

- Meeting May 3 – 12, 2007 in Moskau/St. Petersburg
- Study Period/Call for Contributions (Feb.- April 2007) for
  - Sector Specific ISMS Standards for the Automotive Industry
  - Two Contributions from Sweden and the US
- Resolution 3:
  - ...WG 1 agrees to adopt a set of principles for the inclusion of sector-specific ISMS standards in the 27 000 family of standards ...
- Resolution 18;
  - Extension of the Study period for Sector Specific ISMS Standards for the Automotive Industry (till Sept. 14, 2007)
- SC 27 WG 1 expects a request from the eSafety Steering Group for liaison (Automotive Industry specific ISMS standards)

### WG 1 "Information Security Management Systems"

- WG1 covers the development of ISMS (Information Security Management System) standards and guidelines. This includes:
  - Development and maintenance of the ISO/IEC 27000 ISMS standards family
  - Identification of requirements for future ISMS standards and guidelines

### WG 2 "Cryptography and Security Mechanisms"

### WG 3 "Security Evaluation Criteria"

- Standards for IT security evaluation and certification of IT systems, components, and products. This will include consideration of computer networks, distributed systems, associated application services, biometrics, etc.;
- Three aspects may be distinguished:
  - evaluation criteria;
  - methodology for application of the criteria;
  - administrative procedures for evaluation, certification, and accreditation schemes;
- This work will reflect the needs of relevant sectors in society, as represented through ISO/IEC National Bodies and other organisations in liaison, expressed in standards for security functionality and assurance;
- Account will be taken of related ISO/IEC and ISO standards for quality management and testing so as not to duplicate these efforts.

#### WG 4 "Security controls and services"

- The development and maintenance of standards and guidelines addressing services and applications supporting the implementation of control objectives and controls as defined in ISO/IEC 27001. This includes, but is not limited to
  - IT Network security
  - Information security incident management and disaster recovery
  - Trusted Third Party services
  - Security information objects for access control
  - Identification of requirements for and development of future service and applications
- Standards and guidelines, for example in the areas of
  - Business Continuity
  - Cyber Security
  - Outsourcing

#### WG 5 "Identity management and privacy technologies"

- The development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and privacy.
- Identification of requirements for and development of future standards and guidelines in these areas.

- Following documents have to be checked for applicability in the automotive sector (ISO ...)
  - 13335 Management of information and communications technology security (WG 1)
  - 27000 Information security management system fundamentals and vocabulary (WG 1)
  - 27001 Information security management systems – Requirements (WG 1)
  - 27002 Code of practice for information security management (WG 1), formerly 17799
  - 27003 Information security management systems – Implementation Guidelines (WG 1)
  - 27004 Information security management measurements (WG 1)
  - 27005 Information security risk management (WG 1)
  
  - 15408-1,-2,-3 Evaluation criteria for IT-Security (WG 3)
  - 15443-1,-2,-3 A Framework for IT Security assurance (WG 3)
  - 18045 Methodology for IT security evaluation (WG 3)
  - 19791 Security assessment of operational systems (WG 3)
  - 21827 Systems Security Engineering – Capability Maturity Model) (WG 3)
  
  - 18028-1,-2,-3, -4, -5 IT Network Security (WG 4)
  - 18044 Information security incident management (WG 4)
  
  - New Proposals:
    - A Privacy framework (WG 5)
    - A Privacy reference architecture (WG 5)
- Other interesting documents
  - WELMEC Software Guide (Directive 2004/22/EC)