

# ISO/IEC JTC 1 SC 27

## IT Security Techniques

WG 3 -  
Security Evaluation, Testing  
and Specification

# SC27 Mission

SC 27 develops standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;

# SC27 Mission (II)

- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;

# SC27 Mission (III)

- Conformance assessment, accreditation and auditing requirements in the area of information security;
- *Security evaluation criteria and methodology.*

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure proper development and application of SC 27 standards and technical reports in relevant areas.

# Local vs. international

- Underling concepts are international, how you interpret/implement them is a local issue.



# Reinvent vs. Reuse





# WG3 Mission

## Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

- a) security evaluation criteria;
- b) methodology for application of the criteria;
- c) security functional and assurance specification of IT systems, components and products;
- d) testing methodology for determination of security functional and assurance conformance;
- e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

# Security Evaluation, Testing and Specification

So we have experience in developing assurance methods that are world-wide applied, and we're in the process of improving them (current revision of ISO/IEC 15408).

However, we do not have local interpretations of security requirements for products and services to comply with specific needs, legislative frameworks or customer/citizen needs, that normally are expressed in the form of *Protection Profiles*.



More information at

<http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**Thanks!**

Miguel Bañón

Epoche & Espri, a DEKRA company

mbp@epoche.es