

ISO standards relevant to CSIRTs

(update on ISO/IEC 27053 and TF-CSIRT liaison)

Pascal Steichen – CIRCL

Member of LU-SC27 committee (CNLSI)

pascal.steichen@circl.etat.lu

- (1) “*ISO/IEC JTC1 SC27*” at a glance
- (2) Relevant standards for the CSIRT community
(WG4 roadmap)
- (3) ISO/IEC 27035
(update)
- (4) WG4 & WG3 resolutions (Limassol, Cyprus, 10/2008)
(other CSIRT relevant standards)
- (5) Action items
- (6) Q&A

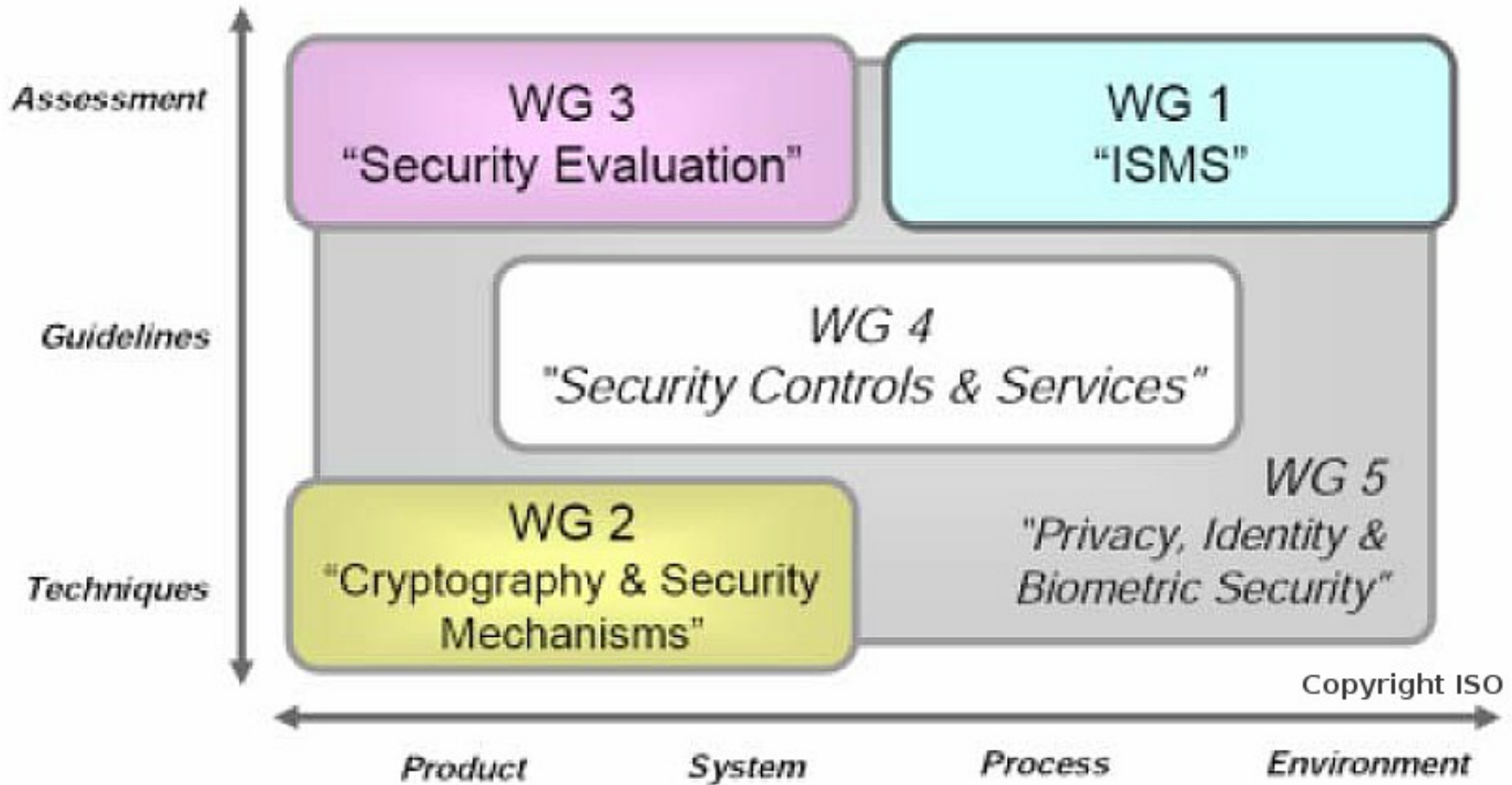


ISO/IEC JTC1 SC27 - IT Security techniques (1)

- Chair: Dr. Walter Fumy (Germany)
- published standards: 76
- Members: 38 (P) , 14 (O)
- Liaisons:
 - ISO TC 68/SC 2, TC 68/SC 7, TC 215, ...
 - ... Ecma, ITU, MasterCard, Visa, **(FIRST)** ...
- Meetings: every 6 months



ISO/IEC JTC1 SC27 - IT Security techniques (2)





- Priorities for Working Group 4:

*consolidate progress on the transfer of projects from WG1 on **supporting ISMS** services and mechanisms. For example, the maintenance and updating of the multipart standard on Network Security (project 1.27.28), and the TTP services standards as well as the successful completion of the Disaster recovery services standard. In addition, WG 4 has initiated work on **new projects** such as **cybersecurity**, application security, ICT readiness for business continuity, security of outsourcing, and **guidance for the identification, collection and/or acquisition, and preservation of digital evidence...***



Relevant standards for the CSIRT community

- Selection, deployment and operation of Intrusion Detection Systems (IDS)
 - ISO/IEC 18043 published since 06/2006
- NP 27035: Information security incident management
 - revision of ISO/IEC TR18044
- Guidelines for identification, collection, and/or acquisition and preservation of digital evidence
 - New work item
- Categorization and classification of information security incident
 - Study period
- Evidence acquisition procedure for digital forensics
 - Study period
- NP 29147: Responsible vulnerability disclosure
 - liaison with FIRST

- SoV (NWIP → WD) (30/38)

Limassol, Cyprus, 10/2008

- "Do you accept the proposal in the attached NWI Proposal document as a sufficient definition of the new work item?"
(23Y ; 7A)
- "Do you support the addition of the new work item to the programme of work of the joint technical committee?"
(22Y ; 8A)
- "Do you commit yourself to participate in the development of this new work item?"
(8Y [AU, CH, JP, KR, MA, ZA, UK, US] ; 13A ; 9N)

- SoV (cont'd)

Limassol, Cyprus, 10/2008

- "Are you able to offer a project editor who will dedicate his/her efforts to the advancement and maintenance of this project?"
(1Y [JP - Yoshihiro Satoh, HP] ; 10A ; 19N)
- "Do you have a major contribution or a reference document ready for submittal?"
(1Y [JP] ; 9A ; 20N)
- "Will you have such a contribution in ninety days?"
(1Y [JP] ; 10A ; 19N)
- "Which standard development track is proposed?"
(24Def; 3Acc ; 3Ext)

- Status: 1st WD (N6750) → 1st CD in Beijing 2009
(*revision*)
- Comments from Germany (3), Japan (20), Luxembourg (20), UK (62, late), USA (38)
- Waiting since 22nd December 2008 on:
 - Disposition of comments on ISO/IEC 1 WD 27035 (N6915)
 - Revised Text of 1st WD ISO/IEC 27035 (N7177)
- Co-editorship:
 - Yoshihiro Satoh
 - Jing-Hua Min



WG4 resolutions Limassol, Cyprus, 10/2008 (1)

- NWIP “Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence”
 - → NWI (SC 27 N7183 ; co-editorship: Maslina Daud and Kyung-Seok Lee)
- SP “Categorization and Classification of Information Security Incidents”
 - be absorbed into relevant sections in ISO/IEC 27035 as part of its development
- NWIP “Evidence Acquisition Procedure for Digital Forensics”
 - → NWI (SC 27 N6432)
- Nothing about liaison with TF-CSIRT



WG3 resolutions Limassol, Cyprus, 10/2008 (2)

- ISO/IEC 29147 “Responsible vulnerability disclosure”
 - *Strangely in WG3 – Security evaluation*
- Status: 1st WD (N6646)
- Established liaisons:
 - CCDB (Common Criteria Development Board)
 - FIRST (in the room?)



Action items or why to liaise with SC27 ?

- Activate (talk to) local/national ISO experts/organisation
 - to get involved
 - to give them feedback
 - help/watch to create “good” standards
 - start using them (the standards)
- *SC27 – TF-CSIRT* liaison for **all** relevant standards why?
 - “official” security standards come from ISO (SC27)
 - many new proposals related to CSIRT work
 - needs follow up from “inside”
 - full (or WG) liaison not so good
 - → ISO wants feedback for every standard then
 - we don't wanna miss this train, do we ?
- Any “experts” out there to participate in this



- **Questions ?**

Thank you for your attention

Pascal Steichen

CIRCL - www.circl.lu

Member of LU-SC27 committee (CNLSI)

pascal.steichen@circl.etat.lu



- SC27 at a glance:
http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=45306
- SC27 business plan:
<http://isotc.iso.org/livelink/livelink/7655125/JTC001-N-9327.pdf?func=doc.Fetch&nodeid=7655125>