

Status on the 27000 series

ISACA IT *security forum*

Alain De Greve (Fortis)
Jean-Luc Allard (VP Information Security – ISACA)

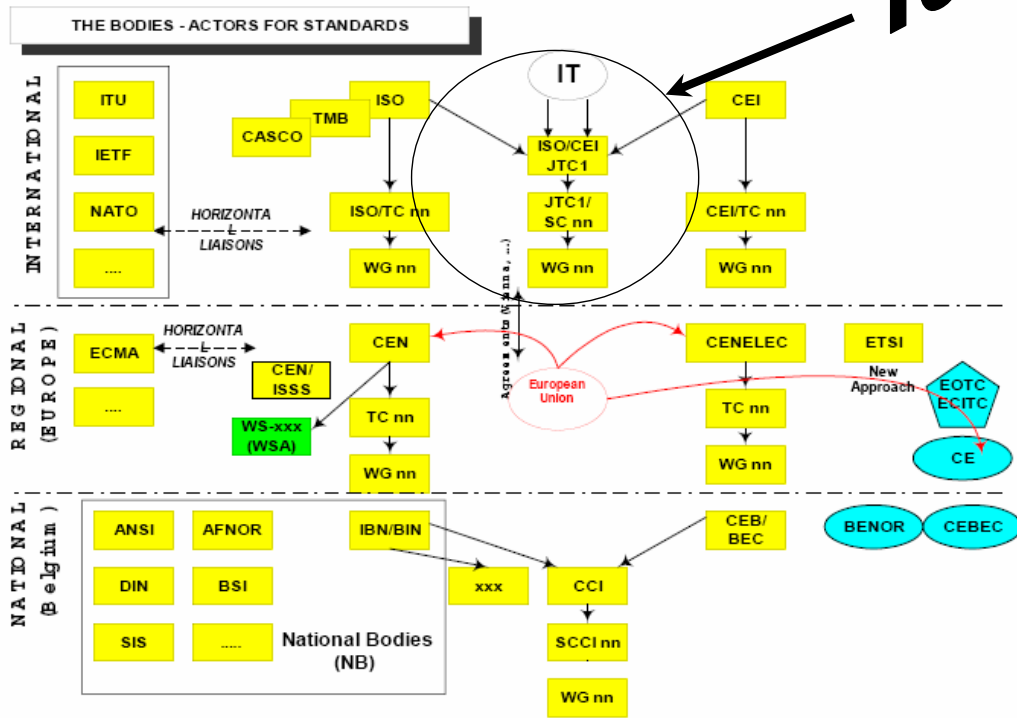
ISRM | Alain De Greve | February 13,2008 | 1

Schedule for the ISACA IT Security Forum

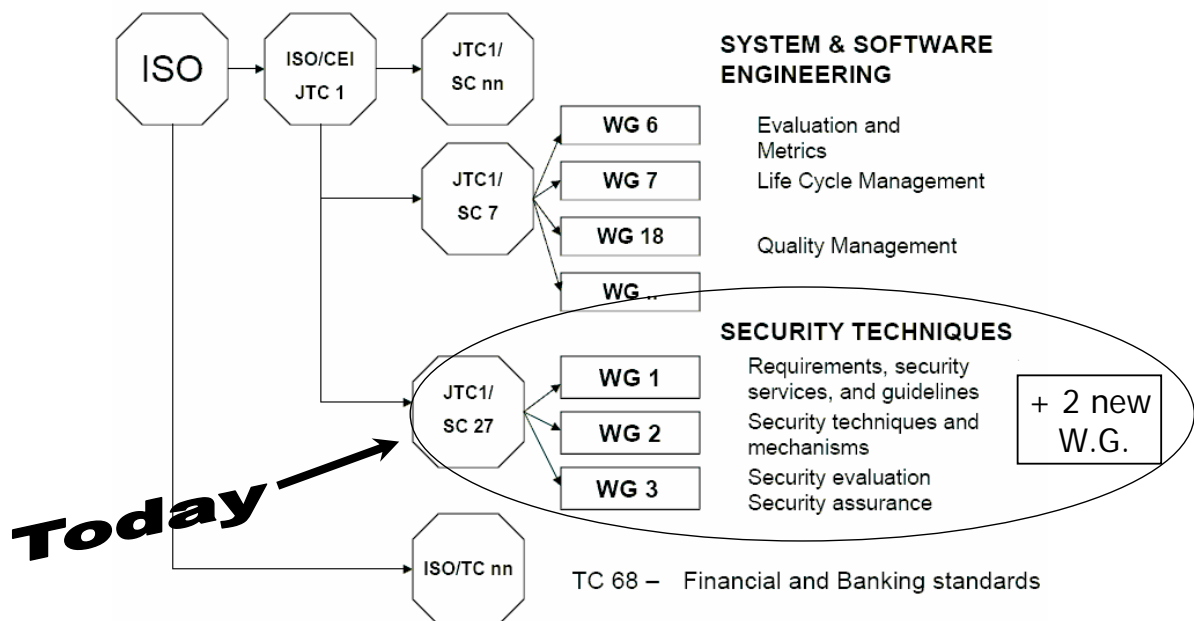
- 17.00 – 17.30 Welcome coffee
- 17.30 – 17.35 Introduction on the forum Jean-Luc Allard (VP Security ISACA Belux)
- 17.35 – 17.45 Introduction of the participants
- 17.45 – 18.05 Update on the status of ISO standards
 - Snapshot SC27, WG1 and WG4 (ADG)
 - Snapshot WG2, WG3 and WG5 (JLA)
- 18.05 – 18.30 Open Discussion: part I
- 18.30 – 19.15 Refreshments & Networking break
- 19.15 – 19.45 Open Discussion: part II
- 19.45 – 19.50 Conclusions Jean-Luc Allard
- 19.50 – 19.55 Selection of the next Topic's

Place of the ISO

Today



Structure of the IT Security techniques



Today

Principles of construction

– ISO standards are developed according to the following principles:

– **Consensus**

The views of all interests are taken into account: manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions and research organizations.

– **Industry-wide**

Global solutions to satisfy industries and customers worldwide.

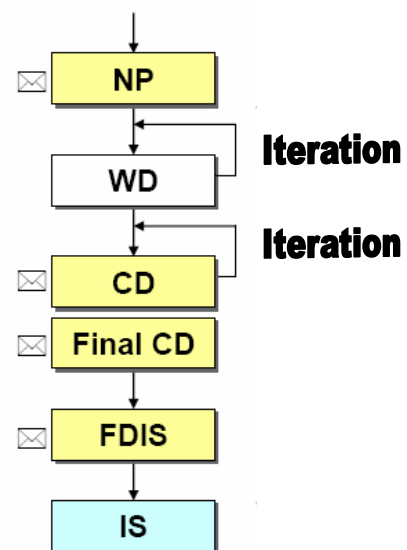
– **Voluntary**

International standardization is market-driven and therefore based on voluntary involvement of all interests in the market-place.

Norm Production Schema (standard)

Maturity level / state of standardization

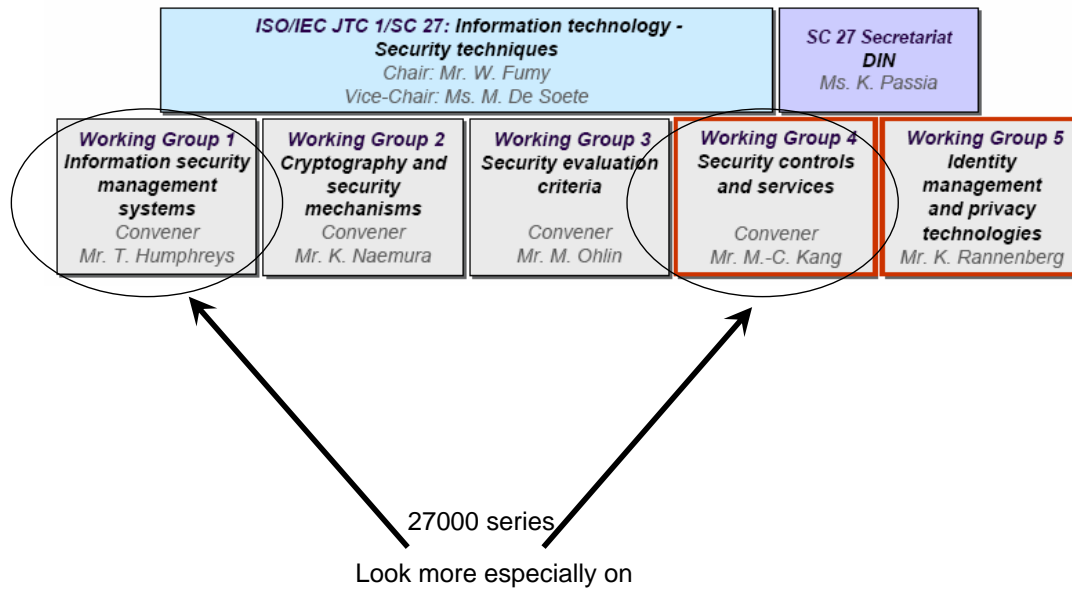
- **Study Period / New Project (NP)**
 - 2 month NP letter ballot*)
- **Working Draft (WD)**
- **Committee Draft (CD/FCD)**
 - 3 month CD ballot(s)
 - 4 month FCD ballot
- **Draft International Standard (DIS/FDIS)**
 - 2 month FDIS ballot
 - no more comments at this stage
- **International Standard (IS)**
 - review every 5 years
 - or after 'defect report'



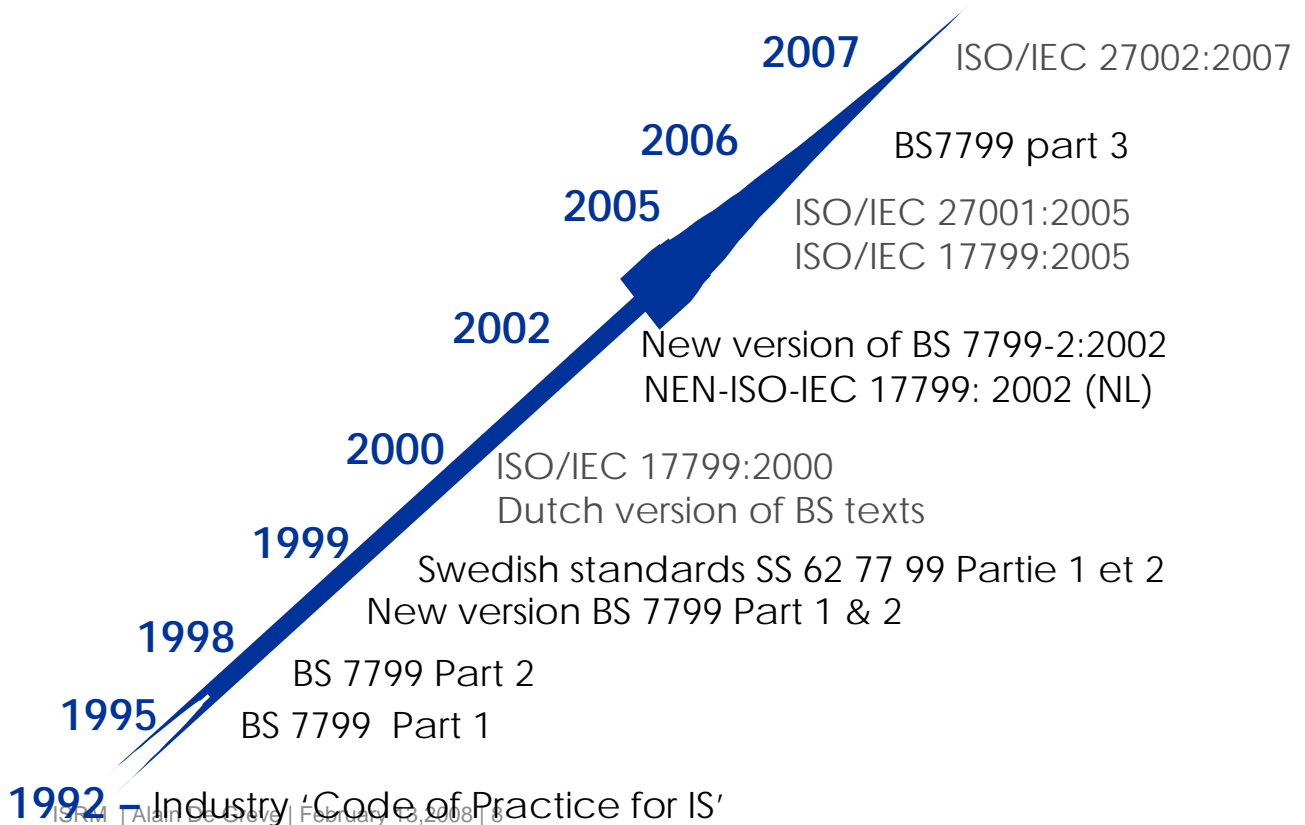
*) one vote per P-member

Thus normally actually around 2.8 years

Actual Structure of the sc27

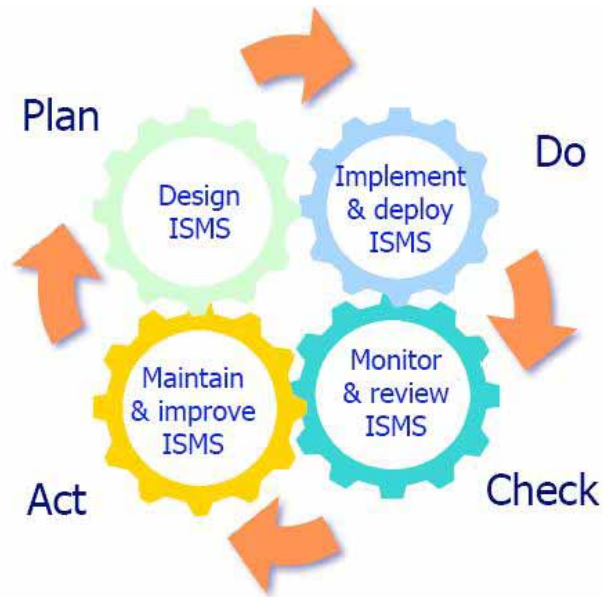


History of « code of practice »

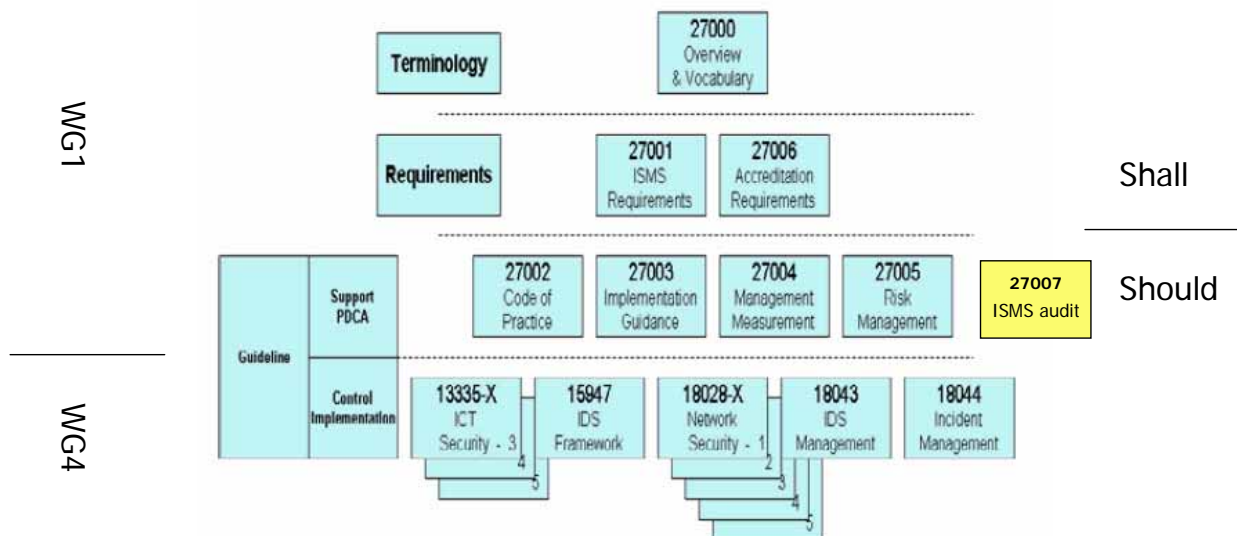


PDCA (Wheel of William Edwards Deming – Shewhart)

Generally accepted principle for plan of ISMS norms

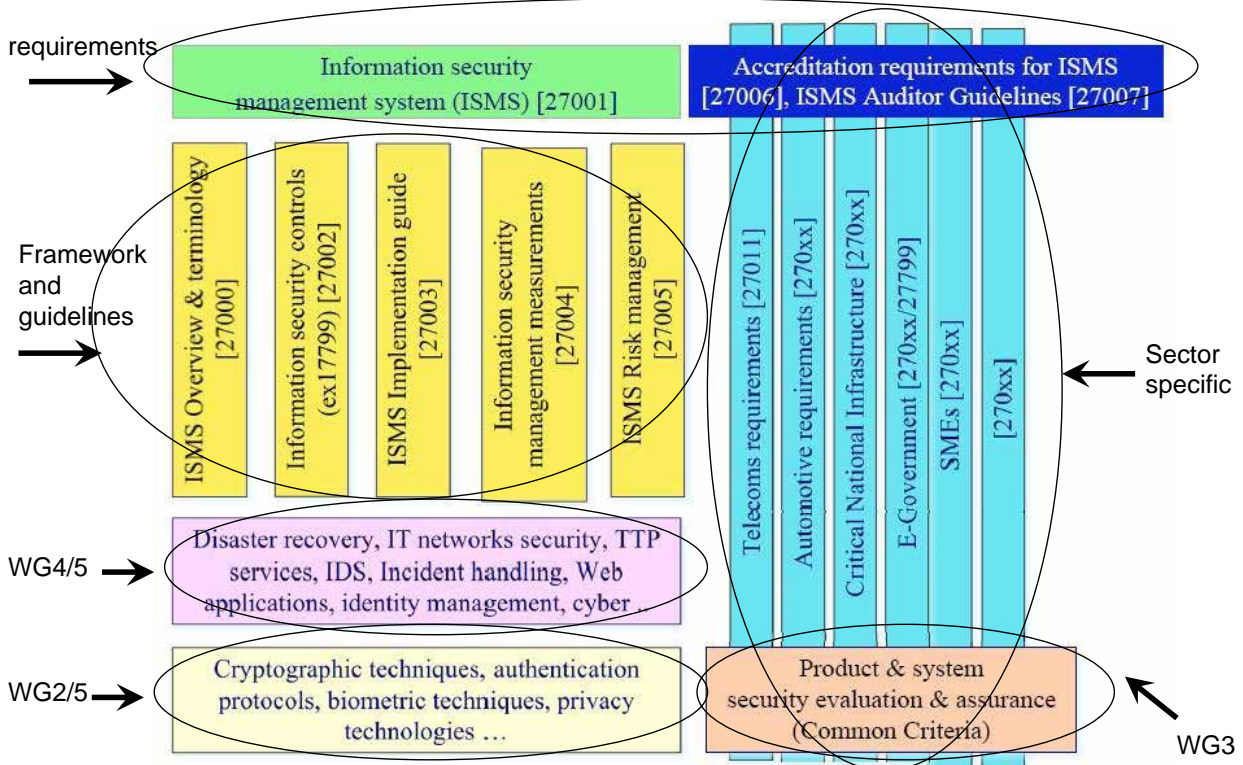


ISMS family pyramid

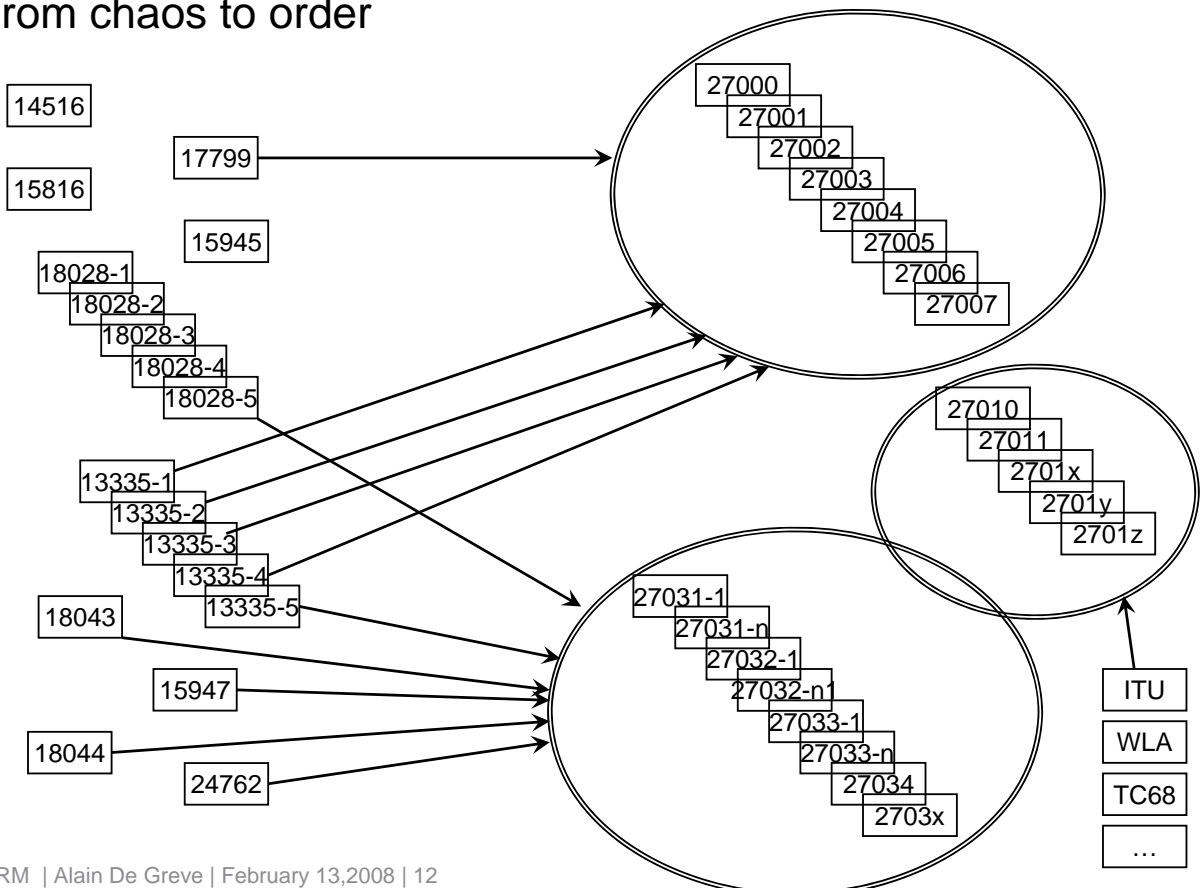


The well known pyramid used since some season's in SC27 presentation on ISMS but now a more explicit exists

ISMS family mapping



From chaos to order



The history of 27000

- Discussion initiated during the fall 2004 in Kuala Lumpur meeting
 - Little trace in the meeting report
- Opening point at the Vienna meeting (spring 2005)
 - Vote on the numbering debate result (was an document issued month before that did focus much attention)
 - Limited scope (27000 till 27005)
 - Personal discussion with Ted during a break (enlarge the range asked at ISO)
- At the fall meeting was known that a substantial range was possible
 - Together with the project of creating new working group and split the wg1
 - Issue for some experts
 - Increase of the number of parallel sessions (see further)
- Actually most of the range 27000 till 27049 is blocked
 - ISO may have concerns on blocking an number without having a document in a short future

- Exception – presence in the range of :
 - ISO DIS 27025 Space systems -- Programme management -- Quality assurance requirements (to be published in 2009)

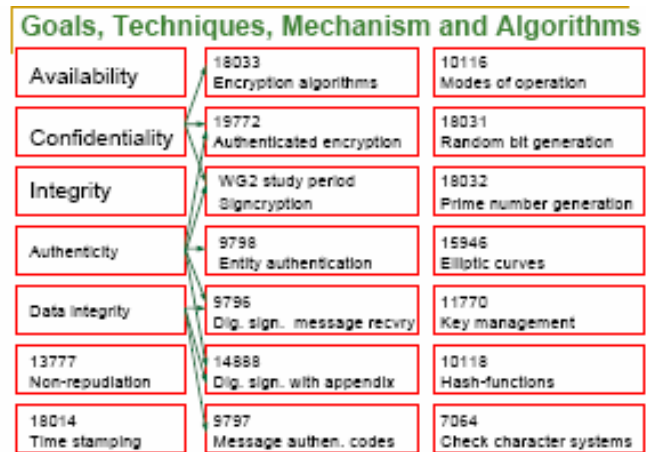
- Why 27000
 - ISO / IEC / JTC1 / SC 27

WG1 – ISMS - plan of work

- ISO/IEC 27000 : ISMS Overview and vocabulary (CD)
- ISO/IEC 27001 : ISMS requirements (published)
- ISO/IEC 27002 : ISMS code of practice(ex.17799) published)
- ISO/IEC 27003 : ISMS implementation guidance (WD)
- ISO/IEC 27004 : ISMS metrics and measurements (WD)
- ISO/IEC 27005 : ISMS risk management (FDIS)
- ISO/IEC 27006 : ISMS accreditation (published)
- ISO/IEC 27007 : ISMS audit guidelines (WD)
- ISO/IEC 2700n : ISMS technical audits (proposition from Sweden)
- ISO/IEC 27011 : ISMS telecommunications (FDIS)
- ISO/IEC 270nn : ISMS world lottery association (np)
- ISO/IEC 270nn : ISMS financial sector (foreseen)
- ISO/IEC 270nn : ISMS automotive industry technical ISMS audits (np)
- ISO/IEC 270nn : ISMS for e-government (study period launched in Lucerne)
- ISO/IEC 270nn : ISMS for critical infrastructure (study period launched in Lucerne)
- ISO/IEC 270nn : ISMS for SME's (foreseen since ENISA meeting last November)
- ISO/IEC 270nn : Recommendations and proforma for the preparation of domain-specific implementation guidelines (np)
- Wg1 roadmap

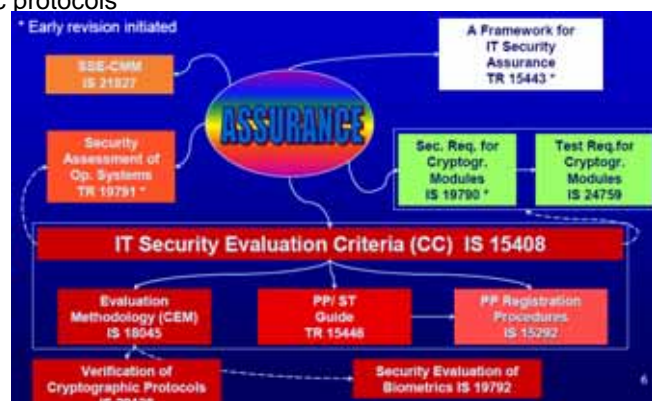
WG2 - Crypto - plan of work

- ISO/IEC 9796 : Digital signature schemes giving message recovery
- ISO/IEC 9797 : message authentication codes
- ISO/IEC 9798 : entity authentication
- ISO/IEC 10118 : hash-functions
- ISO/IEC 11770 : key management
- ISO/IEC 14888 : digital signatures with appendix
- ISO/IEC 15946 : cryptographic techniques based on elliptic curves
- ISO/IEC 18014 : time stamping services
- ISO/IEC 18031 : random bit generation
- ISO/IEC 18032 : Prime number generation
- ISO/IEC 18033 : encryption algorithms
- ISO/IEC 24745 : biometric template protection
- ISO/IEC nnnnn : signcryption
- Wg2 roadmap



WG3 - evaluation - plan of work

- ISO/IEC 15292 : Protection profiles registration procedures (pub)
- ISO/IEC 15408 : Evaluation criteria for IT Security (Common Criteria) (revision)
- ISO/IEC 15443 : A framework for IT security Assurance (partly pub)
- ISO/IEC 18045 : Methodology for IT Security evaluation
- ISO/IEC 19790 : Security requirements for cryptographic modules
- ISO/IEC 19791 : Security assessment of operational systems
- ISO/IEC 19792 : A framework for security evaluation and testing of biometric technology
- ISO/IEC 21827 : Capability Maturity Model(SEE-CMM)
- ISO/IEC nnnnn : responsible vulnerability disclosure (np)
- ISO/IEC nnnnn : Test requirements for cryptographic modules
- ISO/IEC nnnnn : Secure System design
- ISO/IEC nnnnn : Verification of cryptographic protocols
- Wg3 roadmap



SC27 planning

- Next meeting
 - Japan – Kyoto – April 2008 (14-18+plenary 21-22)
 - Cyprus – Lemesos – October 2008
 - China - ??? – Spring 2009 (April)

- Projects (wg1)
 - Some are in study period
 - WLA (but renewed!)
 - Automotive
 - Some will be initiated in Japan
 - ISMS for SME's
 - Revision of 27002
 - 27008 ???
 - Some are frozen
 - ISMS for Banking Sector

	14 th April Mon	15 th April Tues	16 th April Wed	17 th April Thurs	18 th April Fri
WG1 Plenary Room					
WG1 Plenary	09h30 - 11h30		11h30 - 12h30	11h00 - 12h30	10h30 - 12h30
WG1/WG4 Session	11h30 - 12h00			12h30 - 13h00	
ISO/IEC 27007	13h00 - 17h30	09h00 - 17h30	09h30 - 11h30		
Road Map			13h30 - 14h30		
Revision of ISO/IEC 27002			14h30 - 16h00		
Study periods Auto Sect. + WLA			16h00 - 17h30		
Study periods ISMS for e-govmt and crit.infra.				09h00 - 11h00	
ISMS for SMEs				13h30 - 15h00	
Study period on ISMS technical review				15h00 - 17h30	
Room A					
ISO/IEC 27004	13h00 - 17h30	09h00 - 17h30	09h00 - 17h30	09h00 - 17h30	
Room B					
ISO/IEC 27000	13h00 - 17h30	09h00 - 12h30			
ISO/IEC 27003		13h00 - 17h30	09h00 - 17h00	09h00 - 17h30	

SC27 planning

- Projects (wg4)
 - Drafting stage essentially
 - ICT readiness
 - Network security
 - Cybersecurity
 - Application security
 - Main characteristic
 - Multipart's standards
 - Some parts not yet defined
 - Work in parallel (ubiquity)

	14 Apr Mon	15 Apr Tue	16 Apr Wed	17 Apr Thu	18 Apr Fri
WG4 Plenary Room					
WG4 Plenary	09h30-11h30		11h30-12h30	11h30-12h30	10h30-12h30
WG1/4 Joint Plenary	11h30-12h00			12h30-13h00	
ICT Readiness for BC/DR/ER	13h00-17h00	09h00-12h00	14h00-17h00		
Network Security		13h00-17h00	09h00-12h00	09h00-11h30	
Roadmap	17h00-18h00				
Drafting Committee			17h00-18h00	17h00-18h00	09h00-10h30
WG4 Breakout Room					
Application Security	13h00-17h00	09h00-12h00	14h00-17h00	14h00-17h00	
Cyber Security		13h00-17h00	09h00-11h30	09h30-12h00	



Q & A

For further information

•E-mail :

•alain.degreve@fortis.com

•alain.degreve@skynet.be

•jeanluc.Allard@scarlet.be

Discussion 1

- How do you 'feel' the current ISO proposal?
- How far are you informed on what is available and the planning?
- What is your experience with ISO standards?
- What are your current problems with the standards you use(d)?

Thank you

Break

PART 2

- Certification or not ?
- Participation to standardization works

Certifications?

- Be very careful with the scope and the objective (statement of applicability)
- Is not the final target
- Many companies around the world are not only implementing ISO/IEC 27001 ISMS to protect different parts of their business processes, their information and the services they offer but they are also getting 3rd party certified.
- See www.iso27001certificates.com
 - For each country the list of certified companies
 - For some companies details of the scope
 - The list is not complete (based on information received by Ted Humphreys who manage the site)

Situation on standardization in Belgium topics for the discussion

- Some specialists from diverse consultancy and industry companies
- Mirror site hosted at KUL
- Contributions are actually few
- Existence of an XLS that summarize all past ,actual and future work
- Participation on international activities are appreciated (but limited : 1-3/4 persons)
 - Voluntary work , not sponsors at country level
- Support from institution is difficult
- Reorganization recently of national body
- Discussion in order to regulate way of work (some actions are ongoing)
 - Replacing the gap of NBN
 - Enhance the voluntary work of CS, JLA, ADG
 - Enforce the role of hosting and secretariat by Agoria–ICT
 - What can I do to promote my vision, the Belgian vision, the sector vision
 - Roles of professional organizations

Discussion 2

- What would you expect from ISO standards?
- How could you be involved in the comment and creation of future standards?

CONCLUSION

- Current work within ISO is evolving fast in many directions.
- Standards are not imposed on you as such, you may influence it
 - By giving us your concerns
 - By working with the Belgian expert working groups



Getting you there.

Thank you