Humphreys
SC27/WG1 Convenor
edwardj7@msn.com

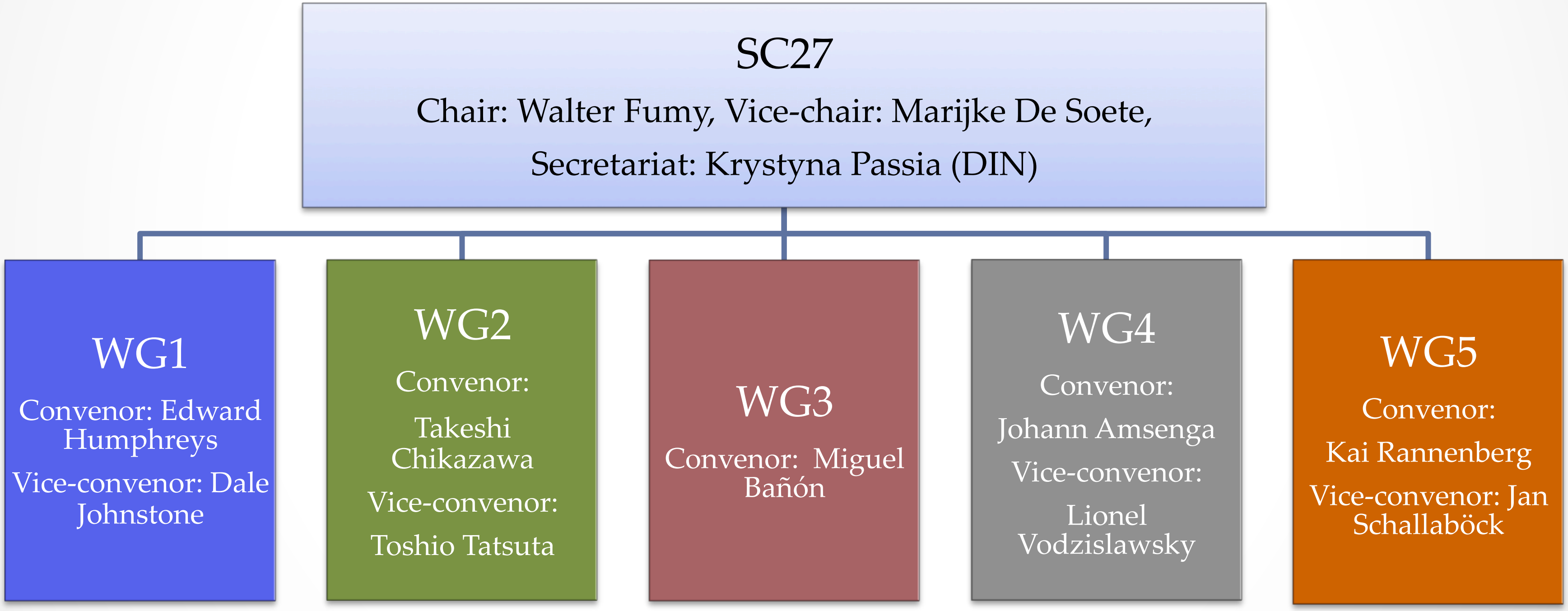
19th Dec 2012

SC27 Mission

SC 27 is an internationally recognized centre of information and IT security standards expertise serving the needs of business sectors as well as governments. Its work covers the development of standards for the protection of information and ICT. This includes **generic methods, techniques and guidelines** to address both **security** and **privacy** aspects, such as:

- Information Security Management Systems (ISMS), requirements, controls and conformance assessment, accreditation and auditing requirements in the area of information security;
- Cryptographic mechanisms;
- Security evaluation criteria and methodology (IT products);
- Security services;
- Security aspects of identity management, biometrics and privacy.

SC27 Working Groups



SC27

Chair: Walter Fumy, Vice-chair: Marijke De Soete,

Secretariat: Krystyna Passia (DIN)

WG1

Convenor: Edward Humphreys

Vice-convenor: Dale Johnstone

WG2

Convenor:

Takeshi Chikazawa

Vice-convenor:

Toshio Tatsuta

WG3

Convenor: Miguel Bañón

WG4

Convenor:

Johann Amsenga

Vice-convenor:

Lionel Vodzislawsky

WG5

Convenor:

Kai Rannenberg

Vice-convenor: Jan Schallaböck

SC27 Members

P-members (voting)

Algeria, Australia, Austria, Belgium, Brazil, Canada, China, Côte-d'Ivoire, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, India, Italy, Ireland, Israel, Japan, Kazakhstan, Kenya, Rep. of Korea, Luxembourg, Malaysia, Mauritius, Mexico, Morocco, The Netherlands, New Zealand, Norway, Peru, Poland, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay. (Total: 49)

O-members (observing)

Argentina, Belarus, Bosnia and Herzegovina, Costa Rica, El Salvador , Ghana, Hong Kong, Hungary, Iceland, Indonesia, Iran, Israel, Kingdom of Saudi Arabia, Lithuania, Portugal, Serbia, Swaziland, Turkey (Total: 18)

Projects Facts & Figures

- **Projects**
  - Total no of projects: 175
  - No of active projects: 75
    - Including for the period of time 2011-11 – 2012-09 new projects: 22
  - Current number of published standards: 116
    - Including for the period of time 2011-11 – 2012-09 new publications: 20
- **Standing Documents** (all freely available from the sites given below)
  - SD6 Glossary of IT Security terminology (http://www.jtc1sc27.din.de/sbe/SD6)
  - SD7 Catalogue of SC 27 Projects and Standards (http://www.jtc1sc27.din.de/sbe/SD7
  - SD11 Overview of SC 27 (http://www.jtc1sc27.din.de/sbe/SD11)
  - SD12 Assessment of cryptographic algorithms and key lengths (http://www.jtc1sc27.din.de/sbe/SD12)

Experts in SC27

- Implementers, developers and managers from commercial organisations
- Government organisations
- Auditors from Certification Bodies
- Assessors from Accreditation Bodies
- Independent consultants
- Academics
- End users

SC27 Liaison Partners

Internal Liaisons within ISO

- ISO/CASCO
- ISO/JTCG Joint technical Coordination Group on MSS
- ISO/TC 46/SC 11 Information and documentation – Archives/Records management
- ISO/TC 68/SC 2 Financial services -- Security
- ISO/TC 176/SC 3 - Quality management and quality assurance - Supporting technologies
- ISO/TC 176/SC 3/WG 16 Quality management and quality assurance – Supporting technologies - Joint WG with TC 207/SC2 for the revision of ISO 19011
- ISO/TC 204 Intelligent transport systems - WG 1 Architecture
- ISO/TC 208 Thermal turbines for industrial application (steam turbines, gas expansion turbines)
- ISO/TC 215 Health Informatics - WG 4 Security
- ISO/TC 223 Societal Security
- ISO/PC 246 Anti-counterfeiting tools
- ISO/PC 251 Project committee: Asset management
- ISO/PC 262 Project committee: Risk management

Internal Liaisons within IEC

- IEC/TC 65 Industrial-process measurement, control and automation - WG 10 Security for industrial process measurement and control - Network and system security

Internal Liaisons within ISO/IEC JTC 1

- JTC 1 Ad Hoc on Vocabulary
- JTC 1/WG 6 Corporate Governance of IT
- JTC 1/WG 7 Sensor networks
- SC 6 Telecommunications and information exchange between systems
- SC 7 Software engineering
- SC 17/WG 3 Machine readable travel documents
- SC 17/WG 4 Integrated circuit cards with contacts
- SC 17/WG 11 Application of Biometrics to Cards and Personal Identification
- SC 22 Programming languages, their environments and system software interfaces
- SC 25 Interconnection of IT Equipment
- SC 31/WG 4 (Automatic Identification and Data Capture Techniques
- SC 36 Information technology for learning, education, and training
- SC 37 Biometrics
- SC 38 Distributed application platforms and services (DAPS)

SC27 Liaison Partners

External CAT A Liaisons

- ECMA International
- ENISA (European Network and Information Security Agency)
- European Payment Council
- ITU Development Sector (ITU-D)
- ITU-T Joint Coordination Activity for Identity Management (JCA-IdM)
- ITU-T Joint Coordination Activity on Cloud Computing (JCA-Cloud)
- ITU-T Study Group 13 (ITU-T SG 17)
- ITU-T Study Group 17 (ITU-T SG 13)
- MasterCard
- VISA Europe

External CAT C Liaisons

- ABC4Trust
- ARTICLE 29 Data Protection Working Party
- ASIS International
- CEN TC 224 Personal identification, electronic signature and cards and their related systems and operations
- Cloud Computing Association (CSA)
- Common Criteria Development Board (CCDB)
- Cyber Security Naming and Information Structure Group Corporation

External CAT C Liaisons

- European Telecommunications Standards Institute (ETSI)
- Forum of Incident Response and Security Teams (FIRST)
- Future of Identity in the Information Society (FIDIS)
- European Network of Excellence for Cryptology II (ECRYPT II)
- Information Security Forum (ISF)
- Information Systems Audit and Control Association/IT Governance Institute (ISACA / ITGI)
- Instituto Latinoamericano de Aseguramiento de la Calidad A. C. (INLAC) (The Latin-American Institute for Quality Assurance A.C.)
- International Conference of Data Protection and Privacy Commissioners
- International Smart Card Certification Initiatives
- International Systems Security Association (ISSA)
- Interpol
- Kantara Initiative
- Privacy and Identity Management for Community Services (PICOS)
- Privacy and Identity Management in Europe for Life (PrimeLife)
- Smart Card Certification Initiatives (ISCI)
- The Open Group
- Trusted Computing Group (TCG)
- TAS3 (Trusted Architecture for Securely Shared Services)

Benefits of SC27 Standards

- **Business**
- Society
- Government

- Cost savings - International Standards can help optimise operations and therefore improve the bottom line
- Enhanced customer satisfaction - International Standards help improve quality, enhance customer satisfaction and increase sales
- Access to new markets - International Standards help prevent trade barriers and open up global markets
- Increased market share - International Standards help increase productivity and competitive advantage

Benefits of SC27 Standards

- Business
- **Society**
- Government

- Consumer confidence - When products and services conform to International Standards consumers can have confidence that they are safe, reliable and of good quality.
- To make sure that the benefits of ISO International Standards are as broad as possible, ISO supports the involvement of consumers in standard development work

Benefits of SC27 Standards

- Business
- Society
- **Government**

- Expert opinion - ISO standards are developed by experts. By integrating an ISO standard into national regulation, governments can benefit from the opinion of experts without having to call on their services directly;
- Opening up the country to world trade benefiting national economies and growth - ISO standards are international and adopted by many governments. By integrating ISO standards into national regulation, governments help to ensure that requirements for imports and exports are the same the world over, therefore facilitating the movement of goods, services and technologies from country-country.

SME Benefits of SC27 Standards

Standards can:

- Help you to compete
  - Giving you a competitive edge
  - Open up export markets for your products and services – creating new business opportunities and sales
  - Add credibility and confidence for your customers
  - Make your brand name internationally recognized
  - Help your company grow and protect, manage and govern itself better
- Drive efficiency in your business operations
- Enable a common "language" to be used across an industry sector
  - Improve communications between buyer and seller, third party suppliers, consumers, customers and clients
  - Help you discover and apply best business practices

Benefit Case Study

- ISO/IEC 27001 Information security management system (ISMS) requirements:
  - ISO/IEC 27001 is a certification standard information security (in the same way that ISO 9001 is for quality, 14001 is for environment etc),
  - ISO/IEC 27001 has become a **common "language"** for information security across all business, industry and government sectors
  - Better management of an organisations information risks
  - Improved performance in protecting information assets and giving better return of (security) investment (ROI/ROSI)
  - Third-party certification audits demonstrating
    - Confidence, trust and assurance
    - 'Fit-for-purpose' to be secure enough to do business with to protect your information

Benefit Case Study and ROSI

Examples of ISO/IEC 27001 and ROI

1. Protect against **Lost of Operations/productivity.** How many employees would be unable to get work done because of a security breach, and for how long? What if your IT were seized by law enforcement for IT forensic analysis? How much time would be spent by security and IT staff repairing damage caused by the breach as opposed to doing other work?

Benefit Case Study and ROSI

Examples of ISO/IEC 27001 and ROI

2. Protect against **Loss of Revenue/income** during system outages. For example web sites that could be taken down by a security incident. How much money might you lose per minute, per hour, or per day in this scenario? What if you lost Internet connectivity – completely or partially?

Benefit Case Study and ROSI

Examples of ISO/IEC 27001 and ROI

3. Protection against **Data Loss**, temporary or permanent. Restoring from a backup can be costly. If an insider destroyed your backups and then deleted data, it could be catastrophic.
4. Protection against **Compromise of Data** such as unauthorised disclosure or modification through. Strategic and product plans, as well as sensitive financial information, are just a couple of examples.

Benefit Case Study and ROSI

Examples of ISO/IEC 27001 and ROI

5. Lowering of **Repair and recovery costs**. You might need to recover lost data, pay legal penalties, buy new hardware, or use disk-recovery services, for example.

6. Organisations can **protect against loss of image, reputation and brand name**. Think about how you'd feel reading about the breach on the front page of a newspaper.

Benefit Case Study and ROSI

Examples of ISO/IEC 27001 and ROI

7. Organisations can protect against non-compliance - **Legal actions** against failing to comply with legislation/ regulations.

8. Return on staff and employee **awareness and training** programmes.

Challenges

a) Engaging stakeholders and users in the development of SC27 standards

- NSBs should inform and seek input from a broad range of relevant national stakeholders – companies, organisations, trade associations, government agencies, consumer interest groups etc

b) Effective and co-operative consensus building

- Recognizing the wider interest and sometimes making certain compromises
- Advancing the global relevance of international standards
- SC27 collaborating with other ISO and JTC1 TCs/SCs and with NSBs, LOs

Challenges

c) Responsive to market and business requirements

- Development of standards in a timely and effective way to meet the needs of the market
- Keeping up with developments in modern business systems, technology

d) Responsive to information security requirements

- Monitoring and responding with standards that address the growing risks and threats (e.g. cyber-security, Cloud services, identity theft and personally identifiable information (PII) etc)
- Growth in legislation and regulation

e) Getting the message across

- Promoting the value, benefits, strength and the authority of SC27 standards in the marketplace

National Incentives of Getting Involved

- Why get should organisations get involved?
  - Giving your company early access to information that could shape the market in the future
  - Giving your company a voice in the development of standards
  - Getting involved in standards development brings your concerns and needs to bear on a process that will affect you in the future.

National Incentives of Getting Involved

Why get should organisations get involved?

"The payoff for engaging in standards work is greater than many small business people realize … it's essential to get involved with the working groups so we can get started early with our planning for future designs and production methods. Globalization means that ISO standards are key for any company that hopes to succeed in export markets." Per Frode (CEO, Sweden)

"What does it cost me if I do not get involved and others define rules that are out of line with my needs, interests and experiences, but which I have to comply with because they are laid down in a standard ? Hence, it is best to join in right at the start." Martin Denison (Managing Director, Austria)

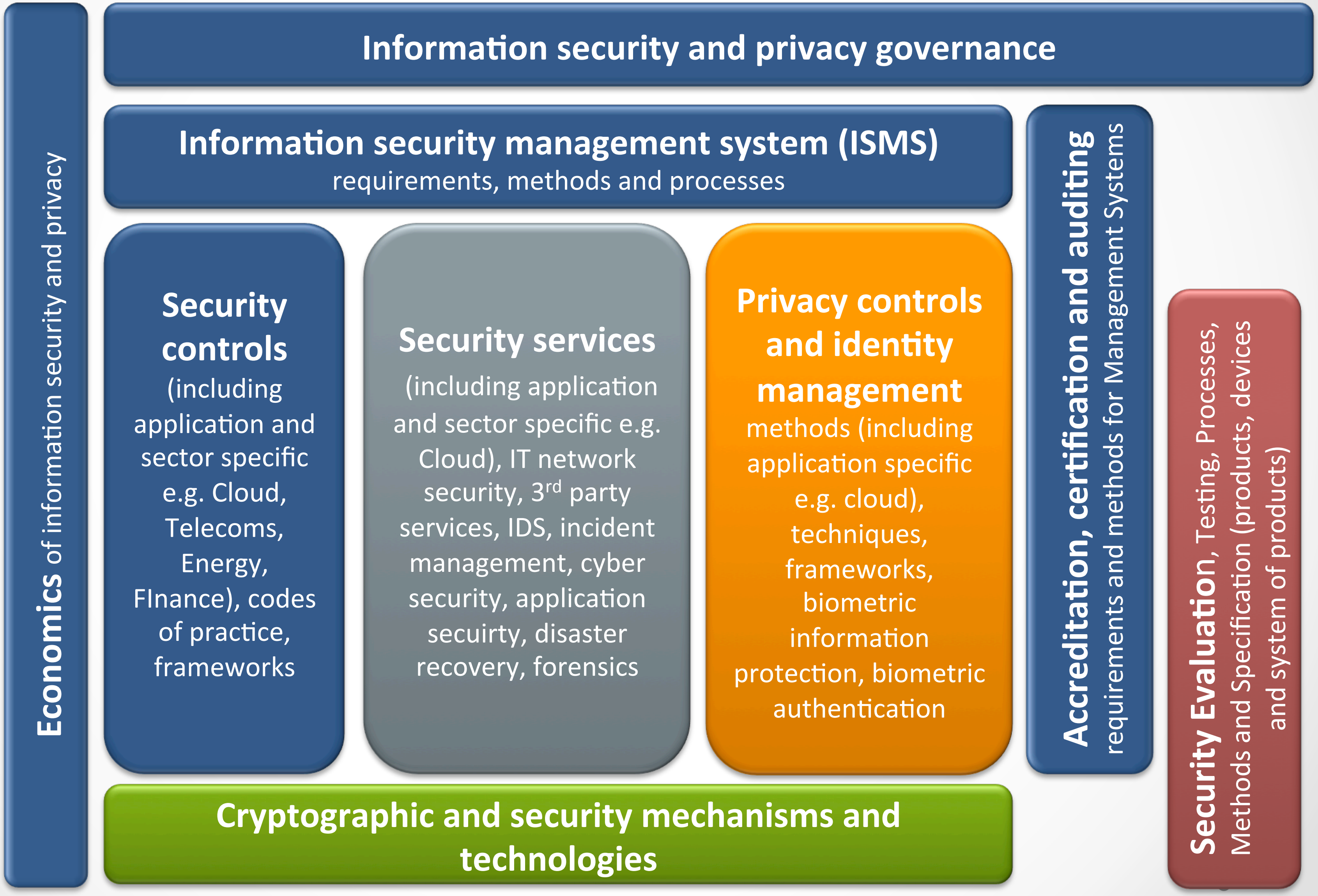
"Taking part in standardization work on nanotechnologies allows our company to have access to standardization developments. Furthermore, this gives us the opportunity to join in and defend current and future interests of Spanish industry. Participating in both national and international standardization committees is a key matter for our company. We are in a time of strong international growth and this participation will allow us to adapt our products to future international regulations."
Julio Gomez (CEO, Spain)

http://www.iso.org/iso/home/standards_development/standardsdevelopment_gettinginvolved.htm

National Incentives of Getting Involved

- Contributing national requirements
  - Influencing the development of standards by bringing national expertise and experience into the development
  - Ensuring national interests gain attention and helping to keep market access open
- Gaining national access to international experts and developments
  - Exchange and Transfer of experiences, knowledge and know-how

SC27 Security and Privacy Topic Areas



Information security and privacy governance

Information security management system (ISMS)
requirements, methods and processes

Economics of information security and privacy

Security controls (including application and sector specific e.g. Cloud, Telecoms, Energy, FInance), codes of practice, frameworks

Security services (including application and sector specific e.g. Cloud), IT network security, 3rd party services, IDS, incident management, cyber security, application secuirty, disaster recovery, forensics

Privacy controls and identity management methods (including application specific e.g. cloud), techniques, frameworks, biometric information protection, biometric authentication

Accreditation, certification and auditing
requirements and methods for Management Systems

Security Evaluation, Testing, Processes, Methods and Specification (products, devices and system of products)

Cryptographic and security mechanisms and technologies

WG 1	🟦
WG 2	🟩
WG 3	🟥
WG 4	⬜
WG 5	🟧

SC27 WG1 Mission

Information Security Management Systems

The scope covers all aspects of standardisation related to information security management system(s) ISMS:

a) Requirements;
b) Methods and processes;
c) Security controls;
d) Sector and application specific use of ISMS;
e) Accreditation, certification, auditing of ISMS;
f) Information security governance;
g) Information security economics.

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27001	Information security management systems – Requirements	1st ed. 2005 Under revision	This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's business activities and the risks it faces.
ISO/IEC 27002	Code of practice for information security controls	1st ed. 2005 Under revision	This International Standard offers a collection of commonly accepted information security control objectives and controls and includes guidelines for implementing these controls. This standard may serve as a practical guideline for developing organizational security standards and effective security management practices.
ISO/IEC 27003	Information security management system implementation guidance	1st ed. 2010	This will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review and improve the ISMS.
ISO/IEC 27004	Information security management measurements	1st ed. 2009 Under revision	This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. This International Standard provides guidance for measurement procedures and techniques to determine the effectiveness of information security controls and information security processes applied in an ISMS.
ISO/IEC 27005	Information security risk management	2nd ed. 2011	This standard ISO/IEC 27005 provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	2nd ed. 2011 Under revision	The scope of this standard is to specify general requirements a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration. This International Standard follows the structure of ISO/IEC 17021 with the inclusion of additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification.
ISO/IEC 27007	Guidelines for information security management systems auditing	1st ed. 2011	This International Standard provides guidance on conducting information security management system (ISMS) audits, as well as guidance on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. It is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.
ISO/IEC 27008	Guidelines for auditors on ISMS controls	1st ed. 2012	This Technical Report provides guidance for assessing the implementation of ISMS controls selected through a risk-based approach for information security management. It supports the information security risk management process and assessment of ISMS controls by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required ISMS controls are implemented.

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications	1st ed. 2012	This International Standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-sector communications.
ITU-T X.1051 | ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	1st ed. 2008	This Recommendation | International Standard: a) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications organizations based on ISO/IEC 27002; b) provides an implementation baseline of Information Security Management within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities and services.
ISO/IEC 27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	1st ed. 2012	This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations which are intending to either: a. Implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa; b. Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or c. Align existing ISO/IEC 27001 and ISO/IEC 20000-1 management system (MS) implementations.

WG1 Standards

Standard	Title	Status	Abstract
ISO/IEC 27014	Information security governance framework	1st ed. 2013	This International Standard provides guidance on the development and use of governance of information security (GIS) through which organisations direct and control the information security management system (ISMS) process as specified in ISO/IEC 27001. This International Standard provides guiding principles for top management of organisations on the effective, efficient, and acceptable use of information security within their organisations.
ISO/IEC 27015	Guidelines for information security management system for financial and insurance services sector	1st ed. 2012	This International Standard provides requirements, guidelines and general principles for initiating, implementing, maintaining, and improving the information security management within finance and insurance sectors based upon ISO/IEC 27001 and ISO/IEC 27002.
ISO/IEC 27016	Information security management - Organisational economics	4th WD 2012	This technical report provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. This Technical Report is applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by managers who have responsibility for information security decisions.
ISO/IEC 27017	Guidelines on Information security controls for the use of cloud computing services based on ISO/ IEC 27002	3rd WD 2012	The scope of this Technical Specification/ International Standard is to define guidelines supporting the implementation of Information Security Management for the use of cloud service. The adoption of this Technical Specification/ International Standard allows cloud consumers and providers to meet baseline information security management with the selection of appropriate controls and implementation guidance based on risk assessment for the use of cloud service.

SC27 WG2 Mission

Cryptography and Security Mechanisms

- The Terms of Reference:
  - a) Identify the need and requirements for these techniques and mechanisms in IT systems and applications; and
  - b) Develop terminology, general models and standards for these techniques and mechanisms for use in security services.
- The scope covers both cryptographic and non-cryptographic techniques and mechanisms including;
  - a) Confidentiality;
  - b) Entity authentication;
  - c) Non-repudiation;
  - d) Key management; and
  - e) Data integrity such as
    - Message authentication,
    - Hash-functions, and
    - Digital signatures.

WG2 Standards

Standard	Title	Status	Abstract
ISO/IEC 18033-1	**Encryption algorithms** Part 1: General	1st ed. 2005 Under revision	This International Standard specifies asymmetric ciphers (including identity-based ciphers) and symmetric ciphers (block ciphers and stream ciphers).
-2	Part 2: Asymmetric ciphers	1st ed. 2006	
-3	Part 3: Block ciphers	2nd ed. 2010	This International Standard specifies symmetric ciphers (block ciphers and stream ciphers) and mechanisms using asymmetric techniques (authentication, key exchange and identity-based signature) which are suitable for lightweight cryptographic applications.
-4	Part 4: Stream ciphers	2nd ed. 2011	
-5	Part 4: Identity-based ciphers	Under development	
ISO/IEC 29192-1	**Lightweight cryptography** Part 1: General	1st ed. 2012	
-2	Part 2: Block ciphers	1st ed. 2012	This International Standard specifies methods for authenticated encryption, i.e., defined ways of processing a data string for data confidentiality, data integrity and data origin authentication.
-3	Part 3: Stream ciphers	Under development	
-4	Part 4: Mechanisms using asymmetric techniques	Under development	
ISO/IEC 19772	**Authenticated encryption**	1st ed. 2009	
ISO/IEC 29150	**Signcryption**	1st ed. 2011	This International specifies mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to their own public and private key pairs.
ISO/IEC 10116	**Modes of operation for an n-bit block cipher algorithm**	3rd ed. 2006	
ISO/IEC 10118-1	**Hash-functions** Part 1: General	2nd ed. 2000	
-2	Part 2: Hash-functions using an n-bit block cipher	3rd ed. 2010	This International Standard specifies modes of operation for a block cipher algorithm, i.e., ECB, CBC, OFB, CFB and CTR.
-3	Part 3: Dedicated hash-functions	3rd ed. 2006	This International Standard specifies some kinds of hash-functions which map arbitrary strings of bits to a given range.
-4	Part 4: Hash-functions using modular arithmetic	1st ed. 1998	
ISO/IEC 15946-1	**Cryptographic techniques based on elliptic curves** Part 1: General	2nd ed. 2008	This International Standard describes the mathematical background and general techniques in addition to the elliptic cuerve generation techniques.
-5	Part 5: Elliptic curve generation	1st ed. 2009	

WG2 Standards

Standard	Title	Status	Abstract
ISO/IEC 9796-2	**Digital signature schemes giving message recovery** Part 2: Integer factorization based mechanisms	3rd ed. 2010	This International Standard specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead.
-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006	
ISO/IEC 14888-1	**Digital signatures with appendix** Part 1: General	2nd ed. 2008	This International Standard specifies digital signature mechanisms with appendix.
-2	Part 2: Integer factorization based mechanisms	2nd ed. 2008	
-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006	This International Standard specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.
ISO/IEC 20008-1	**Anonymous digital signatures** Part 1: General	Under development	
-2	Part 2: Mechanisms using a group public key	Under development	
ISO/IEC xxxxx-1	**Blind digital signatures** Part 1: General	Under development	This International Standard specifies blind digital signature mechanisms which allow a recipient to obtain a signature without giving signer any information about the actual message or resulting signature.
-2	Part 2: Discrete logarithm based mechanisms	Under development	
ISO/IEC 9798-1	**Entity authentication** Part 1: General	3rd ed. 2010	
-2	Part 2: Mechanisms using symmetric encipherment algorithms	3rd ed. 2008	This International Standard specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret.
-3	Part 3: Mechanisms using digital signature techniques	2nd ed. 1998	
-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009	
-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	This International Standard specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity.
ISO/IEC 20009-1	**Anonymous entity authentication** Part 1: General	Under development	
-2	Part 2: Mechanisms based on signatures using a group public key	Under development	
-3	Part 3: Mechanisms based on blind signatures	Under development	

WG2 Standards

Standard	Title	Status	Abstract
ISO/IEC 9797-1	**Message authentication codes (MACs)** Part 1: Mechanisms using a block cipher	2nd ed. 2011	This International Standard specifies message authentication code (MAC) algorithms, which are data integrity mechanisms that compute a short string.
-2	Part 2: Mechanisms using a dedicated hash-function	2nd ed. 2011	
-3	Part 3: Mechanisms using a universal hash-function	1st ed. 2011	This International Standard specifies a set of check character systems capable of protecting strings against errors.
ISO/IEC 7064	**Check character systems**	1st ed. 2003	
ISO/IEC 11770-1	**Key management** Part 1: Framework	2nd ed. 2010	This International Standard describes general models on which key management mechanisms are based, defines the basic concepts of key management, and defines several kinds of key establishment mechanisms .
-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2008	
-3	Part 3: Mechanisms using asymmetric techniques	2nd ed. 2008 Under revision	
-4	Part 4: Mechanisms based on weak secrets	1st ed. 2004	The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. The event or act on can be the generation of a message, sending of a message, receipt of a message, submission of a message transport of a message. This International Standard specifies for the provision of non-repudiation services.
-5	Part 5: Group key management	1st ed. 2011	
ISO/IEC 13888-1	**Non-repudiation** Part 1: General	3rd ed. 2009	
-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2010	
-3	Part 3: Mechanisms using asymmetric techniques	2nd ed. 2009	
ISO/IEC 18014-1	**Time-stamping services** Part 1: Framework	2nd ed. 2008	This International Standard defines time-stamping services that are provided using time-stamp tokens between the participanting entities in addition to the traceability of time sources.
-2	Part 2: Mechanisms producing independent tokens	2nd ed. 2009	
-3	Part 3: Mechanisms producing linked tokens	2nd ed. 2009	This International Standard specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model.
-4	Part 4: Traceability of time sources	Under development	
ISO/IEC 18031	**Random bit generation**	2nd ed. 2011	
ISO/IEC 18032	**Prime number generation**	1st ed. 2005	This standard presents methods for generating prime numbers as required in cryptographic protocols and algorithms.

WG3 Mission

Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

a) security evaluation criteria;

b) methodology for application of the criteria;

c) security functional and assurance specification of IT systems, components and products;

d) testing methodology for determination of security functional and assurance conformance;

e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 11889	Trusted Platform Module	1st Ed	ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general.
ISO/IEC 15408	Evaluation criteria for IT security	3rd Ed	ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
ISO/IEC TR 15443	A framework for IT security assurance	1st Ed Under revision	ISO/IEC TR 15443 guides the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel.
ISO/IEC TR 15446	Guide for the production of Protection Profiles and Security Targets	2nd Ed.	ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408.
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	3rd WD	This International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4.
ISO/IEC 18045	Methodology for IT security evaluation	3rd Ed	ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 19790	Security requirements for cryptographic modules	2nd Ed	ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems
ISO/IEC TR 19791	Security assessment of operational systems	2nd Ed	ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems.
ISO/IEC 19792	Security evaluation of biometrics	1st Ed	ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system.
ISO/IEC 21827	Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)	2nd Ed	ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.
ISO/IEC TR 20004	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	1st Ed	ISO/IEC TR 20004:2012 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.
ISO/IEC 24759	Test requirements for cryptographic modules	1st Ed Under review	ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006.
ISO/IEC 28128	Verification of cryptographic protocols	1st Ed	ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 29147	Vulnerability Disclosure	DIS	This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services.
ISO/IEC TR 29193	Secure system engineering principles and techniques	PDTR	ISO/IEC TR 29193 offers guidance on secure system engineering for Information and Communication Technology systems or products.
ISO/IEC TR 30104	Physical security attacks, mitigation techniques and security requirements	WD	This Technical Report addresses how security assurance can be stated for products where the risk of the security environment requires the support of physical protection mechanisms.
ISO/IEC 30111	Vulnerability handling processes	CD	This International Standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services.
ISO/IEC 30127	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis	WD	This Technical Report provides guidelines for the planning, development and execution of penetration testing under ISO/IEC 15408 and ISO/IEC 18045 Vulnerability Assessment for software targets of evaluation.

SC27 WG4 Mission

Security controls and services

- Developing and maintaining International Standards, Technical Specifications and Technical Reports for information security in the area of *Security Controls and Services*, to assist organizations in the implementation of the ISO/IEC 27000-series of *Information Security Management Systems* (ISMS) International Standards and Technical Reports

- Also the Scope of WG4 includes evaluating and developing International Standards for addressing existing and emerging information security issues and needs and other security aspects that resulted from the proliferation and use of ICT and Internet related technology in organizations (such as multi-nationals corporations, SMEs, government departments, and non-profit organisations).

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party services	1st Ed. 2002	This Technical Report provides guidance for the use and management of Trusted Third Party (TTP) services, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. This Technical Report identifies different major categories of TTP services including time stamping, non-repudiation, key management, certificate management, and electronic notary public.
ISO/IEC 15816	Security information objects for access control	1st Ed. 2002	This International Standard provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1).
ISO/IEC 15945	Specification of TTP services to support the application of digital signatures	1st Ed. 2002	This International Standard defines the services required to support the application of digital signatures for non-repudiation of creation of a document. Since this implies integrity of the document and authenticity of the creator, the services described can also be combined to implement integrity and authenticity services.
ISO/IEC 18028-2	IT network security – Part 2: Network security architecture	1st Ed. 2006 (Being revised by ISO/IEC 27033-2)	This International Standard defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where end-to-end security is a concern and independently of the network's underlying technology.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 18028-3	IT network security – Part 3: Securing communications between networks using security gateways	1st Ed. 2005 (Being revised by ISO/IEC 27033-4)	This International Standard provides an overview of security gateways through a description of different architectures. It outlines the techniques for security gateways to analyse network traffic, and provides guidelines for the selection and configuration of security gateways.
ISO/IEC 18028-4	IT network security – Part 4: Securing remote access	1st Ed. 2005	This International Standard provides guidance for securely using remote access – a method to remotely connect a computer either to another computer or to a network using public networks – and its implication for IT security. In this it introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely.
ISO/IEC 18028-5	IT network security – Part 5: Securing communications across networks using virtual private networks	1st Ed. 2006 (Being revised by ISO/IEC 27033-5)	This International Standard provides detailed direction with respect to the security aspects of using Virtual Private Network (VPN) connections to inter-connect networks, and also to connect remote users to networks. It provides an overview of VPNs, presents VPN security objectives, and summarizes VPN security requirements. It gives guidance on the selection of secure VPNs, on the implementation of secure VPNs, and on the network monitoring of VPN security. It also provides information on typical technologies and protocols used by VPNs.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 18043	Selection, deployment and operations of intrusion detection systems	1st Ed. 2006 (Being revised by ISO/IEC 27039)	This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection System (IDS). In particular, it addresses the selection, deployment and operations of IDS. It also provides background information from which these guidelines are derived.
ISO/IEC 24762	Guidelines for information and communications technology disaster recovery services	1st Ed. 2008	This International Standard provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management, applicable to both "in-house" and "outsourced" ICT DR service providers of physical facilities and services. It covers the requirements that service providers should meet, recognizing that individual organizations may have additional requirements that are specific to them.
ISO/IEC 27031	Guidelines for ICT readiness for business continuity	1st Ed. 2011	This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.
ISO/IEC 27033-1	Network Security – Part 1: Overview and concepts	1st Ed. 2009 (Revision of 18028-1)	This International Standard provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services and end-users, in addition to security of the information being transferred across the communication links.) Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts.

WG4 Standards

Standard	Title	Status	Abstract
ISO/IEC 27033-3	Network Security – Part 3: Reference networking scenarios – Risks, design techniques and control issues	1st Ed. 2010	This International Standard describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. The information in this International Standard is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls.
ISO/IEC 27034-1	Application security – Part 1: Overview and concepts	1st Ed. 2011	ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications. This International Standard presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.
ISO/IEC 27035	Information security incident management	1st Ed. 2011	This International Standard provides a structured and planned approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.
ISO/IEC TR 29149	Best practice on the provision and use of time-stamping services	1st Ed. 2012	This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness and data integrity services, or non-repudiation services (in conjunction with other mechanisms). It covers time-stamp services, explaining how to generate, renew, and verify time-stamp tokens.

SC27 WG 5 Mission

Identity Management & Privacy Technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - Identity management
  - Biometrics, and
  - Privacy

WG 5 Standards

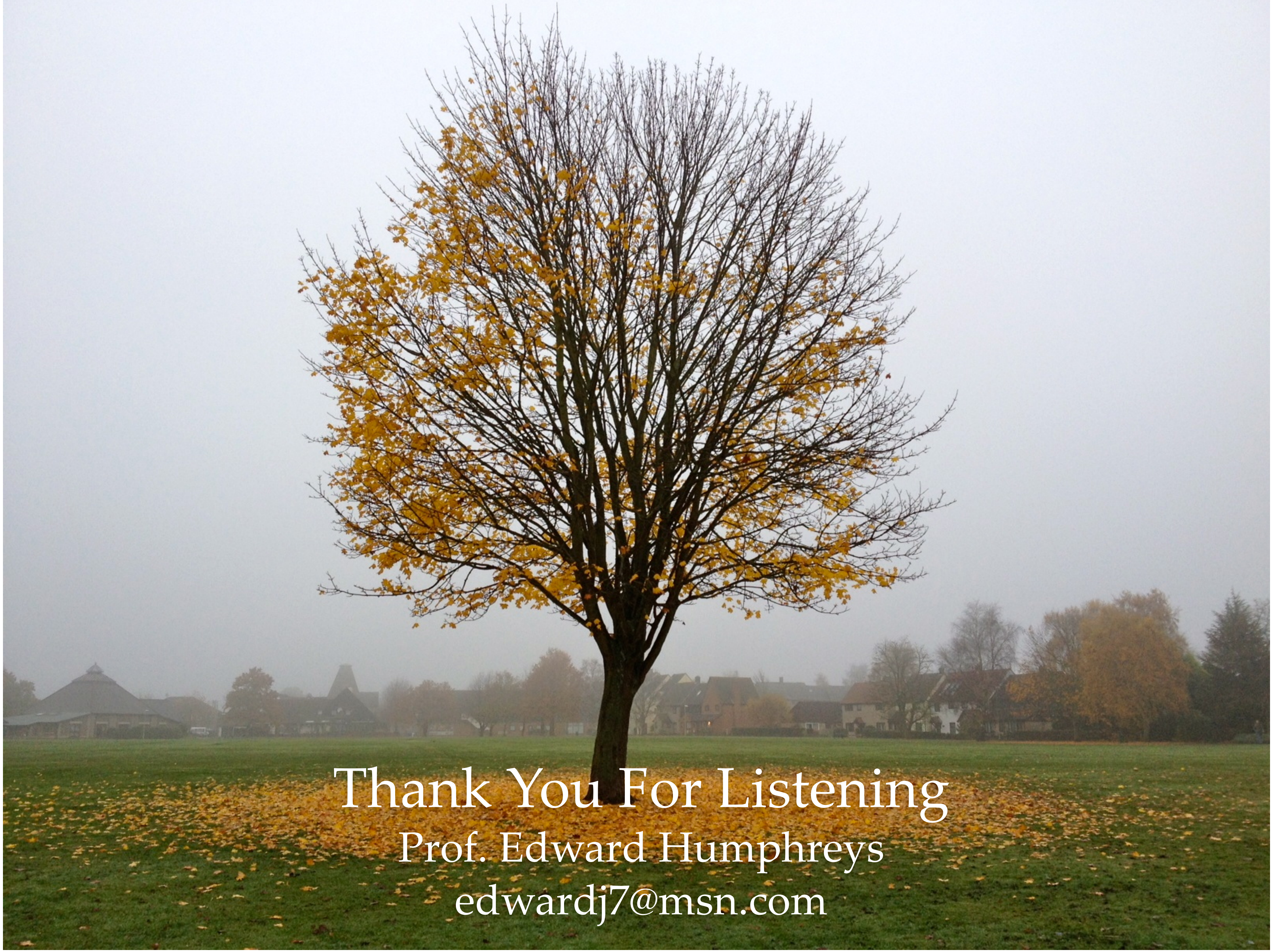
Standard	Title	Status	Abstract
ISO/IEC 24761	Authentication context for biometrics	1st ed. 2009 Technical corr. under vote	ISO/IEC 24761 specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. It allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. ISO/IEC 24761 also specifies the cryptographic syntax of an ACBio instance based on an abstract Cryptographic Message Syntax (CMS) schema.
ISO/IEC 24745	Biometric information protection	1st ed. 2011 1st Pre-review 2014	ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. It does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

WG 5 Standards

Standard	Title	Status	Abstract
ISO/IEC 24760:1	A framework for identity management -- Part 1: Terminology and concepts	1st ed. 2011 1st Pre-review 2014	ISO/IEC 24760-1 • defines terms for identity management, and • specifies core concepts of identity and identity management and their relationships. To address the need to efficiently and effectively implement systems that make identity-based decisions ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations. ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations. Pat 1 of ISO/IEC 24760 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.

WG 5 Standards

Standard	Title	Status	Abstract
ISO/IEC 29100	Privacy framework	1st ed. 2011 1st Pre-review 2014	ISO/IEC 29100 provides a privacy framework which • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology. ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.



Thank You For Listening

Prof. Edward Humphreys

edwardj7@msn.com