Sécurité de l'information dans les TICs
Travaux normatifs en cours

ILNAS / ANEC
Etat des lieux normatif national des TIC - Focus sur la sécurité de l'information
23 novembre 2012

Cédric Mauny
Technology Leader, CISM, CISSP, ISO27001, ITIL
Chairman SC27 LU

SAGS - Security Audit and Governance Services, a Telindus Security department

Etat des lieux normatif national des TIC
Focus sur la sécurité de l'information

- La gestion de l'information est un enjeu stratégique pour toute entreprise
  - Permet d'assurer la pérennité des entreprises dans un environnement de plus en plus dématérialisé

- La maîtrise des risques en sécurité de l'information peut être supporté par des normes et codes de bonnes pratiques
  - Conçues et développées par des experts répartis à travers le monde par consensus
  - Approuvées par des organismes de normalisation indépendants
  - Documents de références dans le secteur des Technologies de l'Information et de la Communication

- ISO a mis en œuvre un comité dédié aux techniques de sécurité des technologies de l'information
  - Créer des normes pour faciliter et accompagner les entreprises dans la gestion de la sécurité de leur patrimoine informationnel

Agenda

De ISO
À ISO/IEC JTC1 SC27 *IT Security Techniques*

Des travaux normatifs pour la sécurité de l'information

Le SC27 en une planche

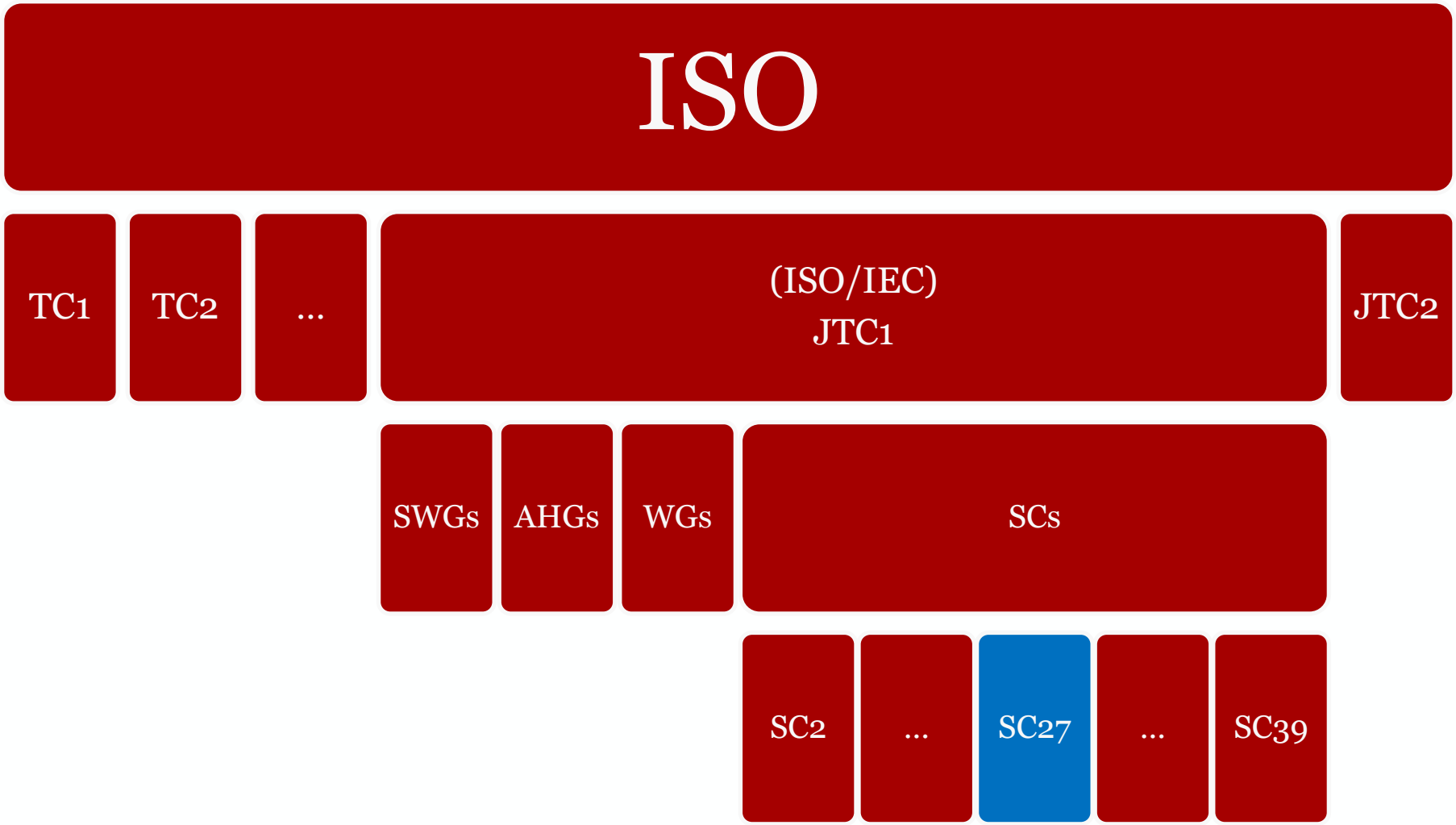
La sécurité de l'information selon l'ISO

De ISO à ISO/IEC JTC1 SC27

La sécurité de l'information au sein de l'ISO
De ISO à ISO/IEC JTC1 SC27

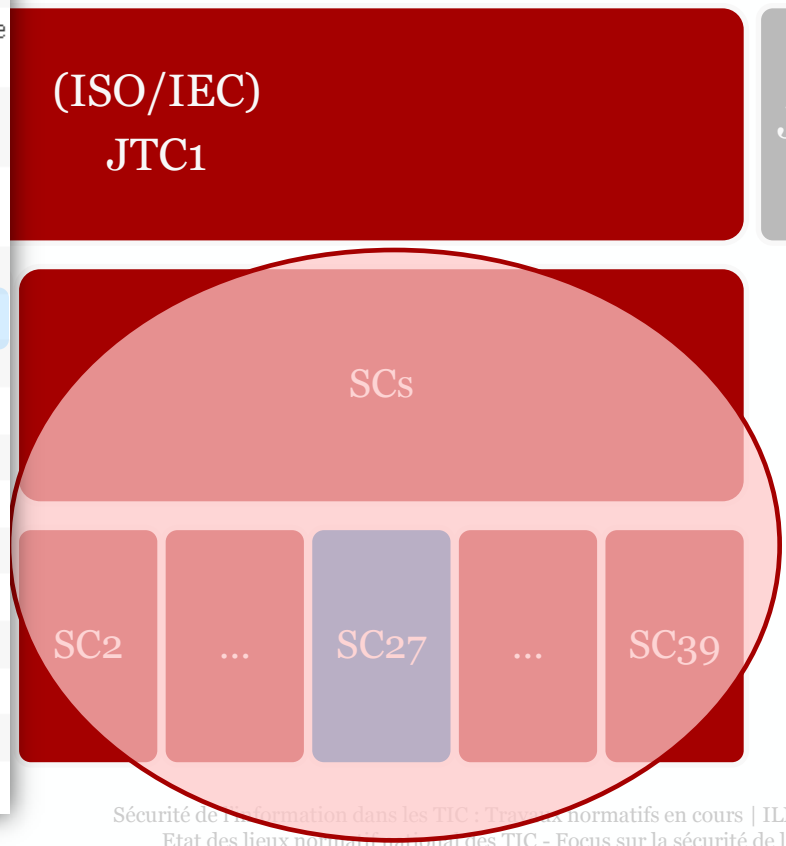
- ISO/IEC
  - ISO : International Standardisation Organisation
  - IEC : International Electrotechnical Commission
- JTC1
  - Joint Technical Committee #1
    - *Information Technology*
- SC27
  - Subcommittee #27
    - *IT Security Techniques*
  - 22 ans

La sécurité de l'information au sein de l'ISO
De ISO à ISO/IEC JTC1 SC27



La sécurité de l'information au sein de l'ISO
De ISO à ISO/IEC JTC1 SC27

JTC 1/SC 2	Coded character sets
JTC 1/SC 6	Telecommunications and information exchange between systems
JTC 1/SC 7	Software and systems engineering
JTC 1/SC 17	Cards and personal identification
JTC 1/SC 22	Programming languages, their environments and system software interfaces
JTC 1/SC 23	Digitally Recorded Media for Information Interchange and Storage
JTC 1/SC 24	Computer graphics, image processing and environmental data representation
JTC 1/SC 25	Interconnection of information technology equipment
JTC 1/SC 27	IT Security techniques
JTC 1/SC 28	Office equipment
JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information
JTC 1/SC 31	Automatic identification and data capture techniques
JTC 1/SC 32	Data management and interchange
JTC 1/SC 34	Document description and processing languages
JTC 1/SC 35	User interfaces
JTC 1/SC 36	Information technology for learning, education and training
JTC 1/SC 37	Biometrics
JTC 1/SC 38	Distributed application platforms and services (DAPS)
JTC 1/SC 39	Sustainability for and by Information Technology



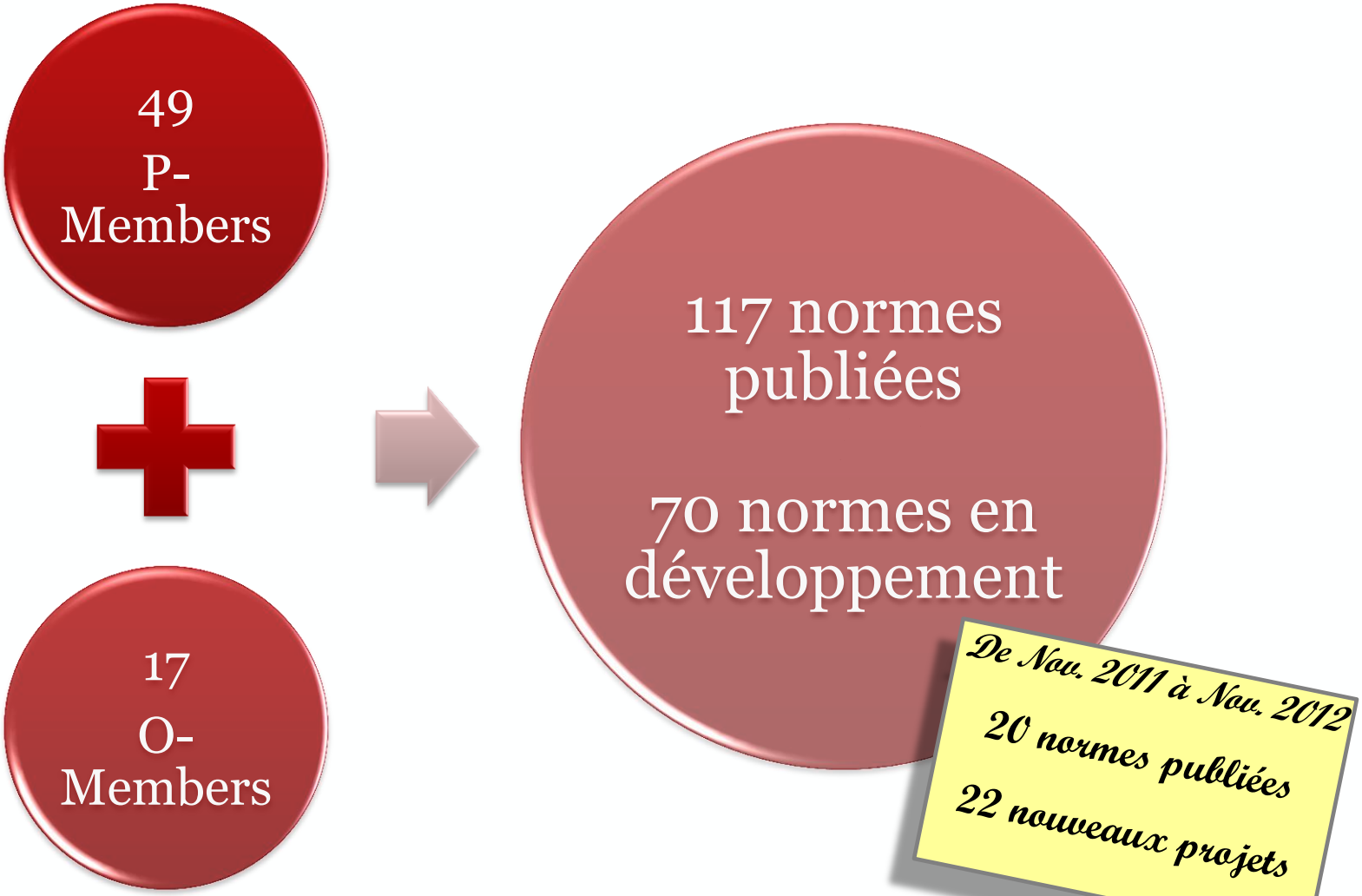
ISO/IEC JTC1 SC27
IT Security Techniques

- Reconnu comme pôle d'information et d'expertise en normalisation de la sécurité IT / information

- Sert les besoins des secteurs privés et publics

- Couvre le développement de normes pour la protection de l'information et des TICs
  - Méthodes génériques, techniques et lignes directrices
  - Considère les aspects *security* et *privacy*

La sécurité de l'information au sein de l'ISO
ISO/IEC JTC1 SC27 – IT Security Techniques



ISO/IEC JTC1 SC27
IT Security Techniques

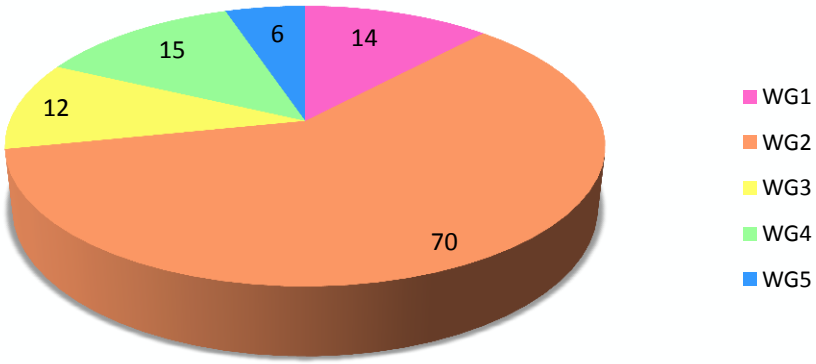
telindus belgacom ICT
together with belgacom tango

SC27

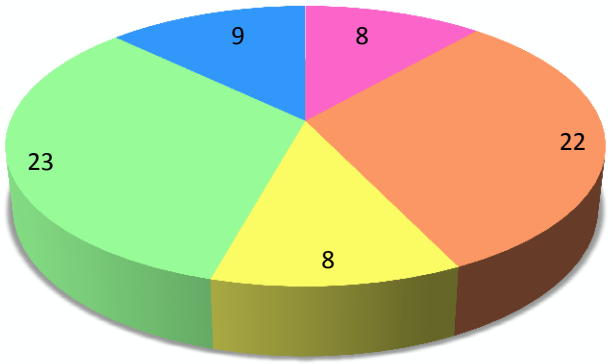
WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

ISO/IEC JTC1 SC27
IT Security Techniques

117 normes publiées



70 normes en développement



ISO/IEC JTC1 SC27
IT Security Techniques

- 2 sessions annuelles
  - Avril / Mai
    - Session plénière
  - Octobre / Novembre

- 5 jours / session
  + 2 jours pour la plénière

- Sessions à travers le monde
  - 2012
    - Mai : Stockholm (SU)
    - Octobre : Rome (IT)
  - 2013
    - Avril : Sophia Antipolis (FR)
    - Octobre : Songdo (KO)
  - 2014
    - Avril : Hong Kong (CN)
    - Octobre : *tba*

ISO/IEC JTC1 SC27
IT Security Techniques

- Les documents normatifs sont habituellement payants…
  - 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
  - WG5 SD2 *Part 1: Privacy References List*
    - http://www.jtc1sc27.din.de/sbe/wg5SD2-1
  - ISO/IEC 27000:2009 *ISMS Overview and Vocabulary*
    - http://standards.iso.org/ittf/PubliclyAvailableStandards/

Des travaux normatifs pour la sécurité de l'information

Information security management systems

ISO/IEC JTC1 SC27
IT Security Techniques

telindus belgacom ICT
together with belgacom tango

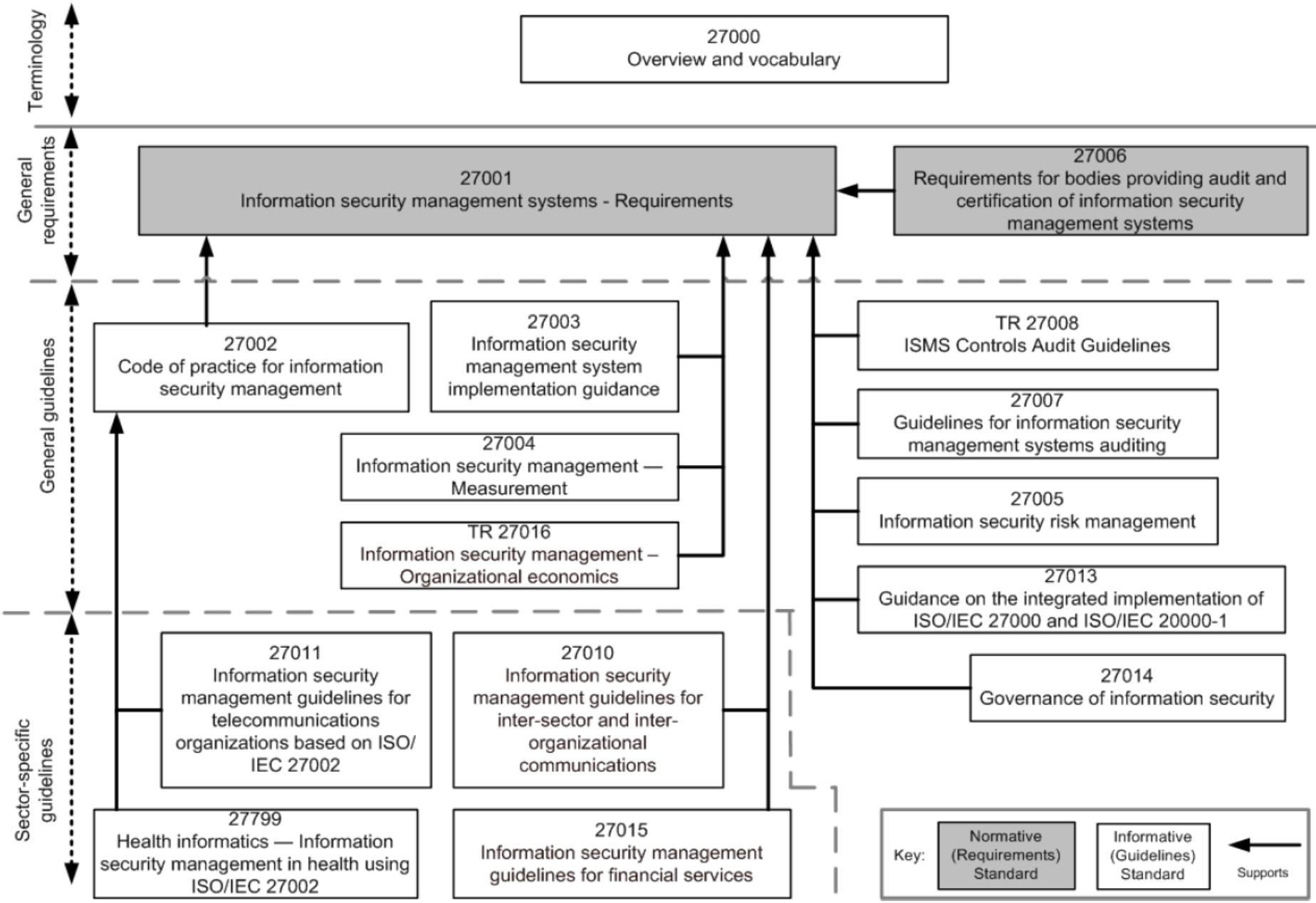
SC27

WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

Information Security Management Systems are everywhere!

WG1 : Information security management systems

- Couvrir tous les aspects de normalisation en lien avec les systèmes de management de la sécurité de l'information (SMSI)
  - *Requirements*
  - *Methods and processes*
  - *Security controls*
  - *Sector and application specific use of ISMS*
  - *Accreditation, certification, auditing of ISMS*
  - *Governance*
  - *Information security economics*


Terminology
27000
Overview and vocabulary
General requirements
27001
Information security management systems - Requirements
27006
Requirements for bodies providing audit and certification of information security management systems
General guidelines
27002
Code of practice for information security management
27003
Information security management system implementation guidance
27004
Information security management — Measurement
TR 27016
Information security management – Organizational economics
TR 27008
ISMS Controls Audit Guidelines
27007
Guidelines for information security management systems auditing
27005
Information security risk management
27013
Guidance on the integrated implementation of ISO/IEC 27000 and ISO/IEC 20000-1
27014
Governance of information security
Sector-specific guidelines
27011
Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
27010
Information security management guidelines for inter-sector and inter-organizational communications
27799
Health informatics — Information security management in health using ISO/IEC 27002
27015
Information security management guidelines for financial services
Key:
Normative (Requirements) Standard
Informative (Guidelines) Standard
Supports

WG1 : Information security management systems

Current version	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Under revision?	✓	✓	✓	✓	✓		✓													
IS / TR	■	■	■	■	■	■	■	■	■		■	■		■		■				
FDIS / DTR	■																			
DIS / PDTR	■	■	■																	■
CD	■	■	■																	■
WD	■	■	■				■													
PD	■	■	■		■		■													
NWIP	■	■	■		■		■													
SP	■	■	■		■		■													
	27000	27001	27002	27003	27004	27005	27006	27007	27008	27009	27010	27011	27012	27013	27014	27015	27016	27017	27018	27019

Statut en sortie de la réunion SC27 de Rome (2012-10)

WG1 : Information security management systems
Projets publiés

- ISMS
  - 2005
    - Requirements [27001]
    - Code of practice for information security management [27002]
  - 2009
    - Overview and vocabulary [27000]
    - Measurement [27004]
  - 2010
    - ISMS implementation guidance [27003]
  - 2011
    - Information security risk management [27005]
    - Requirements for bodies providing audit and certification of information security management systems [27006]
    - Guidelines for information security management systems auditing [27007]
    - Guidelines for auditors on information security controls [27008]

- Secteur spécifique
  - 2008
    - Information security management guidelines for telecommunications organizations based on 27002 [27011]
  - 2012
    - Information security management for inter-sector and inter-organizational communications [27010]
    - Guidance on the integrated implementation of 27001 and 20000-1 [27013]

- Hors scope ISMS
  - 2002
    - Guidelines for the use and management of Trusted Third Party services [14516]
    - Security information objects for access control [15816]

WG1 : Information security management systems
Principaux projets en développement

- Résolution de publication
  - Overview and Vocabulary (2ème édition) [27000]
  - Information security management guidelines for financial services (1ère édition) [TR 27015]

- Promotion en DIS
  - Requirements [27001]
  - Code of practice for information security controls [27002]

- Promotion en DTR / PTDR
  - Organizational economics [27016]
  - Smart Grid / Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry [27019]

WG1 : Information security management systems
Principaux projets en développement (suite)

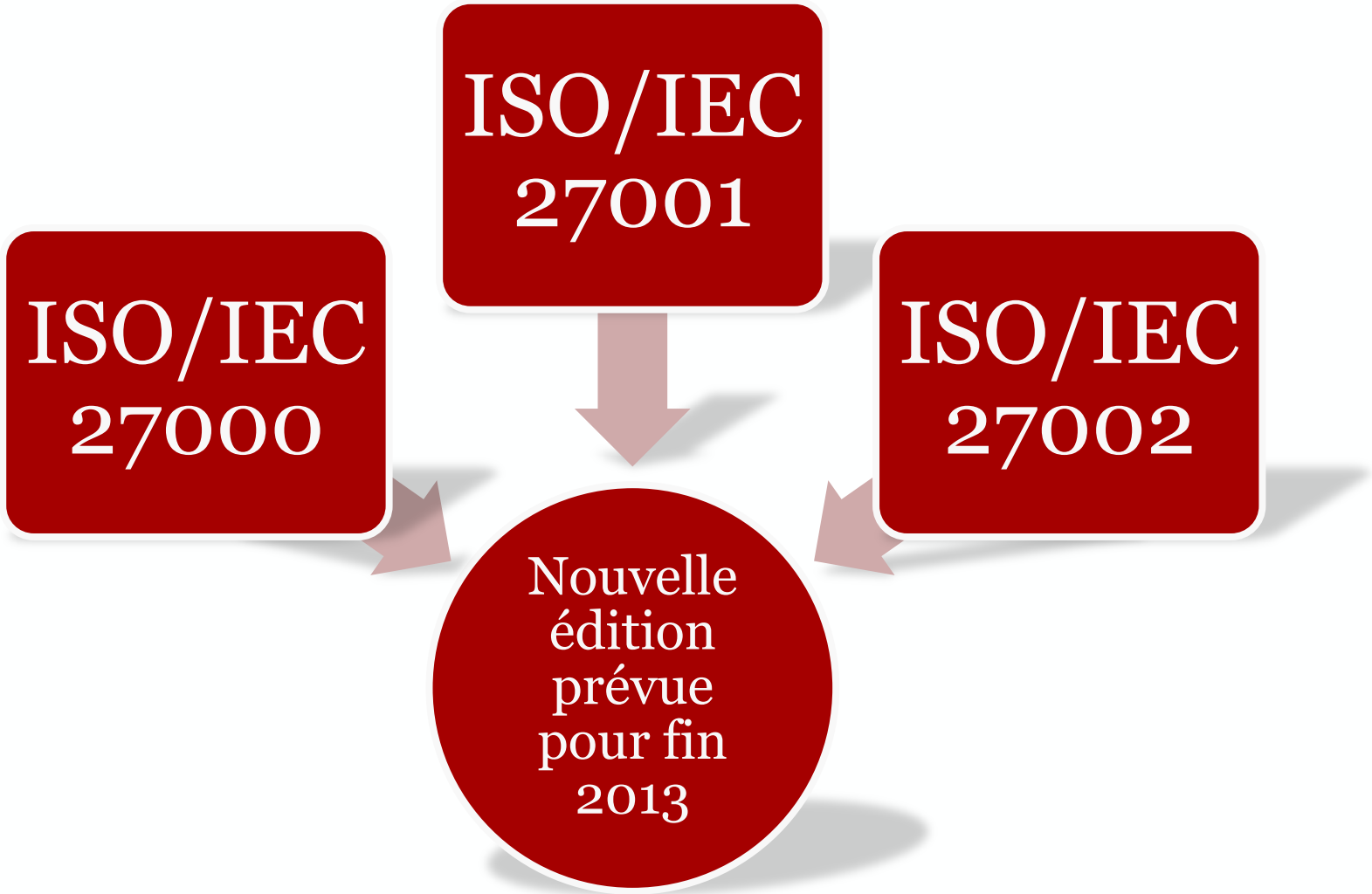
- Début de révision
  - Information security measurements [27004]
  - Information security management system implementation guidance [27003]
  - Overview and Vocabulary [27000]

- En élaboration
  - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 (security) [27017]
  - Code of practice for data protection controls for public cloud computing services (privacy) [27018]

- SP
  - Capability Maturity Framework for Information Security Management
  - Privacy / Personal Information Management Systems (PIMS)
  - Cloud computing security and privacy
  - Information Security within Smart Grid Environments
  - Adjustment of 27000 Vocabulary to align with 27001/2 Revision
  - International Certification of Information Security Management Specialists
  - Vocabulary Editing Document 2012-11-21

- NWIP
  - Use of ISO/IEC 27001 for Sector-Service Specific Third Party Accredited Certifications

WG1 : Information security management systems
Principaux projets en développement (suite)



ISO/IEC 27000

Information Security Management Systems - Overview and Vocabulary

ISO/IEC 27000
Overview and Vocabulary

- 2005 : publication de la 27001 et 27002
- Très rapidement : Nécessité de développer un vocabulaire commun et harmonisé autour de l'ISMS
- 2009 : 1ère édition ISO/IEC 27000
- 2010 : décision de révision pour s'aligner avec les travaux de révision de 27001 et 27002
  - Centraliser les termes et définitions dans la seule 27000
- Octobre 2012 : Promotion en FDIS
  - SU seul pays opposé (16 commentaires transmis)

ISO/IEC 27000
2009 vs 2012

- Définitions inchangées
  - *Information Security*
  - *Information Security Management System*
  - *Asset*
  - *Confidentiality / Integrity / Availability*
  - *Threat*
  - *Vulnerability (exploitation of one or more threats)*

- Suppression de définitions
  - *Information Security Risk*
  - *Information Asset*

- Ajout de définitions en lien avec la qualité / ISO 9000:2005
  - *Management*
  - *Validation*
  - *Verification*

- Modification de définitions
  - *Guideline (description that clarifies what should be done and how)*
  - *Non-repidation* (simplification)

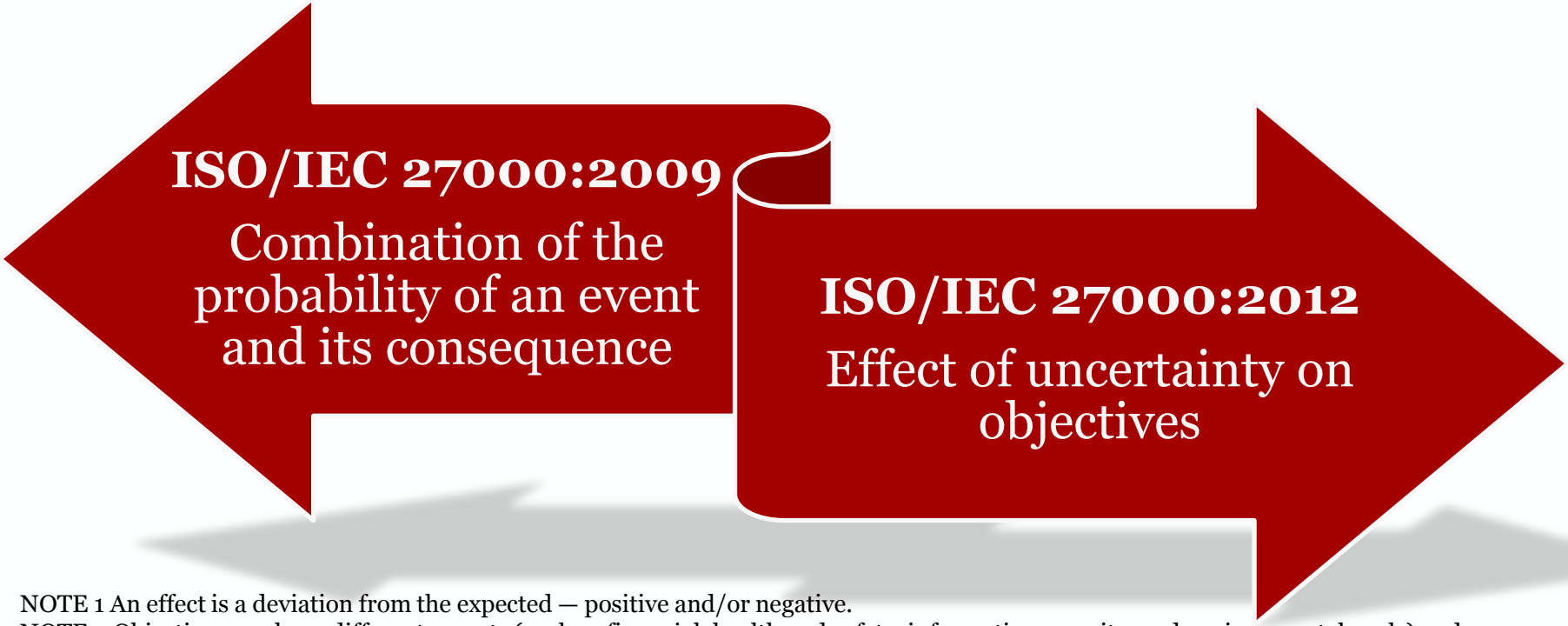
- Suppression de l'*Annex B (Categorized Terms)*,

- Mise à jour de la description et relations des normes de la famille 27000

- Approche plus globale de la gestion du risque
  - Alignement sur le Guide 73:2009 *Risk management – Vocabulary*

ISO/IEC 27000
2009 vs 2012

- Définition du risque
  - Guide 73:2002 *vs* Guide 73:2009



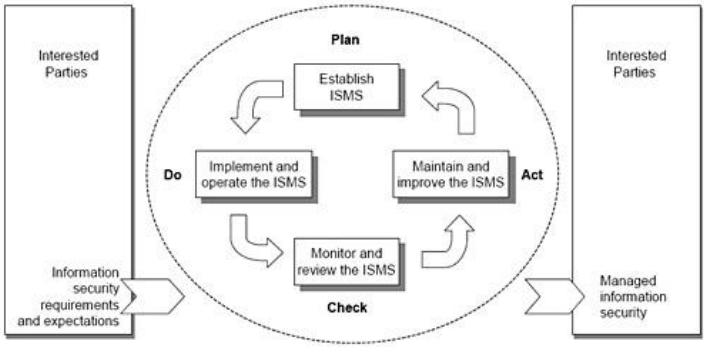
NOTE 1 An effect is a deviation from the expected — positive and/or negative.
NOTE 2 Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).
NOTE 3 Risk is often characterized by reference to potential events (2.24) and consequences (2.15), or a combination of these.
NOTE 4 Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood (2.40) of occurrence.
NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
NOTE 6 Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation

ISO/IEC 27001

Information Security Management Systems - Requirements

ISO/IEC 27001
Information Security Management Systems - Requirements

- 1999 : BS7799-2
- Octobre 2005 : 1ère édition ISO/IEC 27001
- Octobre 2008 : Décision de révision
- Octobre 2012 : Promotion en DIS
  - Oppositions
    - Approche (trop) globale du risque
      - Allocation des éléments en lien avec le risque pas suffisamment bien gérée (sections 6 et 8) [FI]
      - Perte d'exigences sur l'identification des risques, assets, menaces, vulnérabilités (report à une approche globale) [JP]
    - Amélioration (non) continue / Risque de confusion
      - Risque de confusion pour les 8000+ organisations certifiées dans le monde… [JP]
      - Non amélioration de la version en vigueur [AU, PL, NZ]
      - Ne va pas dans l'intérêt des utilisateurs actuels et futurs [AU, PL, NZ]
    - Mise en œuvre
      - Texte générique perdant les clarification et spécificités du domaine de la sécurité de l'information (perte de la présentation par processus) [JP]
      - Assignation de responsabilités fortes au top-management [AU, PL]
      - Comparaison avec les contrôles de l'annexe A alourdissant la démarche [FI]



ISO/IEC 27001
2005 vs 2013

- Approche du risque plus globale
  - Prédominance marquée
    - ISO 31000:2009 *Risk management -- Principles and guidelines*
    - ISO Guide 73:2009 *Risk management – Vocabulary*
    - Adaptation de la ISO/IEC 27005 en conséquence

  \+ norme plus globale

  – perte des spécificités de la sécurité de l'information

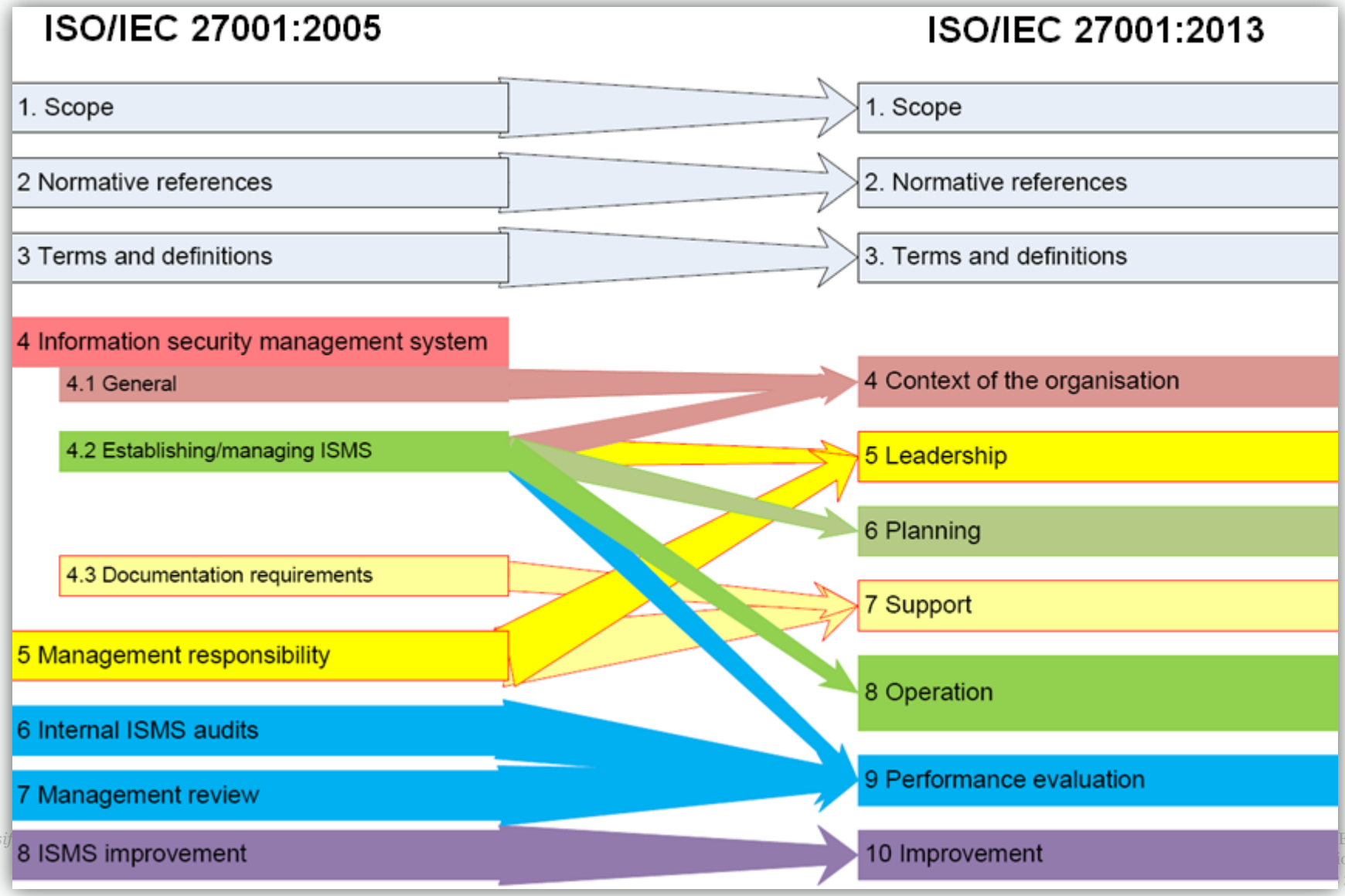
- Changement de structure
  - Décision ISO d'avoir une structure commune à tous les systèmes de management

- Annexe A
  - Sera ré-intégrée une fois ISO/IEC 27002 finalisée
  - Utilisation similaire en combinaison du SoA mais nécessité d'effectuer une comparaison des contrôles choisis avec Annex A

- Termes et définitions
  - Suppression des définitions
  - Alignement du contenu sur celles de ISO/IEC 27000

- Positionnement de ISO/IEC 27001
  - Norme d'exigences
    - Ne doit contenir que des exigences
    - Pas de lignes directrices / guidances ou explications sur la manière de mettre en œuvre les exigences
  - Retrait de tous les éléments non spécifiques à des exigences pour déplacer les guidances / lignes directrices vers les autres normes de la famille (27003, 27005)
  - Alignement des guidances / lignes directrices sur la 27001 et non l'inverse

ISO/IEC 27001
2005 vs 2013



Modèles de certification selon ISO/IEC 27001

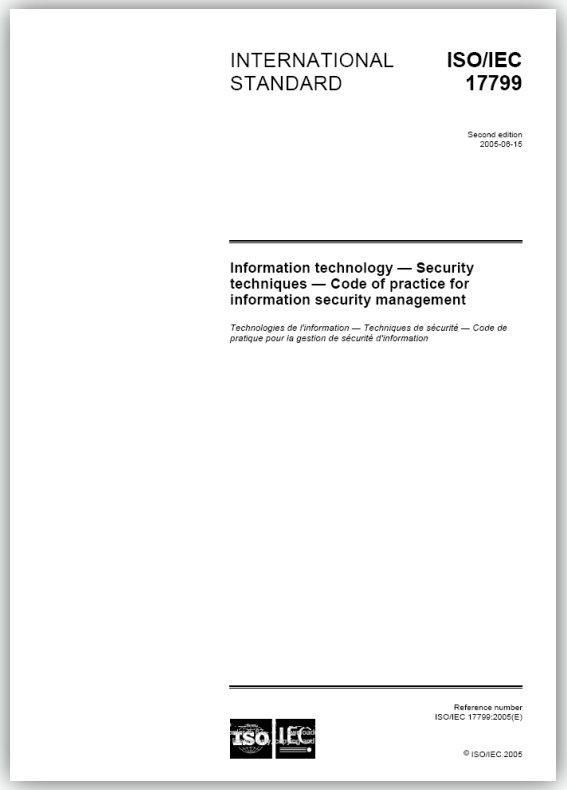
Domaines	Processus ISMS	Mesures de sécurité	Mesures de sécurité sectorielles
Information Security	ISO/IEC 27001	ISO/IEC 27001 Annex A	*none*
Privacy / Personal information	ISO/IEC 27001	ISO/IEC 27001 Annex A	PIMS
Telecommunication	ISO/IEC 27001	ISO/IEC 27001 Annex A	ISO/IEC 27011
Finance	ISO/IEC 27001	ISO/IEC 27001 Annex A	ISO/IEC 27015
Smart Grid	ISO/IEC 27001	ISO/IEC 27001 Annex A	ISO/IEC 27019
Information Security for Cloud Computing consumers	ISO/IEC 27001	ISO/IEC 27001 Annex A	ISO/IEC 27017
Privacy for Cloud Computing providers	ISO/IEC 27001	ISO/IEC 27001 Annex A	ISO/IEC 27018 (& PIMS)

ISO/IEC 27002

Code of practice for information security controls

ISO/IEC 27002
Code of practice for information security controls

- 1995 – 1998 : BS7799-1
- Décembre 2000 : 1ère édition ISO/IEC 17799
- Juillet 2005 : 2ème édition ISO/IEC 17799
- Juillet 2007 : nouvelle numérotation pour ISO/IEC 27002
- Octobre 2008 : Décision de révision
- Octobre 2012 : Promotion en DIS
  - JP opposée à la promotion en DIS
    - *De très nombreux commentaires sur la norme, dont de nombreux au cours de la session de Rome mériteraient plus de réflexion quant à leur adoption*
    - *Souhait d'un 2nd CD au lieu d'une promotion directe en DIS*


INTERNATIONAL STANDARD

ISO/IEC 17799

Second edition
2005-06-15

Information technology — Security techniques — Code of practice for information security management

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

Reference number
ISO/IEC 17799:2005(E)

© ISO/IEC 2005

ISO/IEC 27002
2005 vs 2013

	ISO/IEC 27002:2005		*3rd revision of 27002 (DIS)*	
Security clauses	***Security Categories***	***Security Controls***	***Security Categories***	***Security Controls***
Security policy	1	2	1	2
Organization of information security	2	11	1	7
Asset management	2	5	2	6
Human resources security	3	9	3	10
Physical and environmental security	2	13	2	13
Supplier relationship management	none	none	3	5
Communications and operations management	10	32	10	25
Management of application services on networks	none	none	1	2
Access control	7	25	4	13
Information systems, acquisition, development and maintenance	6	16	4	14
Information security incident management	2	5	1	7
Business continuity management	1	5	1	5
Compliance	3	10	3	9
TOTAL	*39*	*133*	*36*	*118*
TOTAL Security Clauses	*11*		*13*	

Des travaux normatifs pour la sécurité de l'information

Cryptography and security

ISO/IEC JTC1 SC27
IT Security Techniques

telindus belgacom ICT
together with belgacom tango

SC27

WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

WG2 : Cryptography and security mechanisms

- Identification des besoins et exigences pour les techniques et mécanismes de cryptographie dans les systèmes et applications

- Développement de la terminologie, les modèles généraux et normes pour leur utilisation dans des services de sécurité

- Techniques et mécanismes cryptographiques / non-cryptographiques pour
  - Confidentialité
  - Intégrité
    - Authentification des messages
    - Fonctions de hash
    - Signature numérique
  - Authentication des parties
  - Non-répudiation
  - Gestion des clés

WG2 : Cryptography and security mechanisms

- Domaine (très) technique
  - CD 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 F(r_A, g), constructs the key token KT_{A1} = F(r_A, g), and sends it to entity B.

Key construction (B1) Entity B randomly and secretly generates r_B in H, computes F(r_B, g), and constructs the key token KT_{B1} = 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 = kdf(K_{AB}). Entity B further constructs MAC$_K$(2||KT_{A1}||KT_{B1}),

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

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

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

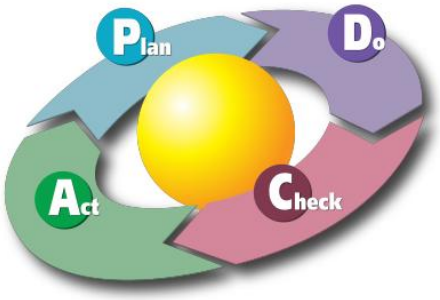
Entity A computes the key K = kdf(K_{AB}). Entity A computes MAC$_K$(2||KT_{A1}||KT_{B1}) and verifies what was sent by entity B. Entity A then computes MAC$_K$(3||KT_{A1}||KT_{B1}),

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

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

WG2 : Cryptography and security mechanisms
Statut

- Domaine (très) technique
  - Key management [11770]
  - Time-stamping services [18014]
  - Encryption algorithms [18033]
  - Anonymous digital signatures [20008]
  - Anonymous entity authentication [20009]
  - …



- Amélioration continue (*Systematic Review* et *Technical Corrigendum*)
  - Entity authentication - Part 2: Mechanisms using asymmetric encipherment algorithms [IS 9798-2:2008]
  - Non-répudiation -- Partie 2: Mechanisms using symmetric techniques [IS 13888-2:2010]
  - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation [IS 15946-5:2009]
  - …

- Nouveaux projets
  - Cryptographic algorithms and security mechanisms conformance testing [NP 18367]
  - Blind digital signatures [NP 18370]
  - Password-based anonymous entity authentication [NWIP]
  - Lightweight hash-functions [NWIP]
  - Criteria for the standardization of encryption algorithms [NWIP]

- Volonté d'harmonisation du vocabulaire
  - Harmonized vocabulary (2nd edition) [SD3]

- Aucune norme internationale récemment publiée

Des travaux normatifs pour la sécurité de l'information

Security evaluation, testing and specification

ISO/IEC JTC1 SC27
IT Security Techniques

telindus belgacom ICT
together with belgacom tango

SC27

WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

WG3 : Security evaluation, testing and specification

- Ingénierie de la sécurité, normalisation des spécifications en sécurité, évaluation, test et certification des systèmes, composants et produits
  - Critères d'évaluation de la sécurité
  - Méthodologie d'application de ces critères
  - Sécurité fonctionnelle et assurance de la spécification des systèmes, composants et produits
  - Méthodologie de test pour la détermination de la sécurité fonctionnelle, conformité et assurance
  - Procédures et schémas pour tests, évaluations, certifications et accréditations

WG3 : Security evaluation, testing and specification
Statut

- Principaux projets publiés
  - Evaluation criteria for IT security [15408] [Common Criteria]
    - Part 1: Introduction and general model
    - Part 2: Security functional components
    - Part 3: Security assurance components
  - Trusted Platform Module [11889]
    - Part 1: Overview
    - Part 2: Design principles
    - Part 3: Structures
    - Part 4: Commands
  - A framework for IT security assurance [15443]
    - Part 1: Overview and framework
    - Part 2: Assurance methods
    - Part 3: Analysis of assurance methods (under revision)
  - Guide for the production of Protection Profiles and Security Targets [15446]
  - Methodology for IT security evaluation [18045]
  - Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) [21827]
  - Refining software vulnerability analysis under 15408 and 18045 [20004]
    - Seul projet publié en 2012

WG3 : Security evaluation, testing and specification
Statut (suite)

- Promotion en DIS
  - Vulnerability disclosure [29147]
  - Vulnerability handling processes [30111]

- Principaux projets en développement
  - Detailing software penetration testing under 15408 and 18045 vulnerability analysis [30127]
  - Physical Security Attacks, Mitigation Techniques and Security Requirements [30104]
  - Secure system engineering principles and techniques [29193]
  - Security assurance framework [15443] (révision)
    - Part 1: Introduction and concepts
    - Part 2: Analysis

Des travaux normatifs pour la sécurité de l'information

Security controls and services

ISO/IEC JTC1 SC27
IT Security Techniques

telindus belgacom ICT
together with belgacom tango

SC27

WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

WG4 : Security controls and services

- Accompagnement dans la mise en œuvre de la série ISO/IEC 27000

- Considération des problèmes de sécurité existants / émergents qui pourraient résulter de l'augmentation de l'usage des TICs et les technologies en lien avec Internet

WG4 : Security controls and services
Nombreuses liaisons avec l'industrie

- Cloud Computing Security & Information security for supplier relationships
  - Cloud Security Alliance (CSA)
  - ISACA
  - EuroCloud
  - ISF
  - JTC1 SC38
- Governance & Information security for supplier relationships
  - ISACA
- IT Security management
  - (ISC)²
- Smart Grid Security
  - ENISA
- Information security incident management & Digital evidence
  - FIRST
  - INTERPOL
- Governance of digital forensic risk framework
  - JTC1 SC7
- Storage Security

WG4 : Security controls and services

Current version	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Under revision?			✓						✓						✓																
IS / TR																															
FDIS / DTR																															
DIS / PDTR																															
CD																															
WD																															
PD																															
NWIP																															
SP																															
	27031	27032	27033-1	27033-2	27033-3	27033-4	27033-5	27033-6	27034-1	27034-2	27034-3	27034-4	27034-5	27034-6	27035	27035-1	27035-2	27035-3	27036-1	27036-2	27036-3	27036-4	27037	27038	27039	27040	27041	27042	27043	27044	24762

Statut en sortie de la réunion SC27 de Rome (2012-10)

WG4 : Security controls and services
Principaux projets

27033 Network Security

- Overview and concepts (2009)
- Guidelines for the design and implementation of network security (2012)
- Reference networking scenarios -- Threats, design techniques and control issues (2010)
- Securing communications between networks using security gateways
- Securing communications across networks using Virtual Private Network (VPNs)
- Securing wireless IP network access

WG4 : Security controls and services
Principaux projets

27034 Application security

- Overview and concepts (2011) (Technical Corrigenda en 2012)
- Organization normative framework
- Application security management process
- Application security validation
- Protocols and application security controls data structure
- Security guidance for specific applications

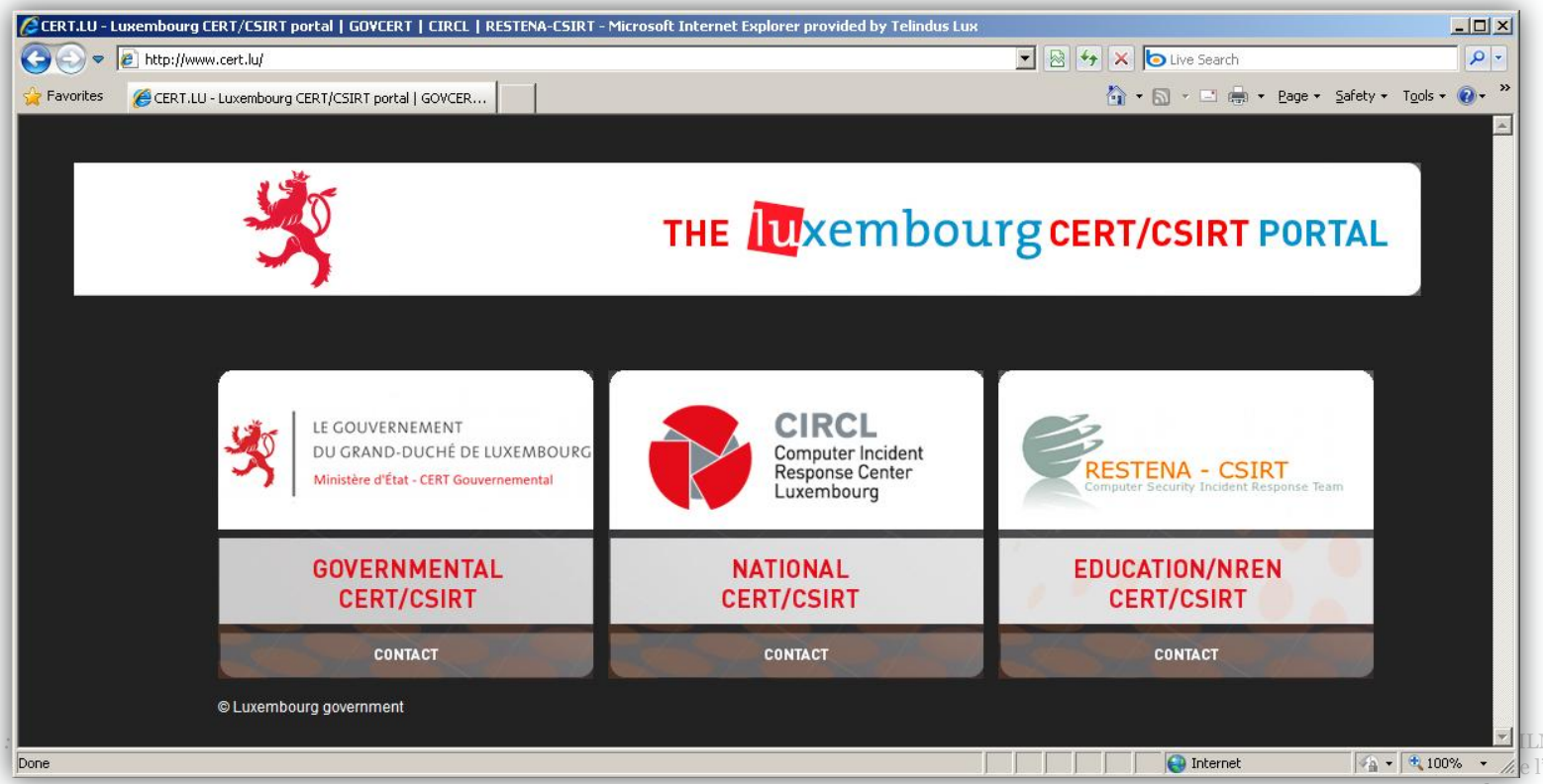
WG4 : Security controls and services
Principaux projets

27035 Information security incident management (2011)

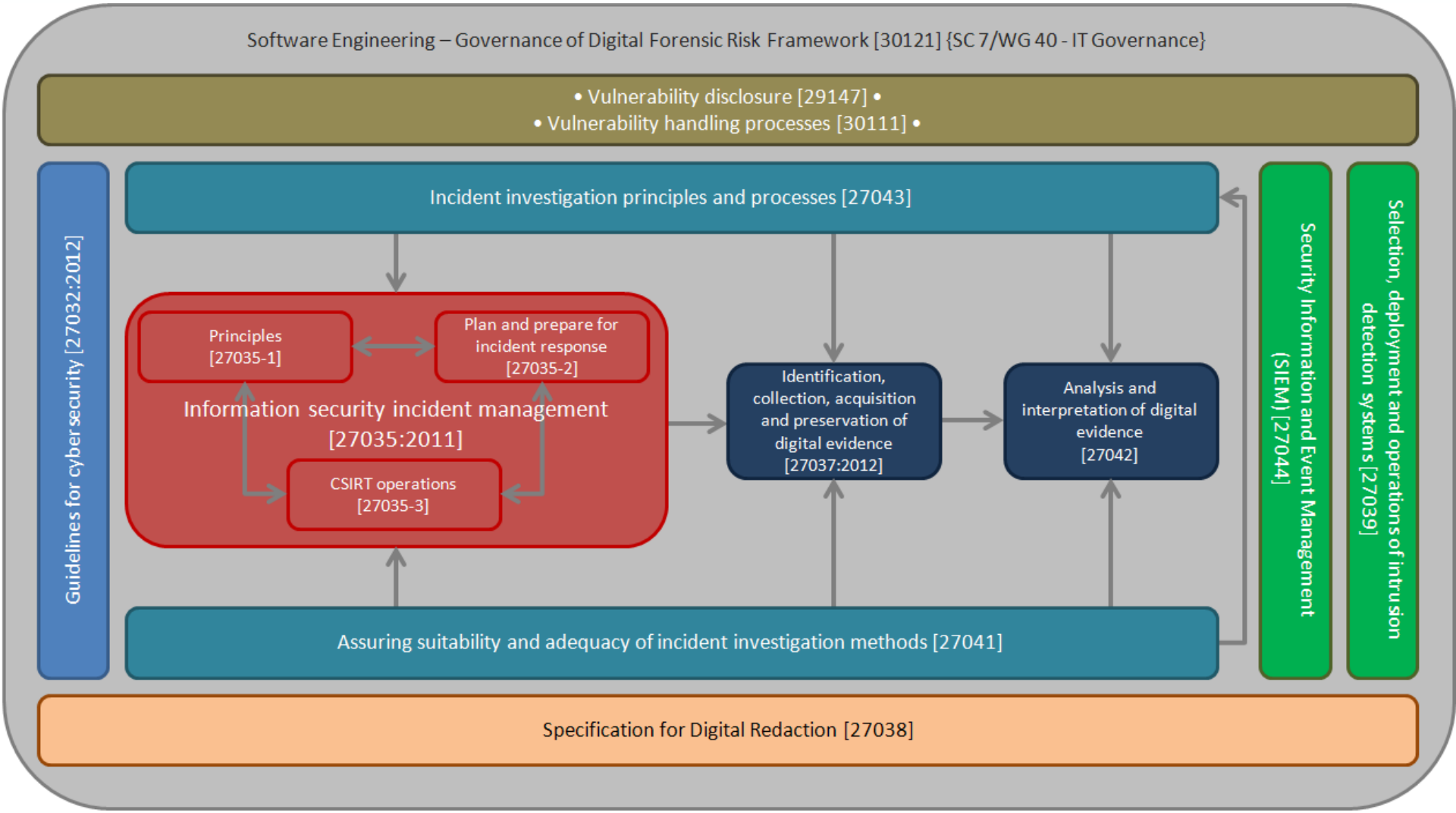
- Principles of incident management
- Guidelines to plan and prepare for incident response
- Guidelines for CSIRT operations

Gérer les incidents de sécurité

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'Etat - Cyber Security Board



Gérer les incidents de sécurité
Les normes ISO du SC27 sur la question



WG4 : Security controls and services
Principaux projets

telindus belgacom ICT
together with belgacom tango

27036 Information security for supplier relationships

- Overview and concepts

  (vouée à gratuité ?)
- Requirements
- Guidelines for ICT supply chain security
- Guidelines for security of cloud services

WG4 : Security controls and services
Autres projets déjà publiés

- Business continuity
  - Guidelines for information and communications technology disaster recovery services [24762:2008]
  - Guidelines for information and communication technology readiness for business continuity [27031:2011]

- Autres normes publiées
  - Best practices for the provision and use of time-stamping services [29149:2012]
  - Specification of TTP services to support the application of digital signatures [15945:2002]
  - Selection, deployment and operations of intrusion detection systems [18043:2006]

Des travaux normatifs pour la sécurité de l'information

Identity management and privacy technologies

ISO/IEC JTC1 SC27
IT Security Techniques

telindus belgacom ICT
together with belgacom tango

SC27

WG1	WG2	WG3	WG4	WG5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and services	Identity management and privacy technologies

WG5 : Identity management and privacy technologies

- Dévelopement et maintenance de normes et lignes directrices considérant les aspects de sécurité en lien avec
  - Identity management
  - Biométrie
  - Privacy

WG5 : Identity management and privacy technologies
Statut

- Principaux projet publiés
  - Identity management
    - A framework for identity management [24760]
      - Part 1: Terminology and concepts
  - Biométrie
    - Biometric information protection [24745]
  - Privacy
    - Privacy framework [29100]
      - Projet de lier un *Privacy / Personal Information Management Systems* (SP PIMS)
    - Privacy references list [SD2]

- Promotion en FDIS
  - Requirements for partially anonymous, partially unlinkable authentication [29191]

- Promotion en norme internationale
  - Entity authentication assurance framework [29115]

WG5 : Identity management and privacy technologies
Principaux projets en développement

Identity Management

- A framework for identity management [24760]
  - Part 2: Reference architecture and requirements [WD]
  - Part 3: Practice [WD]

Access Management

- A framework for access management [WD 29146]

Privacy

- Code of practice for data protection controls for public cloud computing services [WD 27018]
- Privacy / Personal Information Management Systems (PIMS)
- Privacy capability assessment model [WD 29190]
- Privacy architecture framework [CD 29101]
- Privacy impact assessment [NP 29134]

Authentication

- Entity authentication assurance framework [FDIS 29115]
- Requirements for partially anonymous, partially unlinkable authentication [DIS 29191]
- Telebiometric authentication framework using biometric hardware security module [WD 17922]
- Identity proofing [NP 29003]

Le SC27 en une planche

ISO/IEC JTC1/SC27

TITLE	**IT Security techniques**	**DATE OF CREATION**	1990
SECRETARIAT	Deutsches Institut für Normung (DIN)	**P-MEMBERS** **O-MEMBERS**	49 17
SECRETARY	Mrs Krystyna Passia	**PUBLISHED STANDARDS**	117
CHAIRPERSON	Dr. Walter Fumy (Germany) (until end 2013)	**STANDARDS UNDER DEVELOPMENT**	70
SCOPE	Development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects ✓ Management of information and ICT security, information security management systems (ISMS) ✓ Cryptographic and other security mechanisms ✓ Security evaluation criteria and methodology ✓ Security aspects of identity management, biometrics and privacy		
MAIN STANDARDS	ISO/IEC 27001:2005 - Information security management systems – Requirements ISO/IEC 27002:2005 - Code of practice for information security management		

NATIONAL STUDY COMMITEE

MEMBERSHIP	P-Member
DATE OF CREATION	August 2002
NATIONAL EXPERTS	13

NATIONAL CHAIRPERSON

Cédric MAUNY	
Telindus Luxembourg	
Technology Leader CISM, CISSP, ISO27001, ITIL	

telindus
belgacom ICT

Merci pour votre attention

together with
belgacom
tango

MEMBER OF THE ILNAS NETWORK

telindus
belgacom ICT

Questions & Réponses

together with
belgacom
tango

MEMBER OF THE ILNAS NETWORK

telindus
belgacom ICT

Pour me contacter

Cédric Mauny
cedric.mauny@telindus.lu
(+352) 621.200.707

together with
belgacom
tango

MEMBER OF THE ILNAS NETWORK