BRUCON
BISI – Norm track

General information
Objectives
Actual situation

Ir. Alain De Greve, MCA, CISA

Personal presentation

- Agronomist (ULB-Brussels)
- Information Technology since 1986 (MF, DBA, Unix, Win, Sec.)
  - Experience in
    - Insurance (500p. Belgium origin, GB subsidiary , IT 30)
    - Telecom (1500p. ,mobile , IT 120)
    - Banking (>25000p , IST >1000)
- Formation - IST related
  - HEC St Louis (Brussels)
  - MCA (Antwerps)
  - CISA (ISACA)
- Contribution to ISO works
  - ISO/IEC JTC/1 SC27 IT Security Techniques (18044,18028,17799,27nnn,…)
  - ISO/TC68 : Banking sector(13569)
  - General coordinator of the ISO/IEC JTC 1/SC27 Belgian expert's
- Independent expert for the ENISA (www.enisa.europa.eu)
  - Risk assessment / risk management working groups from 2005 till 2008
- Collaborate to Clusib in the past (www.clusib.be)
  - Development of "incident management" research
- Founding member and board member of BCIE (www.bcie.be)
  - Chamber for witness, emanation of the ISACA Belgian chapter
- Co-initiator of the BISI
  - Writing a part of the whitepaper published in September 2008
  - convenor for the norm track

Norm track (extract whitepaper of September 2008)

• Minimal information and ICT security requirements based on international standards [see Annex C] should be specified and fully integrated into the various industry sector regulations. These should deal with aspects such as information security management and control framework, risk management, incident management, business continuity, evaluation and audit, reporting and compliance, etc. The requirements should also mention the need for accreditation for critical systems. The administration should lead the way for industries and private organizations where accreditation is not part of the implementation of security solutions.

• A number of information security standards allow for evaluation/certification. Currently Belgian manufacturers and organizations need to go abroad for the certification of their information security products and services. In view of the increasing professionalism in the sector and the increased demand for certified products and services, Belgium should establish its own information security certification framework, based on international standards in accordance with Belgian law and regulations. In this case the Belgian Accreditation Body (BELAC) should accredit the required information security certification authority and any evaluation center's). This governmental information security certification authority would then be in a position to issue the required certified products and services.
The initiative already begun in this area should continue to receive the necessary support in order to achieve these objectives.
The accredited information security certification organization should collaborate with other national certification bodies within the EU through the Common Criteria Recognition Agreement [7]. The aim would be to establish a harmonious certification framework with the other member states for the translation of standards enforced through European directives into the national certification program. On a larger scale (worldwide) this body needs to establish frameworks with peer organizations for cross-certification.

•Belgian efforts in international information security standardization need to be better coordinated. Although excellent work is being delivered by Belgian experts in these forums, there is no support or recognition from the Belgian Standardization Office (NBN). This coordinating role could, for instance, be fulfilled by Agoria, by acting as a single point of contact for the ICT sector ("sector operator"). These coordinated activities should be supervised by the Ministry of Economic Affairs and the Department of Scientific Policy.

Objective – Term of Reference

- Information Security Norms of interest for Belgium and Belgian's
  - Establish a list of international norms from all kind of origins with a potential interest for citizen and governments
  - Try to find priorities in the forest
- Put in place a "Belgian Scheme" for certification of products, services and systems
  - Identify the aspects regarding information security related certifications (e.g. Common Criteria, ITIL, 27001,…)
  - Look at the Belgian expectations, the actual situation, collaborate wih neighborhood countries to identify best practice and potential synergies and finally ensure independence of Belgium for recognized national strategic sectors, critical infrastructures,…
- Ensure Belgian delegation at international level
  - Ensure presence and contacts of recognized Belgian expert's in international forum and organizations (CEN, ETSI, ISO, ITSMF, ECSA,,…) with as a result a greater visibility for the Belgian community
  - Identify what exits worldwide and where we should put our interest for the public and private Belgian sector
- Phased approach
- The work is done in close collaboration with (among others)
  - Agoria ICT
  - Fedict – Belnis
  - ANS (for the second part)

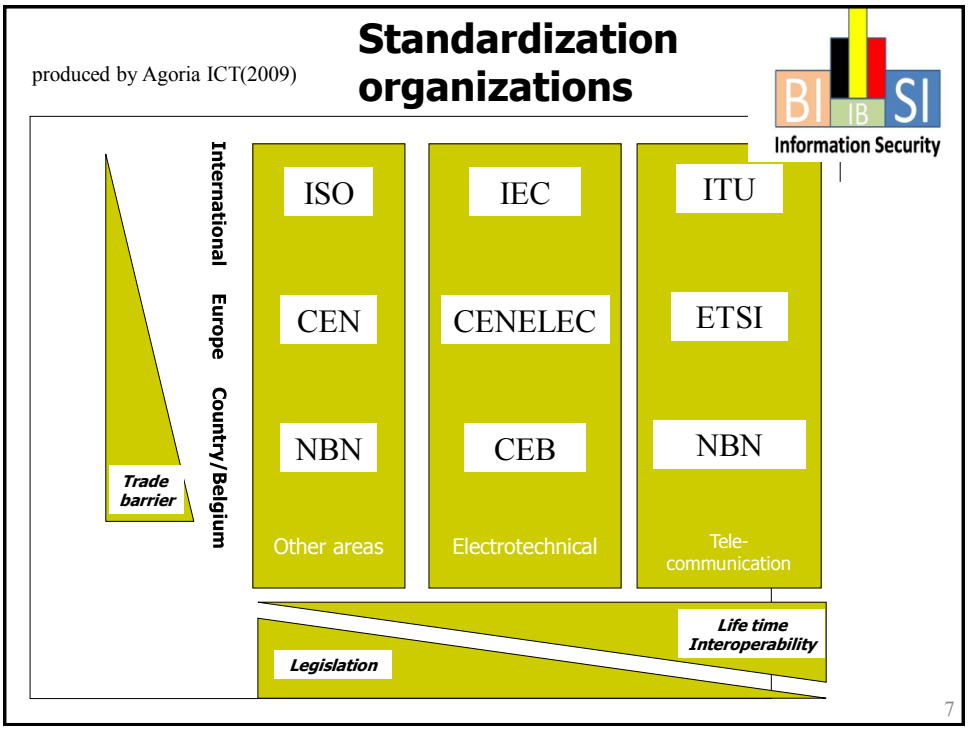
BISI objective: 1 > Inventory

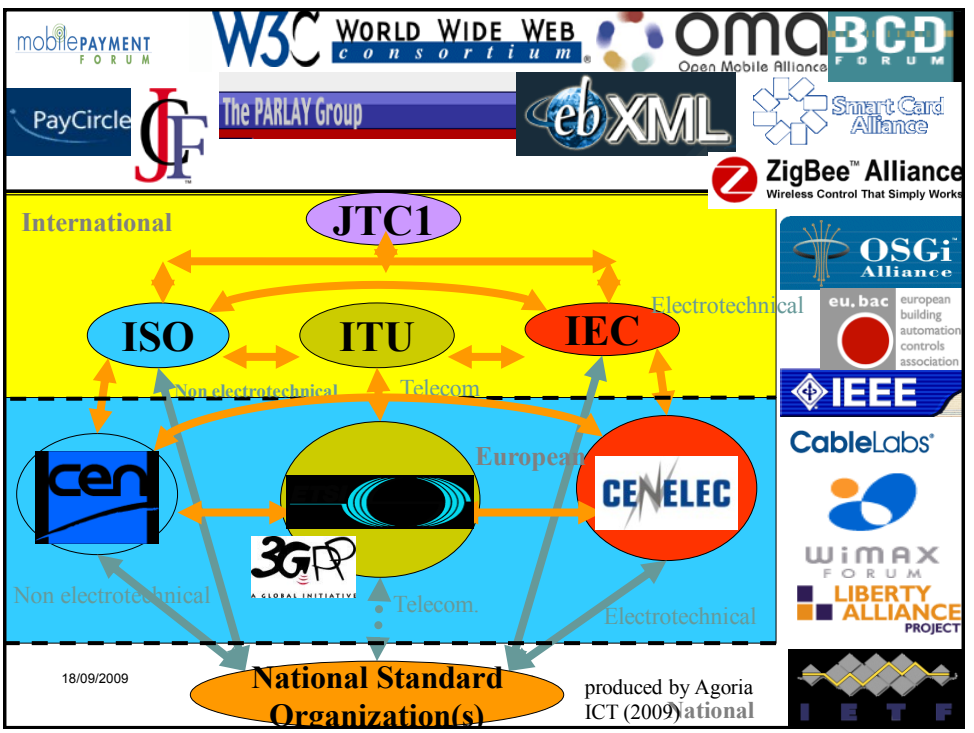
- Inventory
  - Source ENISA
    - www.enisa.europa.eu
  - Source ISO,CEN,ETSI,…
    - www.iso.org
    - www.ictstandards.be
  - Internet
  - Evaluation of each item
    - Target,scope,relevance
  - Personal knowledge
  - Contacts,
  - networking

- Original starting point
  - Personal work done in the context of ENISA Independent expert working groups during 3 years
  - Visible on the ENISA RA/RM website http://www.enisa.europa.eu/rmra/h_home.html

The different actors in the norm sector

World level | Regional level | Country level


produced by Agoria ICT(2009)
Standardization organizations
BI IB SI
Information Security
International
Europe
Country/Belgium
Trade barrier
ISO
CEN
NBN
Other areas
IEC
CENELEC
CEB
Electrotechnical
ITU
ETSI
NBN
Tele-communication
Life time Interoperability
Legislation
7


mobilePAYMENT FORUM
W3C WORLD WIDE WEB consortium
oma Open Mobile Alliance
BCD FORUM
PayCircle
JCF
The PARLAY Group
ebXML
Smart Card Alliance
ZigBee™ Alliance
Wireless Control That Simply Works
International
JTC1
ISO
ITU
IEC
Electrotechnical
Non electrotechnical
Telecom
OSGi Alliance
eu.bac european building automation controls association
IEEE
CableLabs
WiMAX FORUM
LIBERTY ALLIANCE PROJECT
IETF
European
CEN
CENELEC
3GPP
A GLOBAL INITIATIVE
Non electrotechnical
Telecom.
Electrotechnical
18/09/2009
National Standard Organization(s)
produced by Agoria ICT (2009)
National

Non exhaustive list of potential IT Security related norms (under investigation)

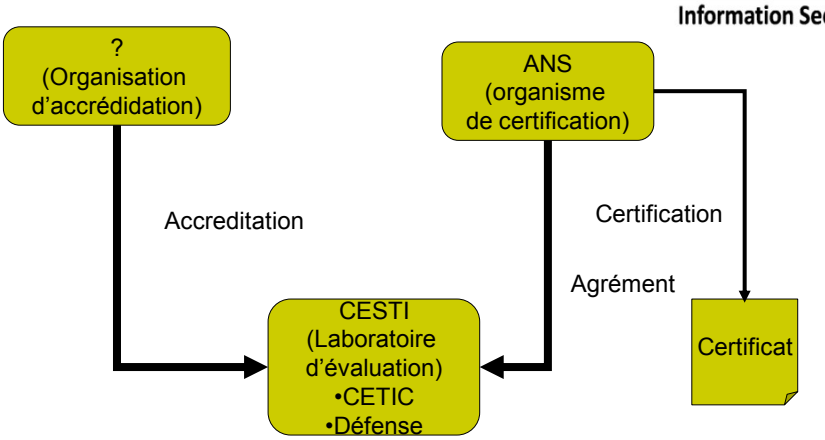
Only ISO level

JTC 1/SC 17 : cards and personal identification
JTC 1/SC 27 : IT Security Techniques
JTC 1/SC 31 : Automatic identification and data capture techniques
JTC 1/SC 37 : biometrics
TC 8 : Ships and marine technology
TC 20 : Aircraft and space vehicles
TC 21 : Equipment for fire productin and fire fighting
TC 22 : Roasd vehicles
TC 28 : Petroleum products and lubricants
TC 34 : Food products
TC 58 : Gas cylinders
TC 67 : Materials ,equipment and offshore strcutures for petroleum ,petrochemical and natural gas industries
TC 68/SC 2 : Security management and general banking operations
TC 68/SC 6 : retail financial services
TC 76 : Transfusion , infusion and injection equipment for medical and pharmaceutical use
TC 85 : Nuclear enery
TC 92 : Fire safety
TC 94 : Personal safety – protective clothing and equipment
TC 98 : Bases for design of strucures
TC 104 : Freight containers
TC 122 : Packaging
TC 145 : Graphical symbols
TC 146 : Air quality
TC 147 : Water quality
TC 154 : Processes, data elements and documents in commerce ,industry and administration
TC 159 : Ergonomics
TC 162 : Doors and windows
TC 184 : Industrial automation systems and integration
TC 190 : Soil quality
TC 192 : Gas turbines
TC 197 : Hydrogen technologies
TC 204 : Intelligent transport systems
TC 211 : Geographic information/Geomantic
TC 212 : Clinical laboratory tesing and in vitro diagnostic test systems
TC 215 : Health informatics
TC 220 : Cryogenic vessels
TC 223 : Civil defence
TC 224 : Services activities relating to drinking water supply systems and wastewater systems – Quality criteria of the service and performance indicators

BISI objective: 2 > certification scheme

- Inventory of needs
  - Advantages
  - Problems
  - Persons
  - Systems
  - Products
  - Entities
- Priority on C. C.
  - First « dry run » succeeded some weeks ago
  - Close collaboration with Cetic and some administration departements (Belac / ANS)
  - Look for next steps in order to finalize a Belgian independence in critical domains

Belgian scheme (in construction)



produced by Cetic (2009)

First step – Dry run

- This draft schema has been played :
  - ETCA (Product of Thales)
  - ANS – Certification authority
  - Cooperation « Defence » - CETIC - CESTI
  - *approval certificate* but not certification
- Business Case
  - Security Target written by Thales evaluated by CETIC and Defence
  - ANS has awarded a certificate of approval
- Not certification → Thus not official at international level

- Next steps in the hands of government (international recognition
- Update on the situation during the next BISI meeting on 30th of September by Bruno Vermeiren from NVO/ANS

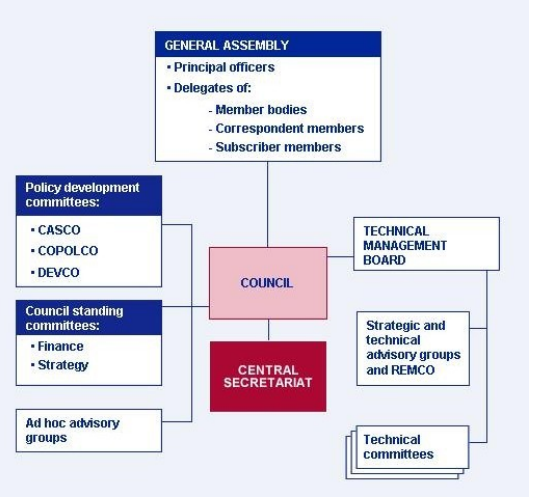
produced by Cetic (2009)

BISI objective: 3 > international support and representation

- Look for needs
  - Priority
  - Resources
  - Points of interest
- ISO ←-
- NIST
- BSI
- CEN ←-
- ITU ←-
- ….
- ←- For collaborating in some committee don't hesitate to contact me or Agoria ICT

- Quite large a scope
  - Step by step approach
  - Support and publicity
  - Control of what is currently done individually
- Role of national institutions (e.g. NBN)
  - Next context with new law
  - Agoria ICT as sector operator plays an active role in this domain helping actually at logistical level

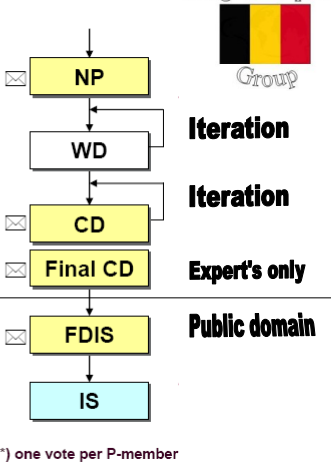
Actual Structure of the ISO



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

ISO/IEC JTC 1/SC 27
IT Security techniques
Chair: Mr. W. Fumy
Vice-Chair: Ms. M. De Soete

SC 27 Secretariat
DIN
Ms. K. Passia

Working Group 1	Working Group 2	Working Group 3	Working Group 4	Working Group 5
Information security management systems	***Cryptography and security mechanisms***	***Security evaluation criteria***	***Security controls and services***	**Identity management and privacy technologies**
Convener	*Convener*	*Convener*	*Convener*	*Convener*
Mr. T. Humphreys	*Mr. K. Naemura*	*Mr. M. Ohlin*	*Mr. M.-C. Kang*	*Mr. K. Rannenberg*

27000-27019 — 27000 series — 27030-27049

WG 1 Roadmap Framework

ISO/IEC JTC1/SC27 Belgian Expert's Group

ISO/IEC 27001
ISMS requirements

ISO/IEC 27001
Supporting
Guidelines

(27002-27005)

ISO/IEC 27001
Accreditation
Requirements and
Auditing Guidelines

(27006-27009)

ISO/IEC 27001
Sector Specific
Requirements and
Guidelines

(27010-27019)

WG1 – 27001 - 27002 - revision

ISO/IEC JTC1/SC27 Belgian Expert's Group

ISO/IEC JTC 1/SC 27 N7827
ISO/IEC JTC 1/SC 27/WG 1 N17827

REPLACES: --

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

DOC TYPE:	national body contribution
TITLE:	**Canadian NB contribution on suggested restructuring of ISO/IEC 27002 text as contained in SC 27 N7804**
SOURCE:	SCC, National Body of Canada
DATE :	2009-07-15
PROJECT:	27002 (revision)
STATUS:	In accordance with resolution 8 (see SC27 N7800) of the 38th SC 27/WG 1 Plenary meeting held in Beijing (China), 04th - 08th May 2009, this document is being circulated for **STUDY AND COMMENT**. National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the above-mentioned Working Draft by **2009-10-02.**
PLEASE NOTE:	For comments please use the SC 27 TEMPLATE separately attached to this document.
ACTION:	**COM**
DUE DATE:	**2009-10-02**
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice Chair E. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	1+ 120 + 6 (Attachment 1)

- 27001 and 27002 are under revision
- New WD for 27001
- 2 different WD for 27002 (based on old one and a Canadian proposition)
- Specific Belgian Task Force created to provide contributions and comments

WG 2 Roadmap Framework

ISO/IEC JTC1/SC27 Belgian Expert's Group

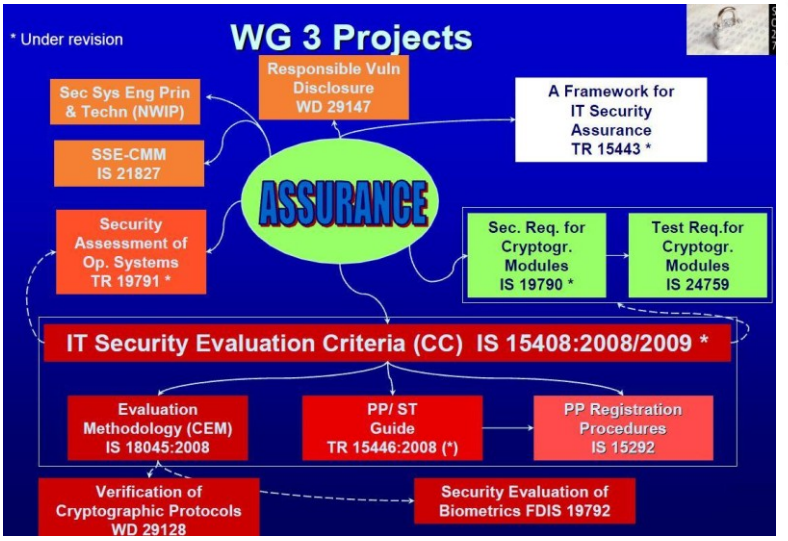
Goals, Techniques, Mechanism and Algorithms

Availability	18033 Encryption algorithms	10116 Modes of operation
Confidentiality	19772 Authenticated encryption	18031 Random bit generation
Integrity	29150 Signcryption	18032 Prime number generation
Authenticity	9798 Entity authentication	15946 Elliptic curves
Data integrity	9796 Dig. sign. message recvry	11770 Key management
13777 Non-repudiation	14888 Dig. sign. with appendix	10118 Hash-functions
18014 Time stamping	9797 Message authen. codes	7064 Check character systems

produced by K. Naemura 2008

WG 3 Roadmap Framework

ISO/IEC JTC1/SC27 Belgian Expert's Group



produced by M. Ohlin 2008

WG 4 Roadmap Framework

Unknown and emerging security issues

Known security issues

Security breaches and compromises

produced by MengChow Kang 2008

WG 4 Projects & Study Periods

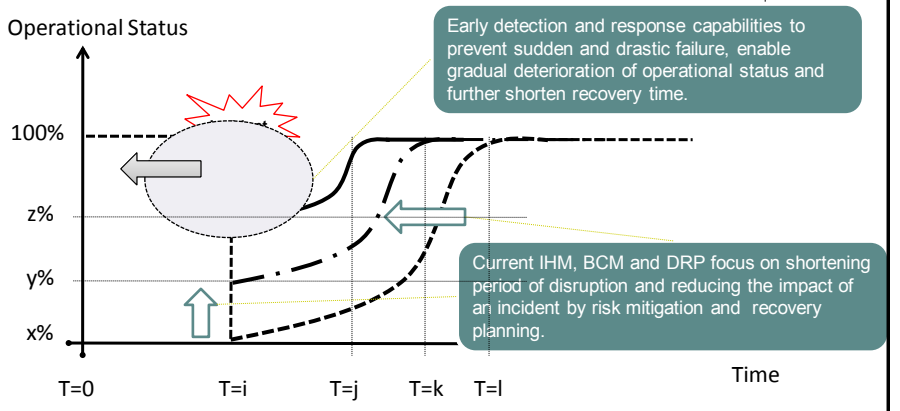
Unknown and emerging security issues

Known security issues

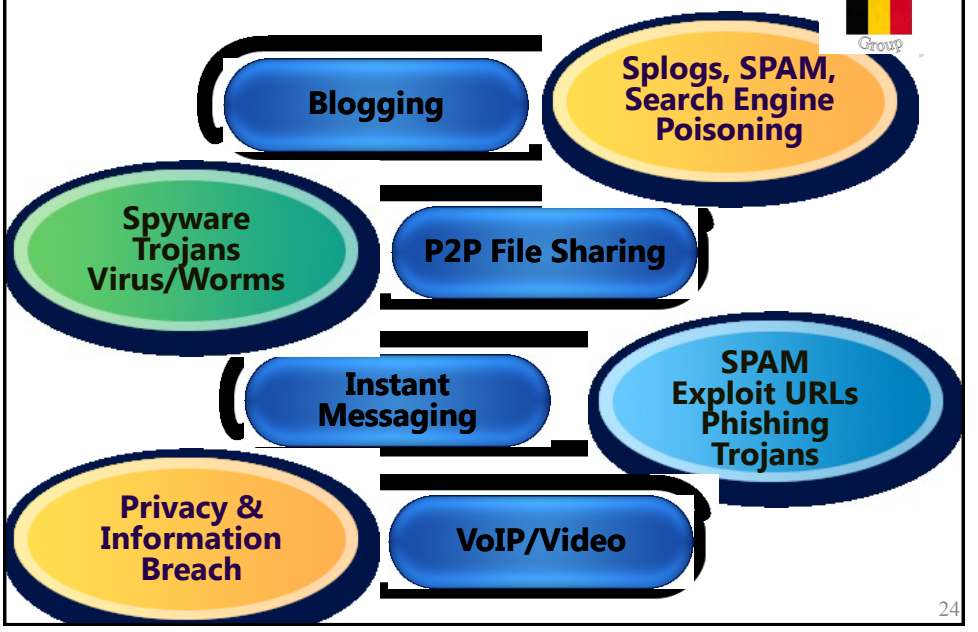
Security breaches and compromises

produced by MengChow Kang 2008

ICT Readiness for Business Continuity (27031)



Web 2.0 Cybersecurity Issues



Guidelines for Cybersecurity(27032)

- "Best practice" guidance in achieving and maintaining security in the cyber environment
  - an overview of Cybersecurity;
  - an explanation of the relationship between Cybersecurity and other types of information security;
  - a definition of stakeholders and a description of their roles in Cybersecurity;
  - guidance for addressing common Cybersecurity issues; and
  - a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

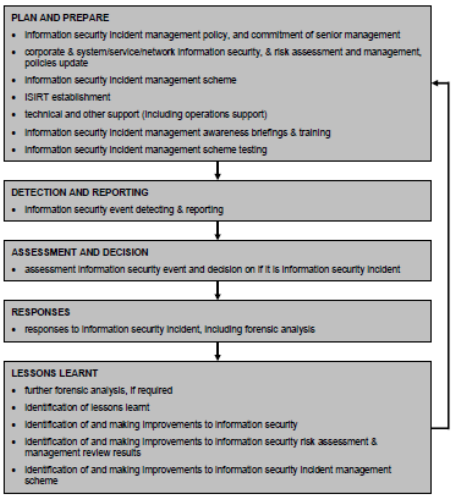
Network Security (27033)

- Revision of ISO/IEC 18028
- Re-focus, re-scoping, and new parts
  - Part 1 – Guidelines (Overview, Concepts, Principles)
  - Part 2 – Guidelines for Design and Implementation
  - Part 3 – Reference Networking Scenarios: Risks, Design, Techniques, and Control Issues
  - Part 4 – Security communications between networks using security gateways
  - Part 5 – Security communications between networks using Virtual private network
  - Part 6 – IP Convergence (project)
  - Part 7 – Wireless (project)

Guidelines for Application Security (27034)

- Reduce security problems at the application layers
- Eliminate common weaknesses at code and process levels
- Strengthen security of code base improve application security and reliability
- Multi-parts standards, including
  - Code Security Certification
  - Process Security Certification
- Code Security
  - Testing and certification per major release of application
- Process Security
  - Security Development Lifecycle
  - Assure security of code from design to operation, including minor releases, patch development & release
- Focus on Web-based applications (major problem areas)

Incident management (27035)

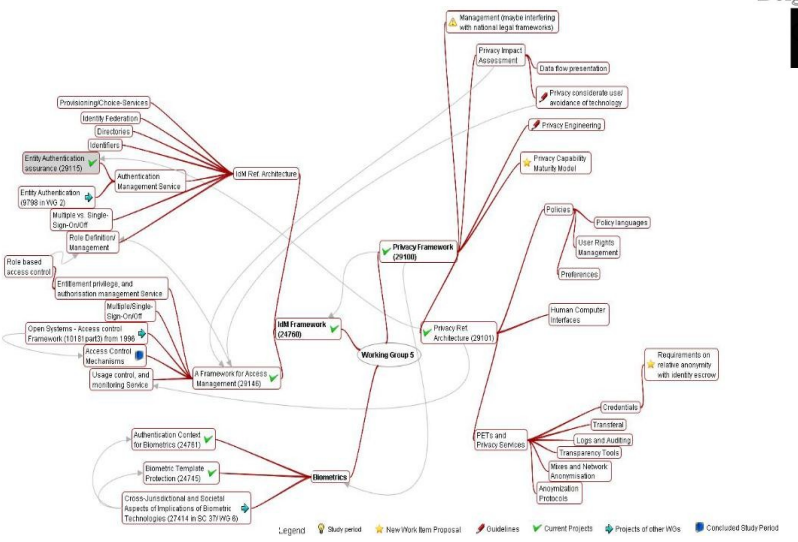


- Revision of ISO TR 18044 with new development
- Almost 85 pages
- Now IS instead of TR
- Actually 2nd CD
- Publication within one year normally

Other new WG4 projects

- Security of outsourcing (27036)
- Guidelines for digital evidence (27037)
- Best practices on the provision of time-stamping services (29149)
- Intrusion Detection (18043) – revision started
- …
- Also internal documents
  - Roadmap
  - Rules for definitions

WG 5 Roadmap Framework



produced by Kai Rannenberg 2008

Coming events

- 30/09/2009 09:30 a.m. BISI meeting with presentation of Br. Vermeiren from ANS on the actual status of C.C. Belgian scheme (among others) and status of objectives
- 30/09/2009 02:00 p.m. ISO SC27 Belgian expert's finalization meeting .Votes positions and validation of comments for the Redmond meeting in November
- Meeting are held at "Diamant Conference Center" (Agoria ICT building)
- Take a look at www.ictstandards.be for more details

Q & A

For further information

E-mail :
alain.degreve@skynet.be