Entschuldigen Sie mich, I did not understand, parlez-vous IT Методы обеспечения защиты?

World Standards Day 2015
ILNAS
2015-10-14

Cédric Mauny, Vice-Chairman of Luxembourg National Committee
ISO/IEC JTC1 SC27 on IT Security techniques

Security Audits and Governance Services (SAGS) – a Telindus Security department

together with

Excuse me, I did not understand, do you speak IT Security Techniques?

World Standards Day 2015
ILNAS
2015-10-14

Cédric Mauny, Vice-Chairman of Luxembourg National Committee
ISO/IEC JTC1 SC27 on IT Security techniques

Security Audits and Governance Services (SAGS) – a Telindus Security department

together with

Agenda

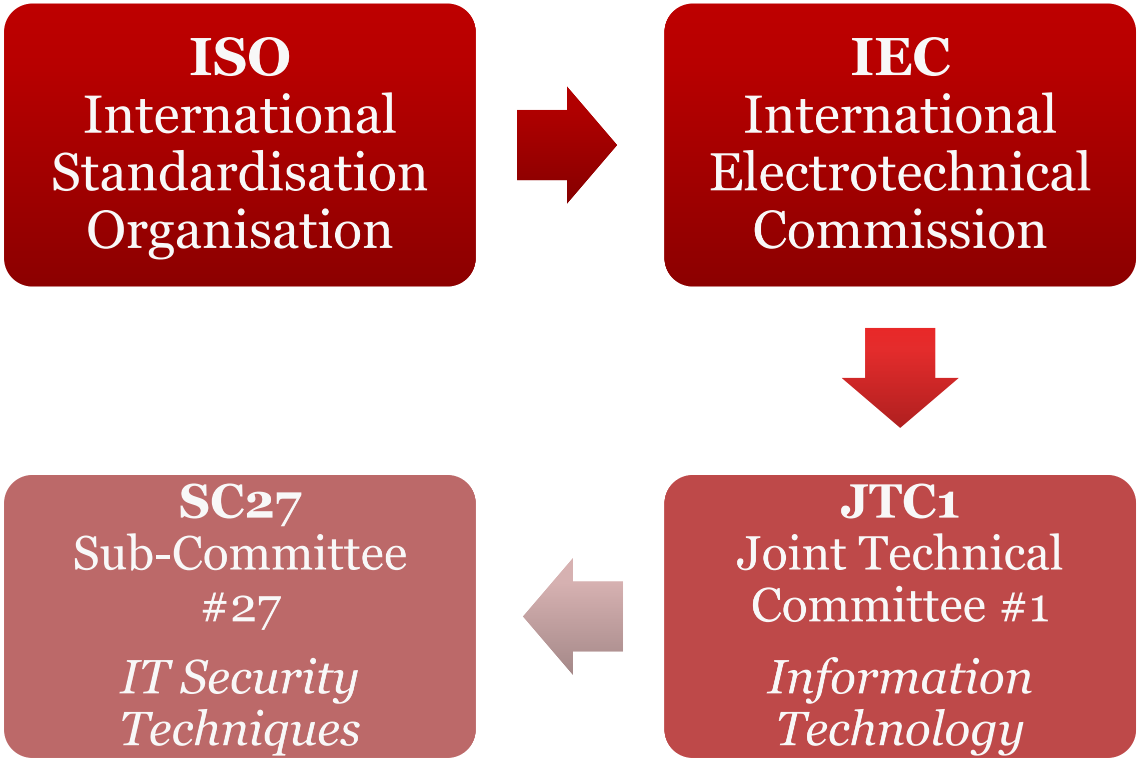
- Presentation of the *IT Security Techniques* within ISO
- Overview of some SC27 International Standards
- Focus on Cloud Computing
  About Security & Privacy
- How to take part into the standardization work?
- SC27 IT Security Techniques in *1 slide*

together with

Presentation of the *IT Security Techniques* within ISO

Information security within ISO

From ISO to ISO/IEC JTC1 SC27



ISO
International Standardisation Organisation

IEC
International Electrotechnical Commission

JTC1
Joint Technical Committee #1

Information Technology

SC27
Sub-Committee #27

IT Security Techniques

ISO International Organization for Standardization
Organisation internationale de normalisation

IEC Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

Leadership of SC27 IT Security Techniques

- Internationally recognized centre of information and IT security standards expertise

International Organization for Standardization
Organisation internationale de normalisation

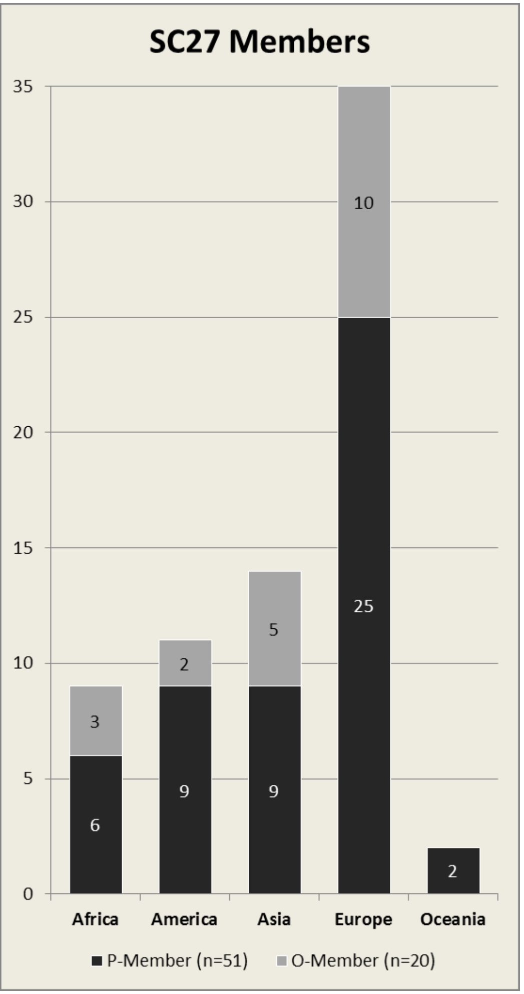
- Serves the needs of all business sectors
  - Public and Private sectors
  - Including governments

- Covers the development of standards for the protection of information and ICT
  - Includes generic methods, techniques and guidelines
  - Addresses both *security* and *privacy* aspects

IEC
Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

Centre of information and IT security standards expertise

Generic methods, techniques and guidelines

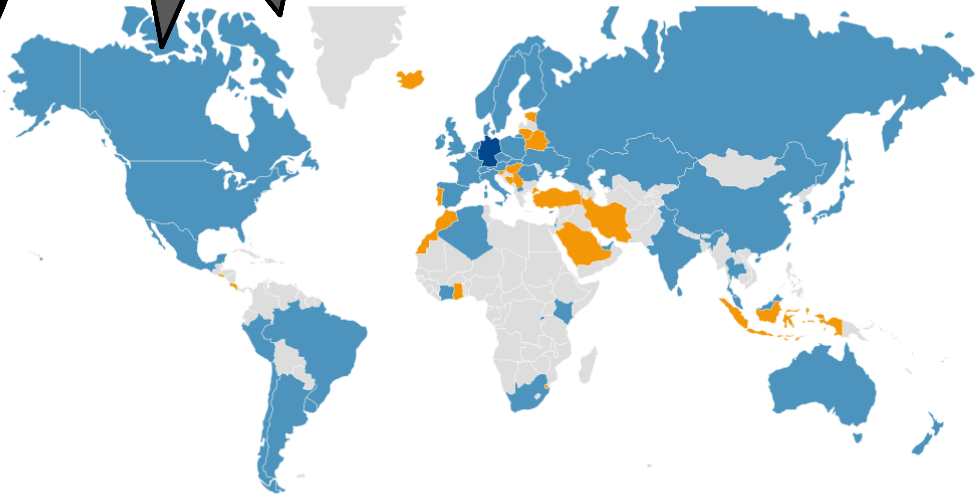


51

P-Members

1 country

1 vote

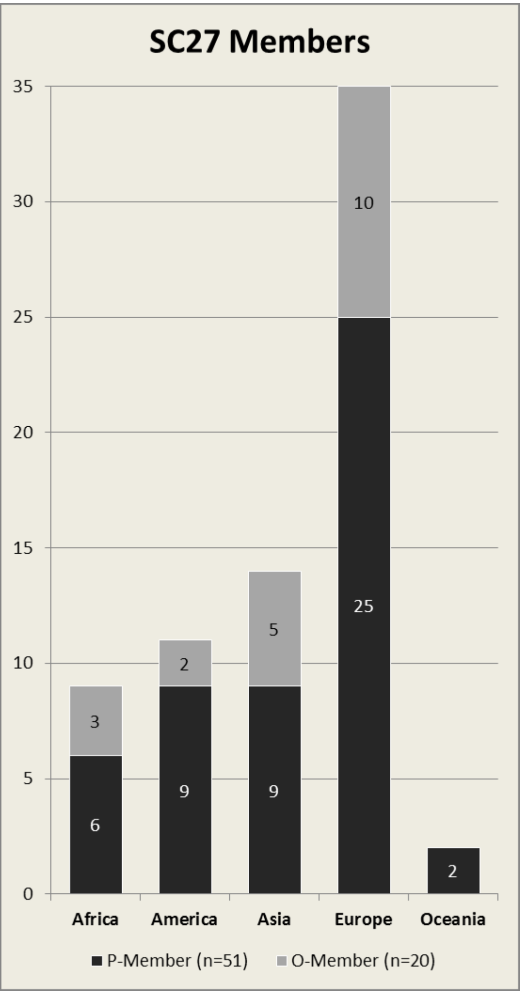


20

O-Members

Centre of information and IT security standards expertise

Generic methods, techniques and guidelines



51

P-Members

+

20

O-Members

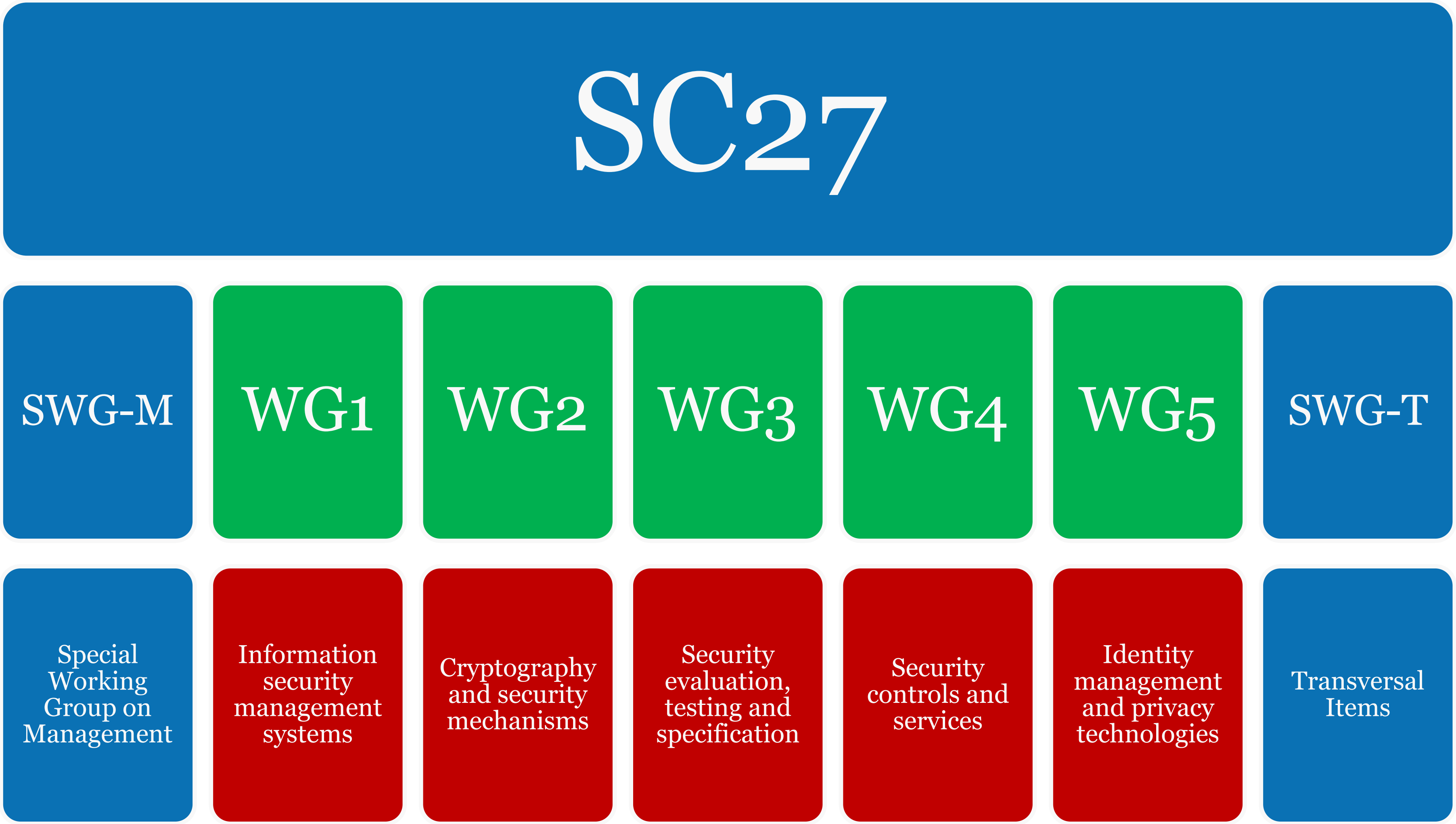
150 published standards

75 standards under development

108 withdrawn standards

ISO/IEC JTC1 SC27

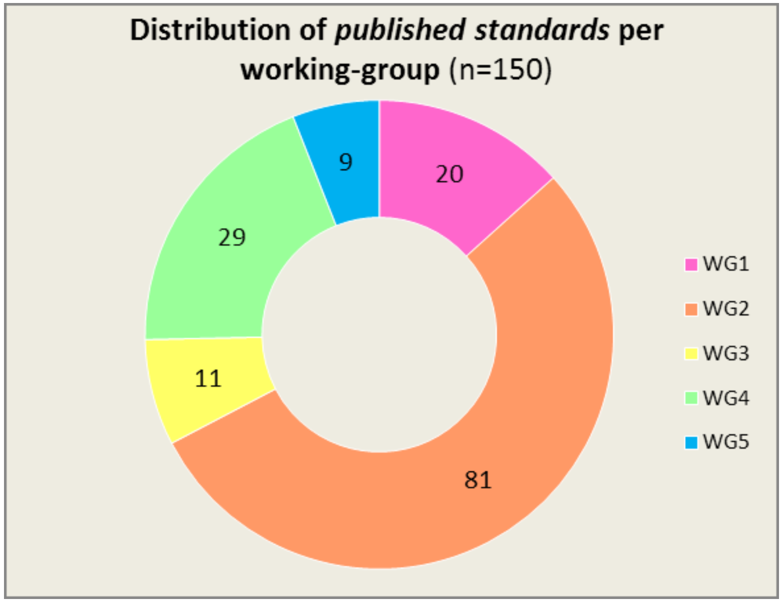
IT Security Techniques

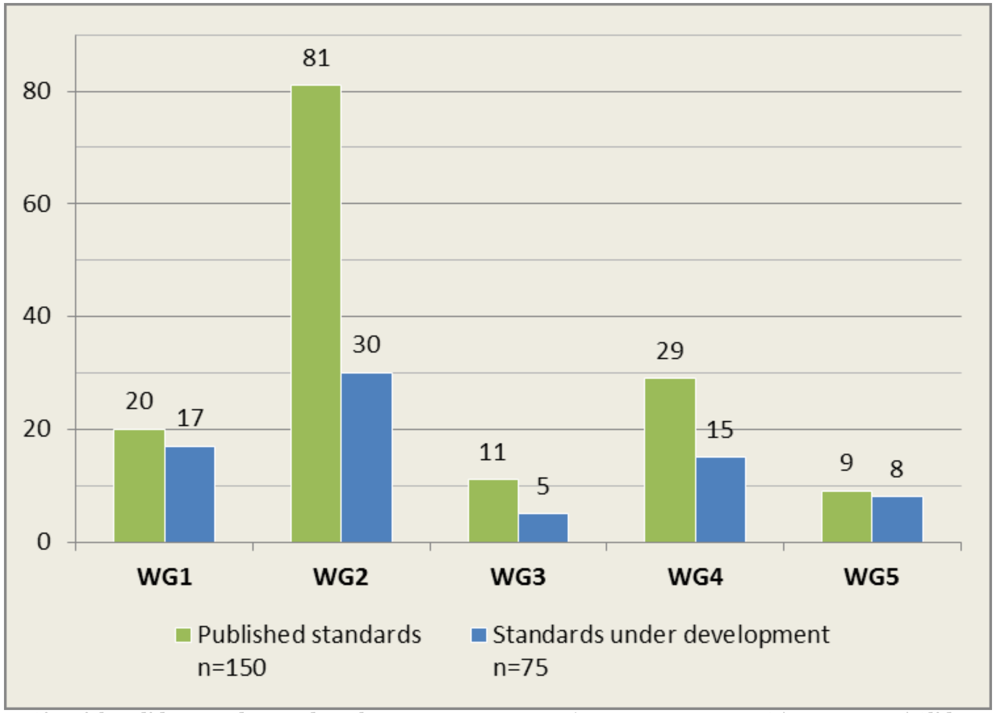


SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

Current status of Published / Under development Standards





WG1 → ISMS
WG2 → Cryptography
WG3 → Security evaluation
WG4 → Controls and services
WG5 → Privacy technologies

Overview of some SC27 International Standards

ISO/IEC JTC1 SC27
IT Security Techniques

SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

Information Security Management Systems are everywhere!

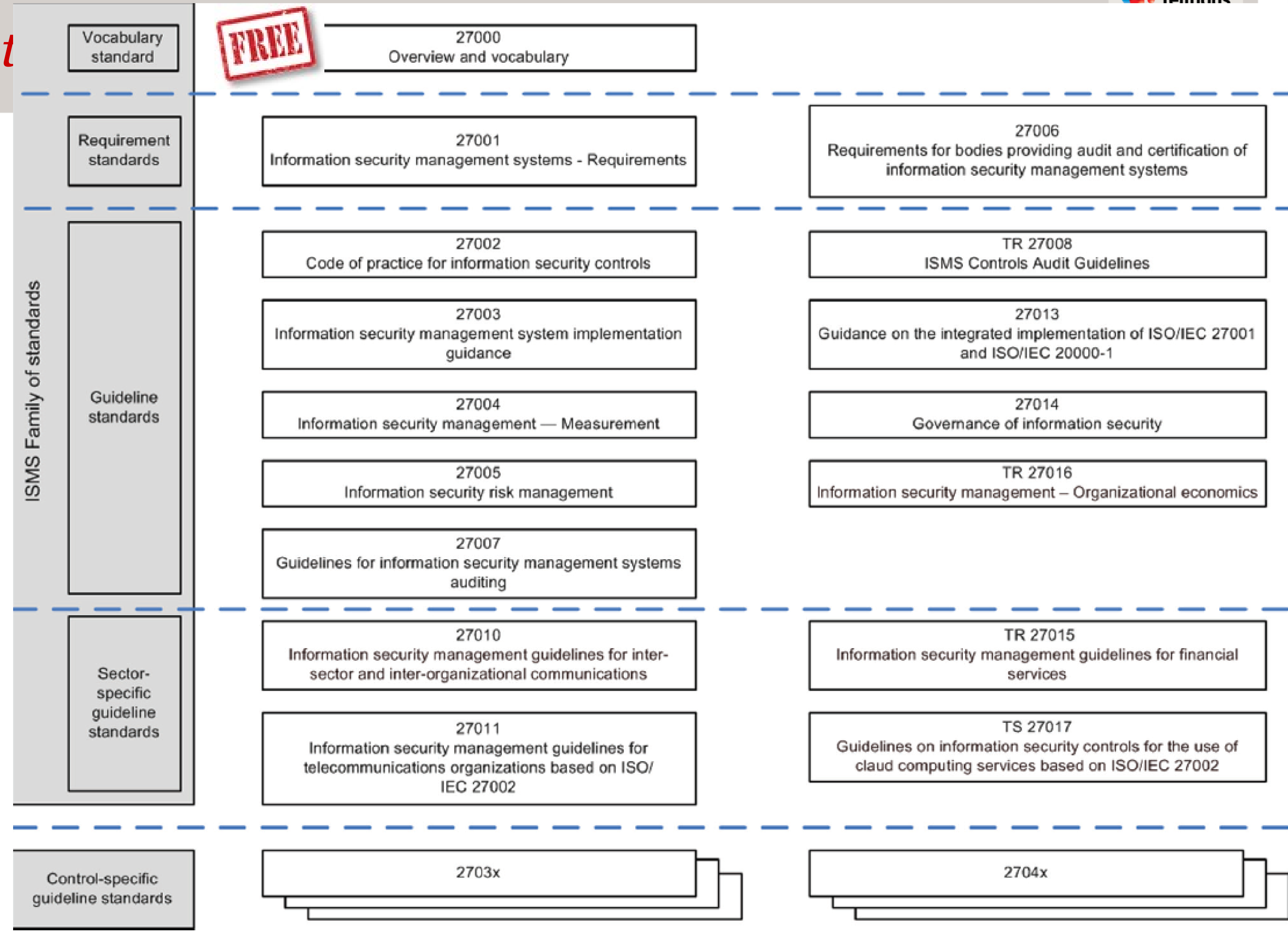
WG1
Informat

16 Standards

- <= 27009 : Core-ISMS Standards
- >= 27010 : Sector-Specific Standards

Not attributed

- 27012
- 27020



Vocabulary standard	27000 Overview and vocabulary	
Requirement standards	27001 Information security management systems - Requirements	27006 Requirements for bodies providing audit and certification of information security management systems
Guideline standards	27002 Code of practice for information security controls	TR 27008 ISMS Controls Audit Guidelines
	27003 Information security management system implementation guidance	27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
	27004 Information security management — Measurement	27014 Governance of information security
	27005 Information security risk management	TR 27016 Information security management – Organizational economics
	27007 Guidelines for information security management systems auditing	
Sector-specific guideline standards	27010 Information security management guidelines for inter-sector and inter-organizational communications	TR 27015 Information security management guidelines for financial services
	27011 Information security management guidelines for telecommunications organizations based on ISO/ IEC 27002	TS 27017 Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002
Control-specific guideline standards	2703x	2704x

Figure 1 — ISMS Family of Standards Relationships

source: ISO/IEC 27000:2014 : Information technology — Security techniques — Information security management systems — Overview and vocabulary

WG1
Other Standards

- Published
  - 27013
    - Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
    - 2012 + under revision at FDIS
  - 27018
    - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
    - 2014

    → see WG5
  - 27019
    - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
    - 2013

- Under development
  - 27009
    - Sector-specific application of ISO/IEC 27001 – Requirements
    - 2nd CD
  - 27017
    - Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002
    - FDIS
  - 27021
    - Competence Requirements for information security Management Professionals
    - NP
  - Cloud Adapted Risk Management Framework
    - SP
  - Information Security Library
    - SP

ISO/IEC JTC1 SC27
IT Security Techniques

SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

WG2

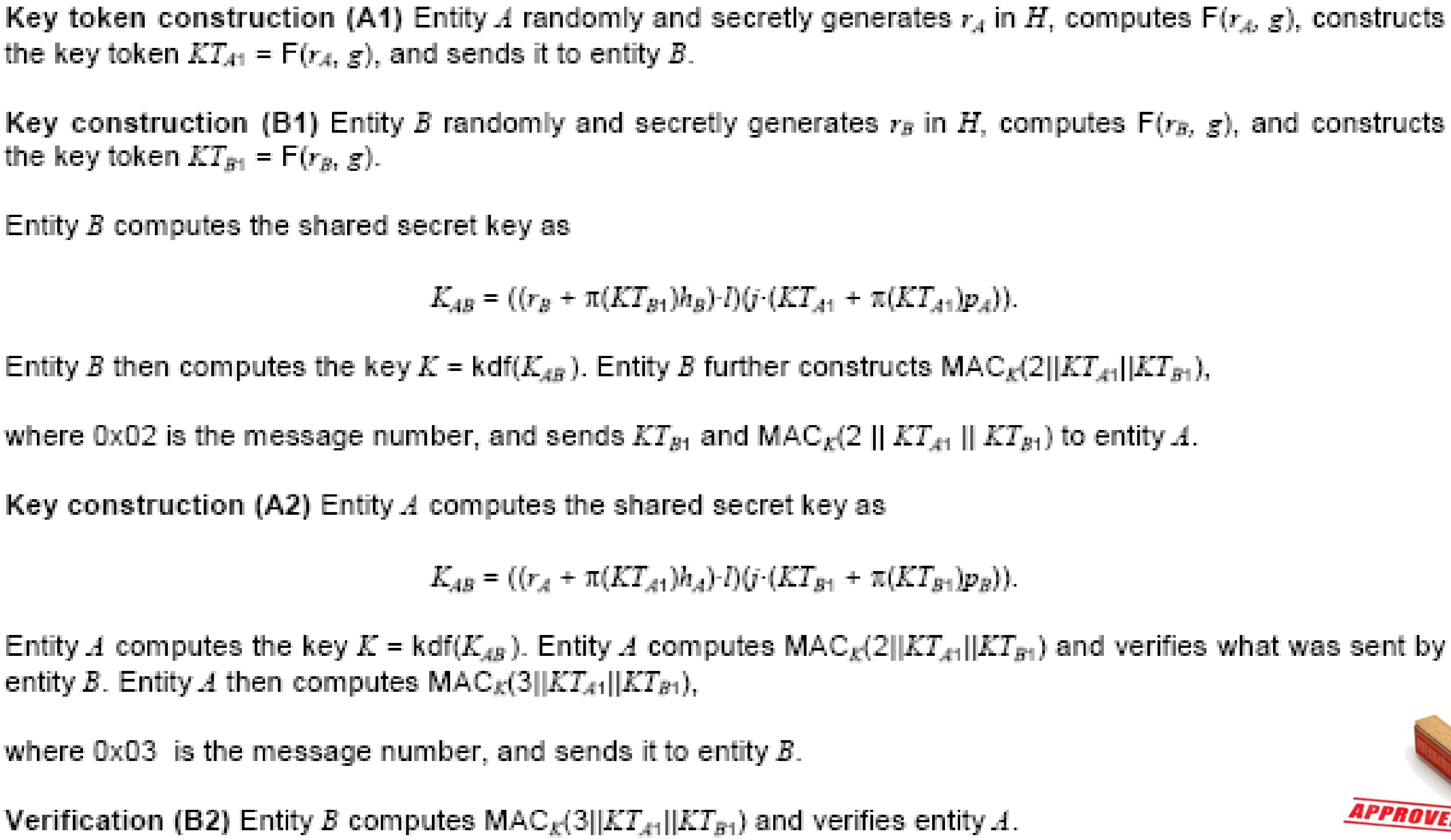
Cryptography and security mechanisms

- Cryptographic techniques and mechanisms
  - confidentiality
  - entity authentication
  - non-repudation
  - key management
  - data integrity such as
    - message authentication
    - hash-functions
    - digital signatures
- The most prolific working-group
  - 81 published standards (54% of all SC27)
  - 30 standards under development (40% of all SC27)

WG2

Cryptography and security mechanisms

- *Very* technical working-group
  - Example of Standard 11770-3 : *Key management — Part 3: Mechanisms using asymmetric techniques*



Key token construction (A1) Entity A randomly and secretly generates r_A in H, computes $\mathrm{F}(r_A, g)$, constructs the key token $KT_{A1} = \mathrm{F}(r_A, g)$, and sends it to entity B.

Key construction (B1) Entity B randomly and secretly generates r_B in H, computes $\mathrm{F}(r_B, g)$, and constructs the key token $KT_{B1} = \mathrm{F}(r_B, g)$.

Entity B computes the shared secret key as

$$K_{AB} = ((r_B + \pi(KT_{B1})h_B)\cdot l)(j\cdot(KT_{A1} + \pi(KT_{A1})p_A)).$$

Entity B then computes the key $K = \mathrm{kdf}(K_{AB})$. Entity B further constructs $\mathrm{MAC}_K(2||KT_{A1}||KT_{B1})$,

where 0x02 is the message number, and sends KT_{B1} and $\mathrm{MAC}_K(2 \,||\, KT_{A1} \,||\, KT_{B1})$ to entity A.

Key construction (A2) Entity A computes the shared secret key as

$$K_{AB} = ((r_A + \pi(KT_{A1})h_A)\cdot l)(j\cdot(KT_{B1} + \pi(KT_{B1})p_B)).$$

Entity A computes the key $K = \mathrm{kdf}(K_{AB})$. Entity A computes $\mathrm{MAC}_K(2||KT_{A1}||KT_{B1})$ and verifies what was sent by entity B. Entity A then computes $\mathrm{MAC}_K(3||KT_{A1}||KT_{B1})$,

where 0x03 is the message number, and sends it to entity B.

Verification (B2) Entity B computes $\mathrm{MAC}_K(3||KT_{A1}||KT_{B1})$ and verifies entity A.

APPROVED

WG2

Cryptography and security mechanisms

- Message authentication codes (MACs) [9797]
- Hash-functions [10118]
- Key management [11770]
- Non-repudiation [13888]
- Cryptographic techniques based on elliptic curves [15946]
- Time-stamping services [18014]
- Random bit generation [18031]
- Prime number generation [18032]
- Encryption algorithms [18033]
- Time-stamping services [18014]
- Secret sharing [19592]
- Authenticated encryption [19772]
- Anonymous digital signatures [20008]
- Anonymous entity authentication [20009]
- Signcryption [29150]
- Lightweight cryptography [29192]
- …

ISO/IEC JTC1 SC27
IT Security Techniques

SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

WG3
Security Evaluation, Testing and Specification

- Security engineering and standards for IT security specification, evaluation, testing and certification of IT systems, components, and products

- Consider computer networks, distributed systems, associated application services, biometrics, …

WG3

Security Evaluation, Testing and Specification

- Evaluation criteria for IT security [15408] *a.k.a. Common Criteria*
  - Part 1: Introduction and general model
  - Part 2: Security functional components
  - Part 3: Security assurance components
- A framework for IT security assurance [15443]
- Guide for the production of Protection Profiles and Security Targets [15446]
- Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 [19608]
- Methodology for IT security evaluation [18045]
- Security evaluation of biometrics [19792]
- Refining software vulnerability analysis under 15408 and 18045 [20004]
- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) [21827]
- Test requirements for cryptographic modules [24759]
- Verification of cryptographic protocols [29128]
- Vulnerability Disclosure [29147]
- Physical security attacks, mitigation techniques and security requirements [30104]
- Vulnerability handling processes [30111]
- …

ISO/IEC JTC1 SC27
IT Security Techniques

SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

WG4
Security controls and services

- Standards and guidelines addressing services and applications supporting the implementation of control objectives and controls as defined in ISO/IEC 27001

- Different domains
  - System and system life cycle security
    - Acquisition, Development, Supply, Storage, Processing, Communication, …
  - Security incidents
    - Detection, Investigation, Management, Recovery

- Several series of standards… ;)
  - e.g. 6 series of standards represent total of 28 documents!

WG4
Security controls and services

together with

27033 Network Security

- Part 1: Overview and concepts (2009 / 2015)
- Part 2: Guidelines for the design and implementation of network security (2012)
- Part 3: Reference networking scenarios -- Threats, design techniques and control issues (2010)
- Part 4: Securing communications between networks using security gateways (2014)
- Part 5: Securing communications across networks using Virtual Private Network (VPNs) (2013)
- Part 6: Securing wireless IP network access (DIS)

WG4

Security controls and services

27034
Application security

Part 1: Overview and concepts

(2011- Technical Corrigenda in 2014)

Part 2: Organization normative framework

(2015)

Part 3: Application security management process

(CD)

Part 4: Application security validation

(CD)

Part 5: Protocols and application security controls data structure

(CD)

Part 6: Security guidance for specific applications

(DIS)

Part 7: Application security assurance prediction

(CD)

Part 5-1: Protocols and application security controls data structure -- XML schemas

(PDTS)

WG4
Security controls and services

together with

27035
Information security incident management

(2011)

Part 1: Principles of incident management

(DIS)

Part 2: Guidelines to plan and prepare for incident response

(DIS)

Part 3: Guidelines for CSIRT operations

(PDTS)

WG4
Security controls and services

telindus
together with
proximus tango

27036
Information security for supplier relationships

FREE

Part 1: Overview and concepts

(2014)

Part 2: Requirements

(2014)

Part 3: Guidelines for information and communication technology supply chain security

(2013)

Part 4: Guidelines for security of Cloud services

(CD)

WG4
Security controls and services

together with

27050
Electronic discovery
(under development)

Part 1: Overview and concepts

(1st CD)

Part 2: Guidance for governance and management of electronic discovery

(2nd WD)

Part 3: Code of Practice for electronic discovery

(2nd WD)

Part 4: ICT readiness for electronic discovery

(2nd WD)

WG4
Security controls and services

14516
Guidelines for the use and management of Trust Service Providers

(revision of ISO/IEC TR 14516:2002)

Part 1: Overview and concepts

(1st WD)

Part 2: Guidelines on information security of PKI Trust Service Providers

(1st WD)

Part 3: Guidelines on provision of services by PKI Trust Service Providers

(1st WD)

WG4
Security controls and services

- Series of standards on Guidelines for the use and management of Trust Service Providers [14516]
  - (revision of ISO/IEC TR 14516:2002)
- Security information objects for access control [15816]
  - 2002
- Specification of TTP services to support the application of digital signatures [15945]
  - 2002
- Selection, deployment and operations of intrusion detection systems [18043]
  - 2006
  - Currently under revision as ISO/IEC 27039
- Guidelines for ICT readiness for business continuity [27031]
  - 2011
- Guidelines for cybersecurity [27032]
  - 2012
- Series of standards on Network Security [27033]
- Series of standards on Application Security [27034]
- Series of standards on Information Security Incident Management [27035]
- Series of standards on Information security for supplier relationships [27036]
- Series of standards on Electronic Discovery [27050]
- Guidelines for the identification, collection, acquisition and preservation of digital evidence [27037]
  - 2012
- Specification for digital redaction [27038]
  - 2014
- Selection, deployment and operation of intrusion detection and prevention systems (IDPS) [27039]
  - 2015
- Storage security [27040]
  - 2015
- Guidance on assuring suitability and adequacy of incident investigative methods [27041]
  - 2015
- Guidelines for the analysis and interpretation of digital evidence [27042]
  - 2015
- Incident investigation principles and processes [27043]
  - 2015
- Best practice on the provision and use of time-stamping services [29149]
  - 2012

WG4

Security controls and services

- 27044
  - Guidelines for security information and event management (SIEM)
  - 4th WD

ISO/IEC JTC1 SC27

IT Security Techniques

SC27

SWG-M	WG1	WG2	WG3	WG4	WG5	SWG-T
Special Working Group on Management	Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies	Transversal Items

WG5
Identity management and privacy technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - Identity management
  - Biometrics
  - Privacy / protection of personal data
- Collaboration with each other Working Groups in SC 27

WG5
Identity management and privacy technologies

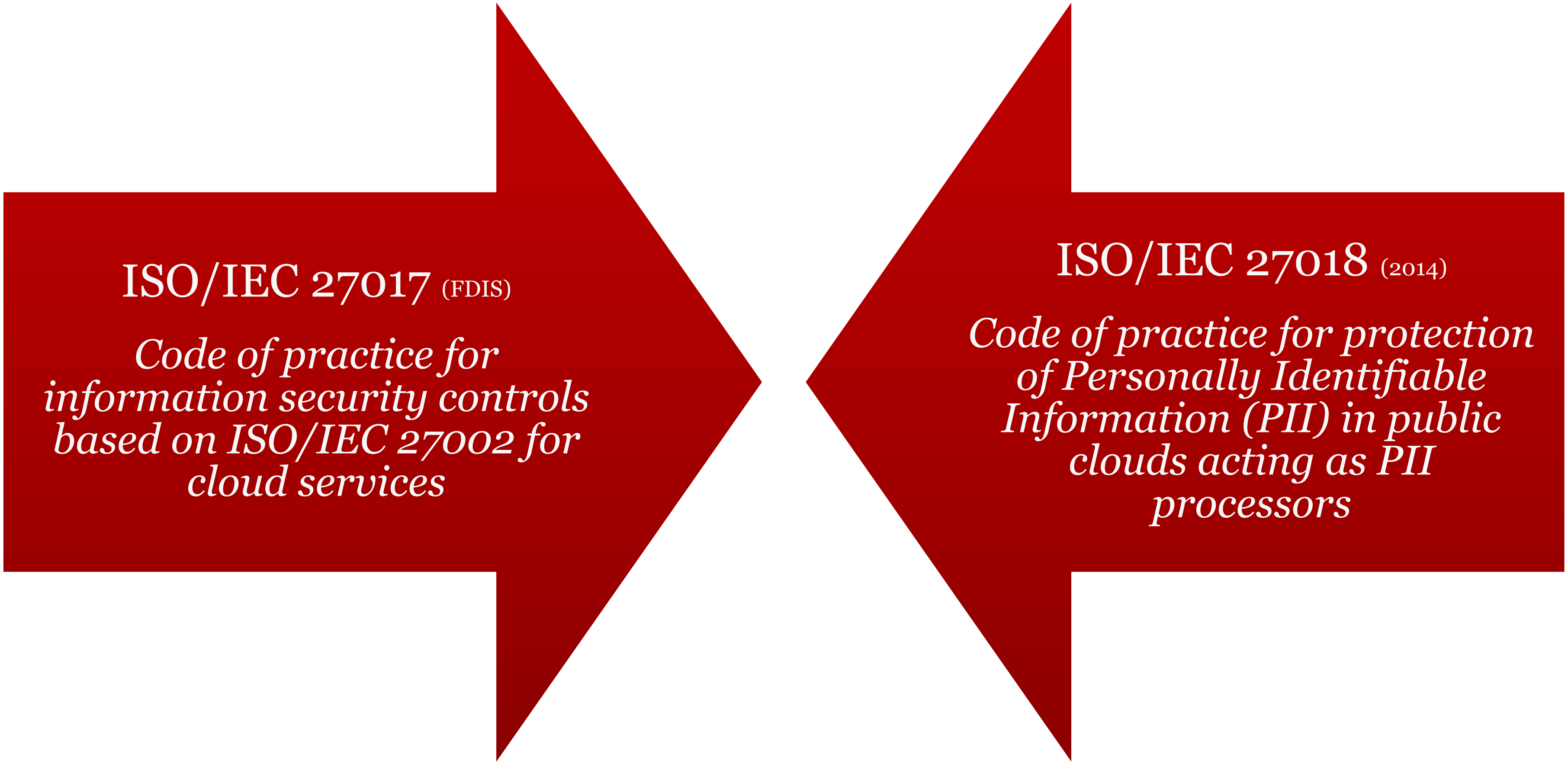
- Authentication context for biometrics [24761]
  - 2009
  - Cor.1 2013
- Biometric information protection [24745]
  - 2011
- A framework for identity management [24760]
  - FREE Part 1: Terminology and concepts
    - 2011
  - Part 2: Reference architecture and requirements
    - 2015
- FREE Privacy framework [29100]
  - 2011
- Entity authentication assurance framework [29115]
  - 2013
- Privacy capability assessment model [29190]
  - 2015
- Requirements for partially anonymous, partially unlinkable authentication [29191]
  - 2012
- Code of practice for PII protection in public clouds acting as PII processors [27018]
  - 2014
- FREE Privacy references list [SD2]
- Standards privacy assessment [SD4]

Focus on Cloud Computing

About Security & Privacy

Focus on Cloud Computing

About Security & Privacy



ISO/IEC 27017 (FDIS)

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018 (2014)

Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

Focus on Cloud Computing

About Security & Privacy

ISO/IEC 27017 (FDIS)

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

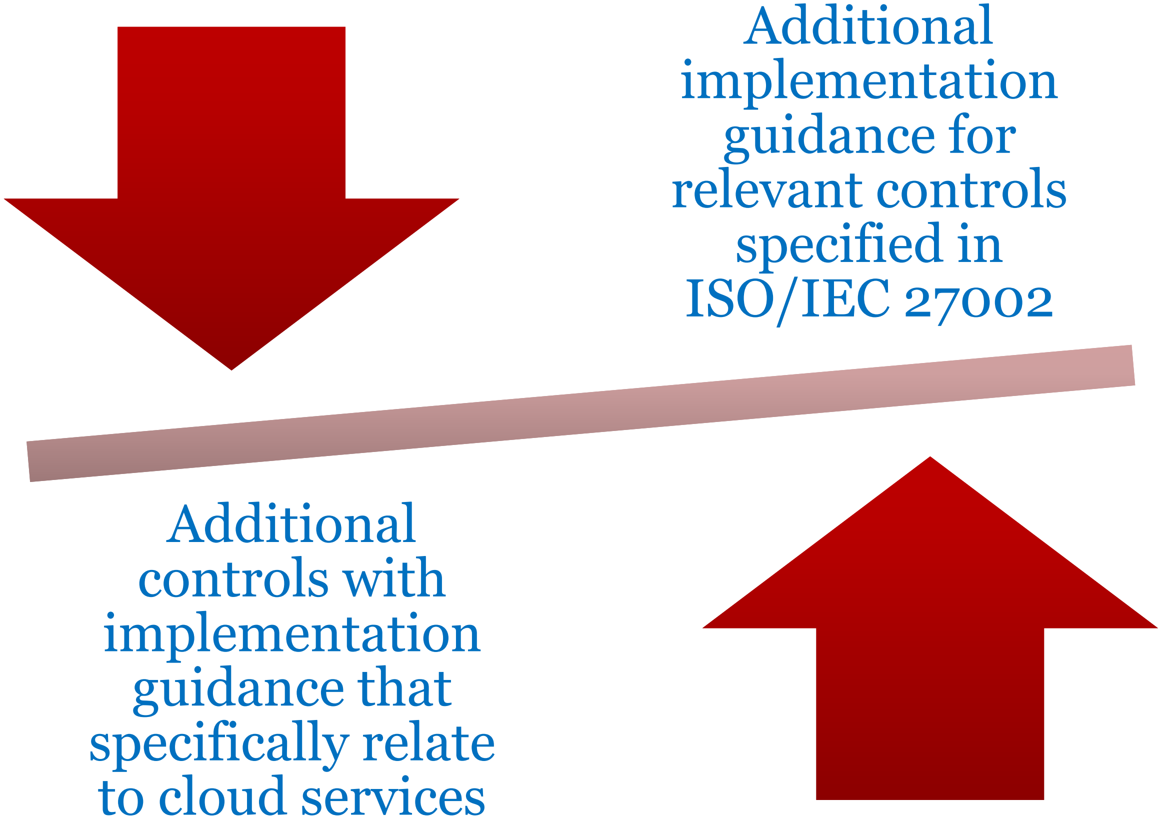
ISO/IEC 27018 (2014)

Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

ISO/IEC 27017 (FDIS)

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- Guidelines for information security controls applicable to the provision and use of cloud services



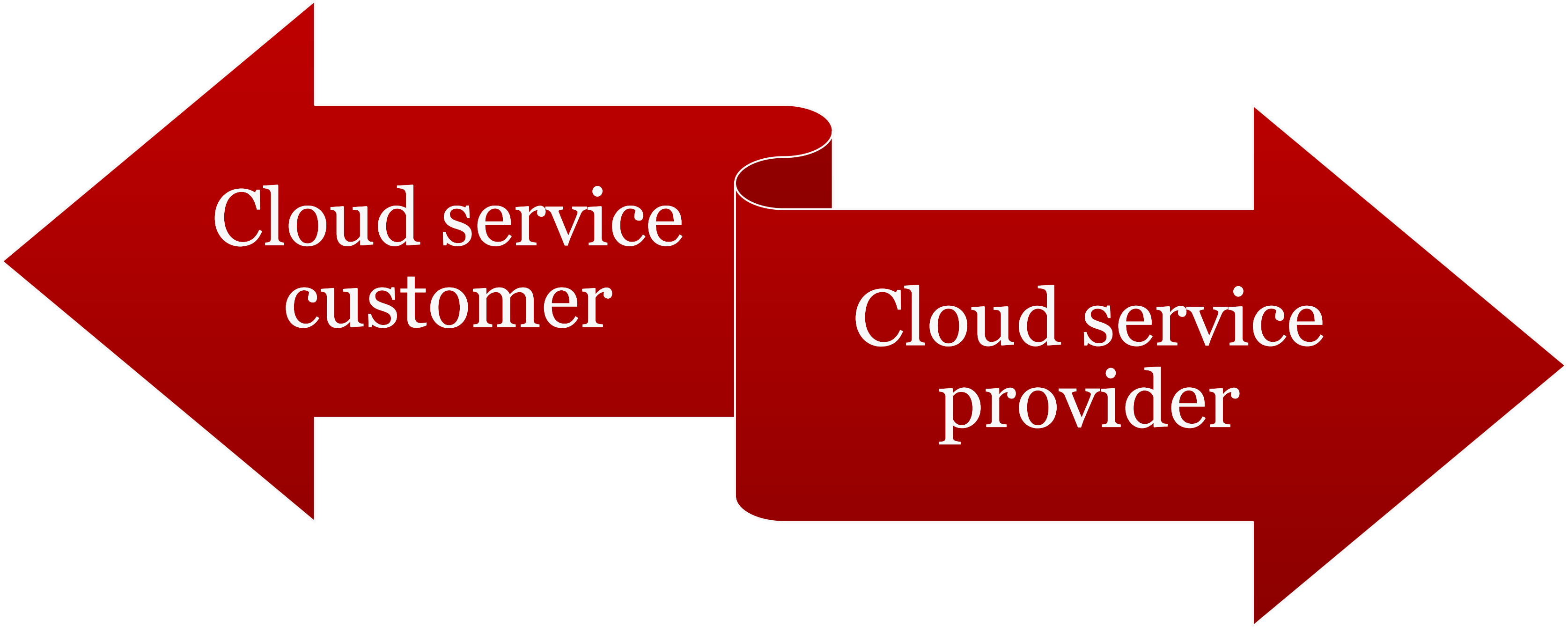
Additional implementation guidance for relevant controls specified in ISO/IEC 27002

Additional controls with implementation guidance that specifically relate to cloud services

ISO/IEC 27017 (FDIS)

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- Provides controls and implementation guidance for both cloud service providers and cloud service customers



Cloud service customer

Cloud service provider

ISO/IEC 27017 (FDIS)

Table of contents

- Enhancement of ISO/IEC 27002 clauses

  39 enhanced controls

  5. Information security policies (1)
  6. Organization of information security (2)
  7. Human resource security (1)
  8. Asset management (2)
  9. Access control (7)
  10. Cryptography (2)
  11. Physical and environmental security (1)
  12. Operations security (8)
  13. Communications security (1)
  14. System acquisition, development and maintenance (2)
  15. Supplier relationships (3)
  16. Information security incident management (2)
  17. Information security aspects of business continuity management (2)
  18. Compliance (5)

- New clauses

  - Annex A Cloud Service Extended Control Set (normative)

    7 additional controls distributed over 6 additional clauses

    - CLD.6.3 Relationship between cloud service customer and cloud service provider
    - CLD.8.1 Responsibility for assets
    - CLD.9.5 Access control of cloud service customer's data in shared virtual environment
    - CLD.12.1 Operational procedures and responsibilities
    - CLD.12.4 Logging and monitoring
    - CLD.13.1 Network security management

  - Annex B References on information security risk related to cloud computing (informative)

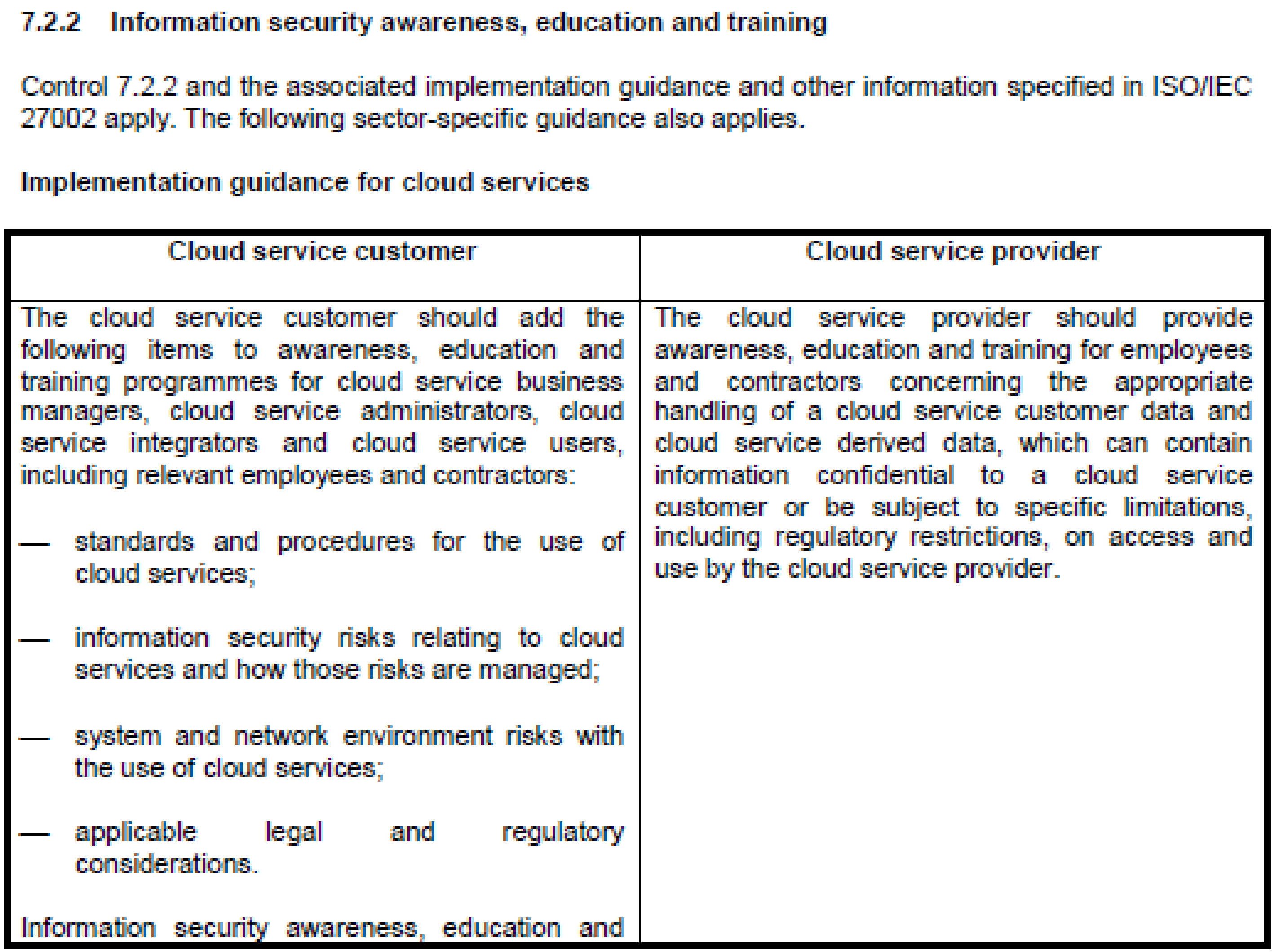
ISO/IEC 27017 (FDIS)

Focus on the Enhancement of ISO/IEC 27002 clauses

telindus

together with

proximus tango



7.2.2 Information security awareness, education and training

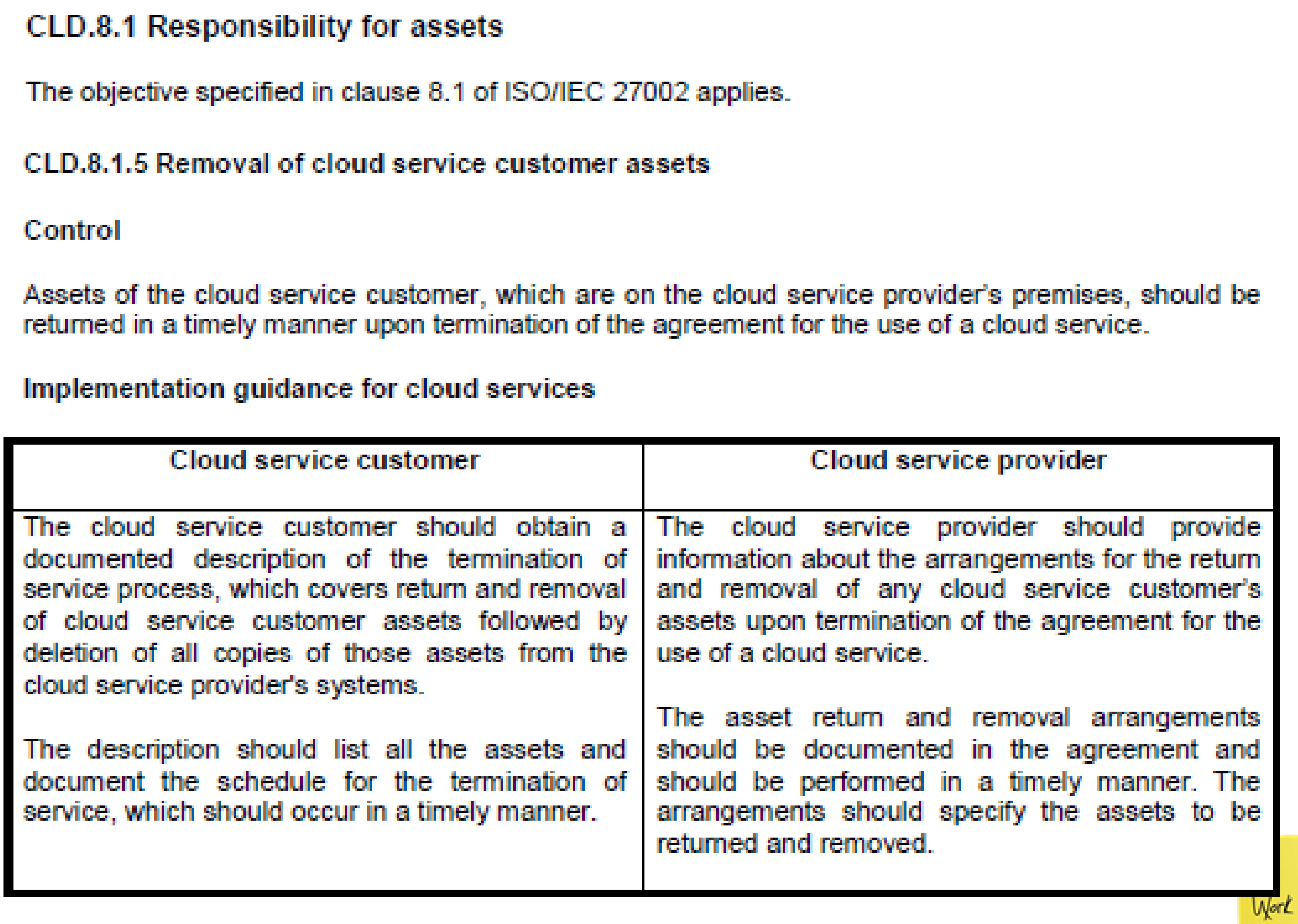
Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors: — standards and procedures for the use of cloud services; — information security risks relating to cloud services and how those risks are managed; — system and network environment risks with the use of cloud services; — applicable legal and regulatory considerations. Information security awareness, education and	The cloud service provider should provide awareness, education and training for employees and contractors concerning the appropriate handling of a cloud service customer data and cloud service derived data, which can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.

ISO/IEC 27017 (FDIS)

Focus on the "Cloud Service Extended Control Set"



CLD.8.1 Responsibility for assets

The objective specified in clause 8.1 of ISO/IEC 27002 applies.

CLD.8.1.5 Removal of cloud service customer assets

Control

Assets of the cloud service customer, which are on the cloud service provider's premises, should be returned in a timely manner upon termination of the agreement for the use of a cloud service.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should obtain a documented description of the termination of service process, which covers return and removal of cloud service customer assets followed by deletion of all copies of those assets from the cloud service provider's systems. The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.	The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service. The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.

Focus on Cloud Computing

About Security & Privacy

ISO/IEC 27017 (FDIS)

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018 (2014)

Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

ISO/IEC 27018 (2014)

Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

- Based on ISO/IEC 27002

- For implementing measures to protect Personally Identifiable Information (PII)
  - in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment

ISO/IEC 27018 (2014)
Table of contents

- Enhancement of ISO/IEC 27002 clauses

  15 enhanced controls

  5. Information security policies (1)
  6. Organization of information security (1)
  7. Human resource security (1)
  8. Asset management (0)
  9. Access control (3)
  10. Cryptography (0)
  11. Physical and environmental security (1)
  12. Operations security (4)
  13. Communications security (1)
  14. System acquisition, development and maintenance (0)
  15. Supplier relationships (0)
  16. Information security incident management (2)
  17. Information security aspects of business continuity management (0)
  18. Compliance (1)

- New clauses

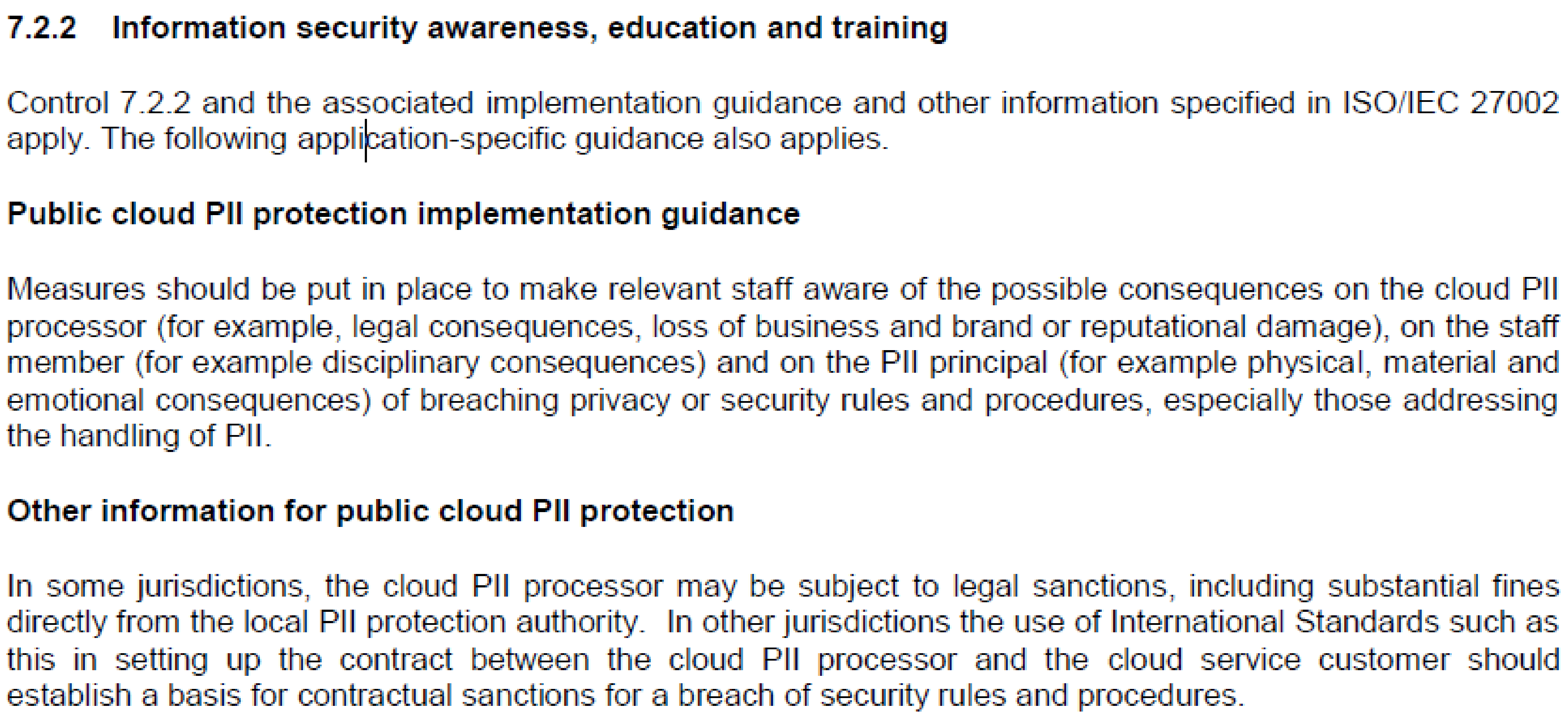
  - Annex A Public cloud PII processor extended control set for PII protection (normative)

    22 additional controls distributed over 11 privacy principles coming from ISO/IEC 29100

    1. Consent and choice
    2. Purpose legitimacy and specification
    3. Collection limitation
    4. Data minimization
    5. Use, retention and disclosure limitation
    6. Accuracy and quality
    7. Openness, transparency and notice
    8. Individual participation and access
    9. Accountability
    10. Information security
    11. Privacy compliance

ISO/IEC 27018 (2014)

Focus on the Enhancement of ISO/IEC 27002 clauses



7.2.2 Information security awareness, education and training

Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following application-specific guidance also applies.

Public cloud PII protection implementation guidance

Measures should be put in place to make relevant staff aware of the possible consequences on the cloud PII processor (for example, legal consequences, loss of business and brand or reputational damage), on the staff member (for example disciplinary consequences) and on the PII principal (for example physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

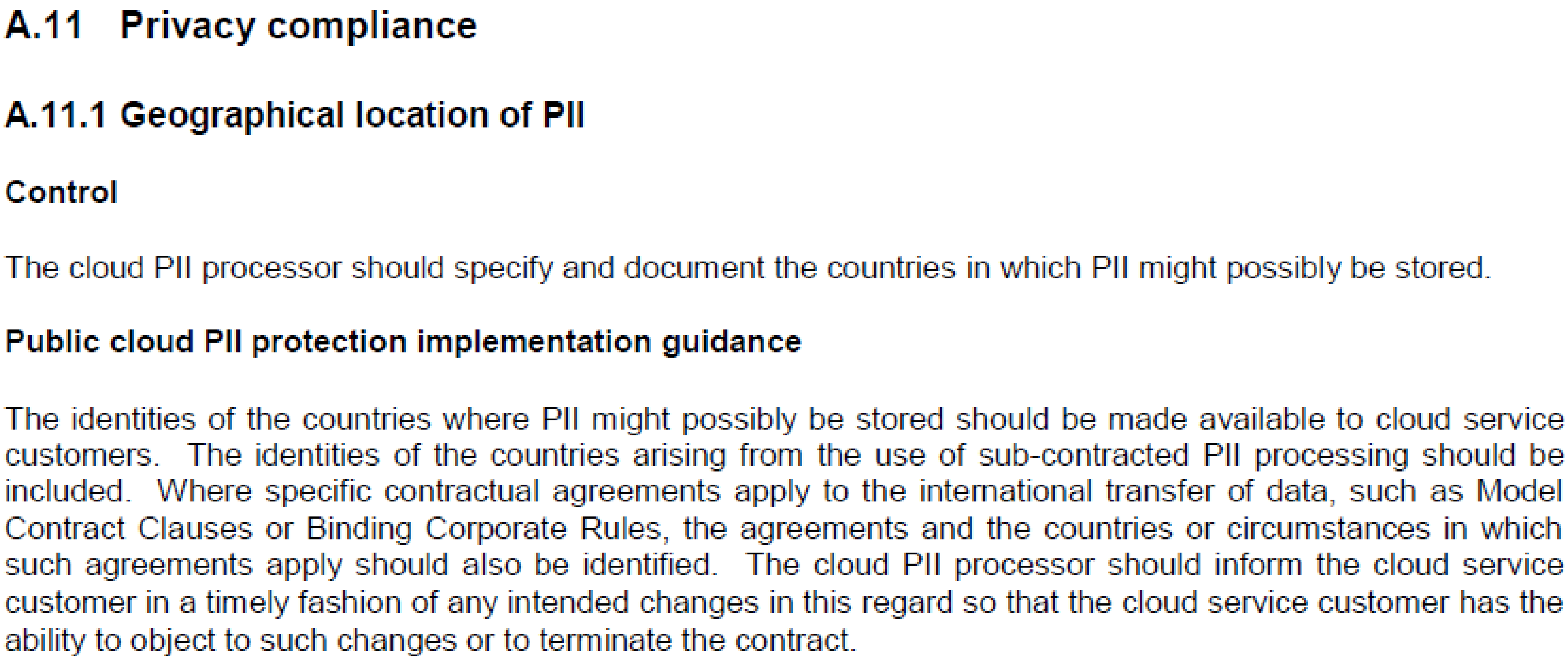
Other information for public cloud PII protection

In some jurisdictions, the cloud PII processor may be subject to legal sanctions, including substantial fines directly from the local PII protection authority. In other jurisdictions the use of International Standards such as this in setting up the contract between the cloud PII processor and the cloud service customer should establish a basis for contractual sanctions for a breach of security rules and procedures.

APPROVED

ISO/IEC 27018 (2014)

Focus on "public cloud PII processor extended control set for PII protection"



A.11 Privacy compliance

A.11.1 Geographical location of PII

Control

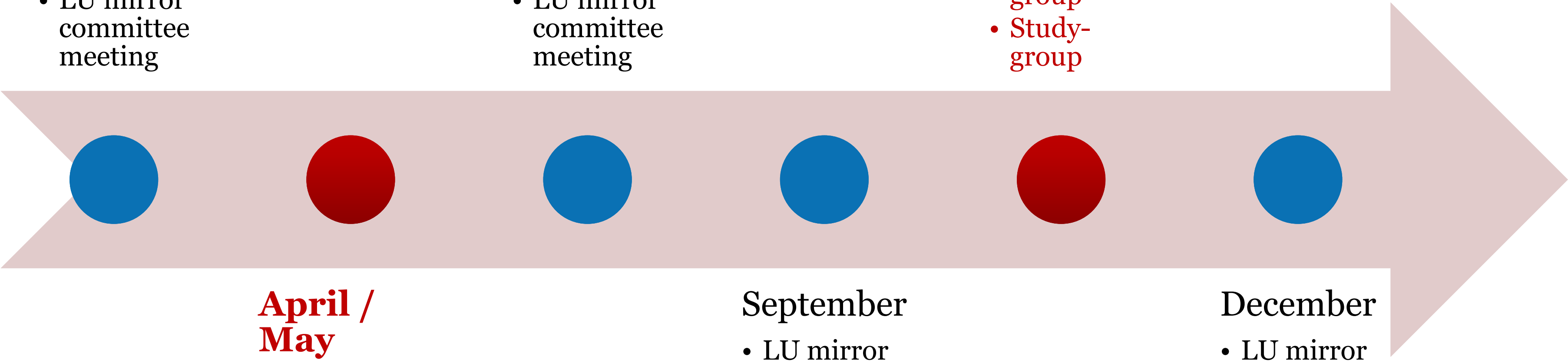
The cloud PII processor should specify and document the countries in which PII might possibly be stored.

Public cloud PII protection implementation guidance

The identities of the countries where PII might possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses or Binding Corporate Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

How to take part into the standardization work?

2 international meetings per year
3+ LU mirror committee meetings



March

- LU mirror committee meeting

April / May

- International meetings
  - Plenary
  - Working-group
  - Study-group

June

- LU mirror committee meeting

September

- LU mirror committee meeting

October / November

- International meetings
  - Working-group
  - Study-group

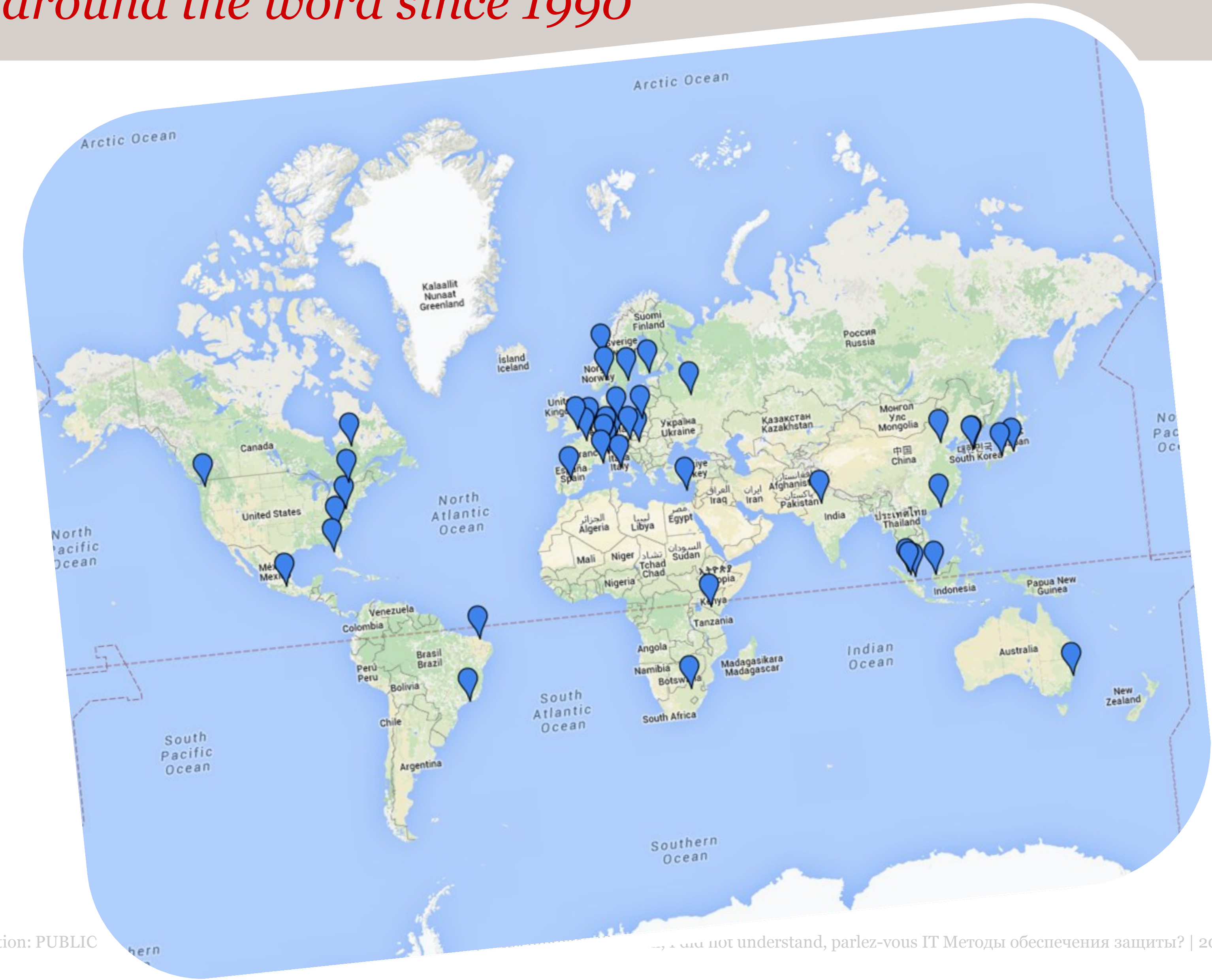
December

- LU mirror committee meeting

2 international meetings per year

All around the word since 1990

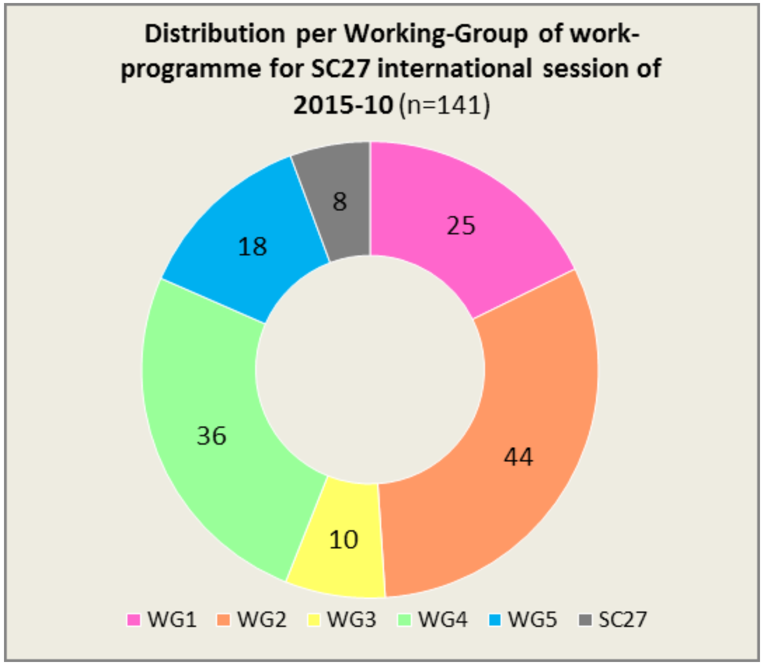
together with

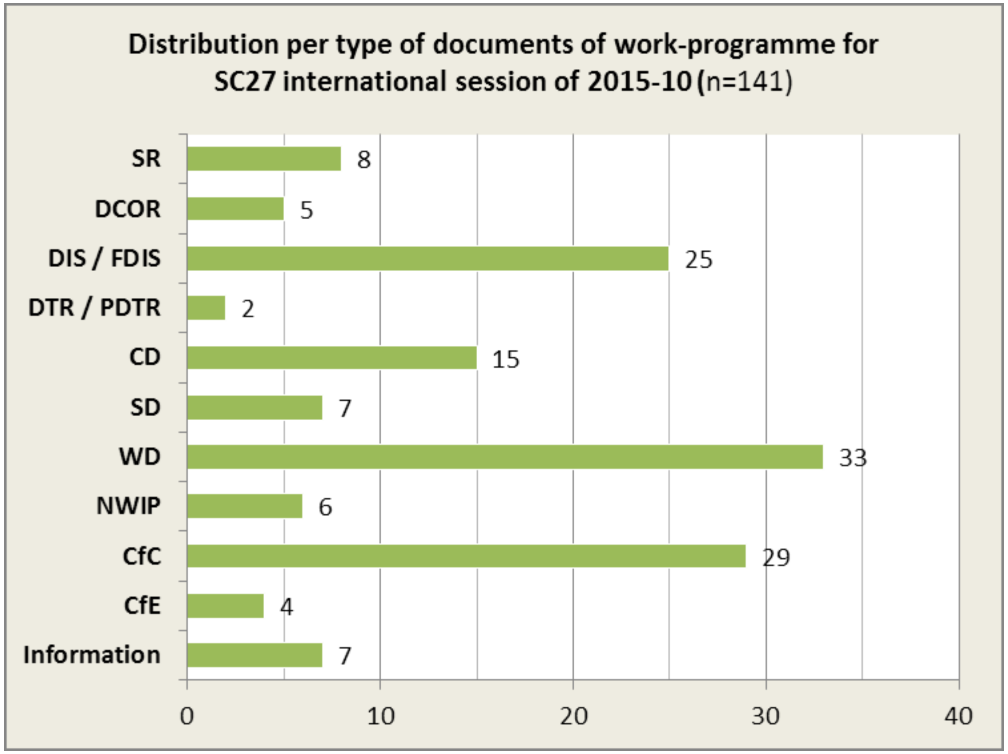


Next meeting will take place in जयपुर (Jaipur, India)

2015, October 26th > 30th

telindus
together with proximus tango





WG1 → ISMS
WG2 → Cryptography
WG3 → Security evaluation
WG4 → Controls and services
WG5 → Privacy technologies

How to participate at LU-level / international-level?
Ask our today's host!

How to participate at LU-level / international-level?
Ask our today's host!

SC27 IT Security Techniques *in 1 slide*

ISO/IEC JTC1/SC27

TITLE	IT Security techniques	**DATE OF CREATION**	1990
SECRETARIAT	Deutsches Institut für Normung (DIN)	**P-MEMBERS** **O-MEMBERS**	51 20
SECRETARY	**Mrs Krystyna Passia**	**PUBLISHED STANDARDS**	150
CHAIRPERSON	**Mr Walter Fumy (Germany)** **(2013-11 → 2016-11)**	**STANDARDS UNDER DEVELOPMENT**	75

SCOPE

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:

✓ Management of information and ICT security / ISMS

✓ Cryptographic and other security mechanisms

✓ Security aspects of identity management, biometrics and privacy

✓ Conformance assessment, accreditation and auditing requirements in the area of information security and security evaluation criteria and methodology

MAIN STANDARDS

ISO/IEC 27001:2013 - Information security management systems – Requirements
ISO/IEC 27002:2013 - Code of practice for information security controls
ISO/IEC 29192 series - Lightweight cryptography
ISO/IEC 15408 series - Evaluation criteria for IT security (a.k.a the "Common Criteria")

NATIONAL STUDY COMMITEE

MEMBERSHIP	P-Member
DATE OF CREATION	August 2002
NATIONAL EXPERTS	26

NATIONAL VICE-CHAIRPERSON

Cédric MAUNY

Telindus Luxembourg

Head of Technical Unit
Security Audits and Governance Services (SAGS)
Risk Manager

Want to take a look on some ISO/IEC JTC1 SC27 documents and standards ?

- Usually ISO Standards are not FREE but…

  - http://www.din.de/en/meta/jtc1sc27/downloads
    - SD6 *Glossary of IT Security terminology*
    - SD7 *Catalogue of SC 27 Projects and Standards*
    - SD11 *Overview of SC 27 Work*
    - SD12 *Assessment of cryptographic algorithms and key lengths*
    - WG5 SD2 *Part 1: Privacy References List*
    - WG 5 SD4 *Standard Privacy Assessment (SPA)*

  - http://standards.iso.org/ittf/PubliclyAvailableStandards/
    - ISO/IEC 27000 about *ISMS Overview and Vocabulary*
      - EN + FR + RU
    - ISO/IEC 27036-1 about *Information security for supplier relationships, Part 1: Overview and concepts*
    - ISO/IEC 24760-1 about *A framework for identity management, Part 1: Terminology and concepts*
    - ISO/IEC 29100 about *Privacy framework*

    + Many others (600+) in various domains

    - *Please read the ISO Copyright for the freely available standards*

One more thing...

SC 27 has received the Lawrence D. Eicher Leadership Award 2015 for its standardization work

- LDE awards is going to the ISO technical committees (TC) or subcommittees (SC) who have shown great leadership, use innovative approaches and promote the involvement of developing countries

Thank you for your attention

together with

Questions & Answers

telindus

together with

proximus tango

Contact information

Cédric MAUNY

cedric.mauny@telindus.lu

(+352) 621.200.707

telindus

together with

proximus tango