Development of Security and Privacy Standards at ISO

DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative

Standards Relating to Application Security at ISO

- 26 Sub-Committees / Working Groups – SC7 (Software & System Engineering), SC27 (IT Security Techniques), Smart Grid, Internet of Things, Governance of IT, Biometrics, others
- SC27 – 123 standards published
  - **WG1 – Information security management systems**
  - **WG2 - Cryptography and security mechanisms**
  - **WG3 - Security evaluation, testing and specification**
  - **WG4 - Security controls and services**
  - **WG5 - Identity management and privacy technologies**
  - How can I participate? Indian Mirror Committee – BIS - LITD 17 ;

    DSCI Coordinating Indian Participation

Member Countries

JTC1 SC 27 has

51 participating countries

(P-members)

and

20 Observing countries

(O-members)

Participating countries

Algeria (IANOR)	Ireland (NSAI)	Romania (ASRO)
Argentina (IRAM)	Israel (SII)	Russian Federation (GOST R)
Australia (SA)	Italy (UNI)	Rwanda (RSB)
Austria (ASI)	Jamaica (BSJ)	Singapore (SPRING SG)
Belgium (NBN)	Japan (JISC)	Slovakia (SOSMT)
Brazil (ABNT)	Kazakhstan (KAZMEMST)	South Africa (SABS)
Canada (SCC)	Kenya (KEBS)	Spain (AENOR)
Chile (INN)	Korea, Republic of (KATS)	Sri Lanka (SLSI)
China (SAC)	Luxembourg (ILNAS)	Sweden (SIS)
Cyprus (CYS)	Malaysia (DSM)	Switzerland (SNV)
Czech Republic (UNMZ)	Mauritius (MSB)	Thailand (TISI)
Côte d'Ivoire (CODINORM)	Mexico (DGN)	The Former Yugoslav Republic of Macedonia (ISRM)
Denmark (DS)	Netherlands (NEN)	Ukraine (DTR)
Finland (SFS)	New Zealand (SNZ)	United Arab Emirates (ESMA)
France (AFNOR)	Norway (SN)	United Kingdom (BSI)
Germany (DIN)	Peru (INACAL)	United States (ANSI)
India (BIS)	Poland (PKN)	Uruguay (UNIT)

The work is open to technical experts nominated by Member bodies

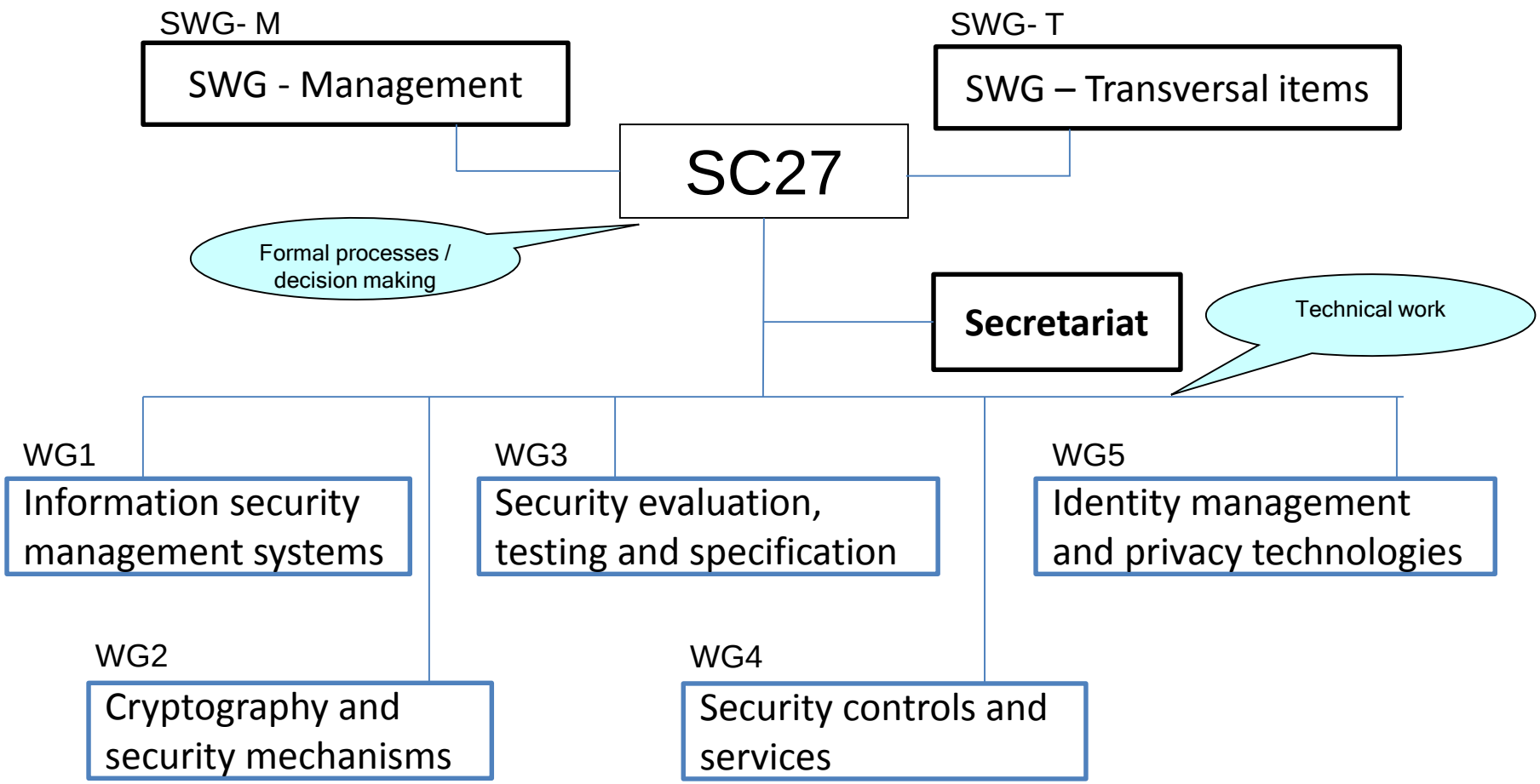
source:
www.iso.org

Observing countries

Belarus (BELST)	Iran, Islamic Republic of (ISIRI)
Bosnia and Herzegovina (BAS)	Lithuania (LST)
Costa Rica (INTECO)	Morocco (IMANOR)
El Salvador (OSN)	Palestine, State of (PSI) (Correspondent member)
Estonia (EVS)	Portugal (IPQ)
Ghana (GSA)	Saudi Arabia (SASO)
Hong Kong (ITCHKSAR) (Correspondent member)	Serbia (ISS)
Hungary (MSZT)	Slovenia (SIST)
Iceland (IST)	Swaziland (SWASA) (Correspondent member)
Indonesia (BSN)	Turkey (TSE)

source:
www.iso.org

JTC1 SC27 structure



WGs prepare the content of the standards, process comments received from around the world, and ultimately finalize the work for submission as a draft international standard

India is a Participating Member in SC27

P-members (participating members) are ISO member bodies which wish to play an active role in the work of a technical committee or subcommittee.
This also involves participation in the **annual plenary and interim** meetings

Apart from a duty to play an active role in the work of their committee, they also have an obligation to vote in all official ballots related to the work of the committee.

They have a duty to identify experts who may be able to contribute to the related working group activities.

They will work on the preparation of International Standards and provide a feed-back route to their national organizations.

Working groups and experts

- A working group comprises of experts individually appointed by the P-members to deal with the specific task allocated to the working group

- The experts act in a personal capacity and keep close contact with that P-member to inform them about the progress of the work and of the various opinions in the working group at the earliest possible stage

source: JTC1 directives

Delegates

Delegates to the ISO technical committees and subcommittees (e.g. ISO/IEC JTC1 SC27) have the task of ensuring that the views and positions of the particular national member body which they represent are known and understood by the committee.

Delegates participate in negotiation and consultation intended to lead to the development of a consensus international opinion that considers the view of the delegate's country position in the outcome.

source: JTC1 directives

Head of delegation

A head of delegation is the official spokesperson for a delegation.

A head of delegation is expected to ensure that his/her delegate present a homogeneous view during meetings or, if there are conflicting views within the delegation, will determine which view is to be presented to the meeting.

They should ensure that members of their delegation represent the position of their country's member body.

Heads of delegation will often be assigned the responsibility of reporting on the outcome of meetings to their respective member body or assigned organization.

source: JTC1 directives

Standard Development Process

1. Proposal Stage (NWIP)
2. Preparatory Stage (WD)
3. Committee Stage (CD)
4. Enquiry Stage (DIS)
5. Approval Stage (FDIS)
6. Publication Stage (IS)

- Comments and Voting at each stage
- Review of International Standards (Confirmation, Revision, Withdrawal)
- Fast-track procedure

WG highlights

- WG1
  - Smart Grid Security and Certification of Security Personal (in keeping with accreditation standard ISO 17024).
  - Competence requirements for information security management Professionals (ISO 27021)
- WG2
  - ISO/IEC 11770-6: Key management – Par t 6: Key derivation
  - ISO/IEC 20009-4: Anonymous entity authentication– Part 4: Mechanisms based on weak secrets
  - ISO/IEC 29192-5: Lightw eight cryptography – Part 5: Hash-functions
  - cooperation with TC 68 on Banking and Related Financial Services
- WG3
  - secure technology, products, systems and services, and their security evaluation and testing
  - cryptographic module security testing, and cryptography implementation conformance testing
  - security problems of supply chain and product specific protection profiles

WG highlights

- WG4
  - Security incidents
    - eDiscovery (ISO/IEC 27050).
    - guidelines for security information and event management (ISO/IEC 27044, WD)
    - information security incident management (ISO/IEC 27035, CD)
  - System and system life cycle security
    - IDPS (ISO/IEC 27039) and storage security (ISO/IEC 27040)
    - application security (ISO/IEC 27034)
    - network security (ISO/IEC 27033)
    - revision of ISO/IEC TR 14516 has been started to focus on the use and management of Trust Service Providers, especially PKI
    - Cloud computing – Service Level Agreement (SLA) framework – Part 4: Security and privacy (ISO/IEC 19086WD)
- WG5
  - ISO/IEC 24760 A framework for identity management)
  - ISO/IEC 29146 A framework for access management,
  - ISO/IEC 29190 Privacy capability assessment model
  - tele biometric authentication (ITU-T X.1085 (bhsm) | ISO/IEC 17922),
  - Privacy impact assessment (ISO/IEC 29134),
  - Identity proofing (ISO/IEC29003),
  - Code of practice for PII protection (ISO/IEC 29151)

New Projects

- ISO/IEC NP TR 14516: Guidelines for the use and management of trust service providers
  - Part 1: Overview and concepts
  - Part 2: Guidelines on information security of PKI trust service providers
  - Part 3: Guidelines on provision of services by PKI trust service providers
- ISO/IEC NP 19592: Secret sharing
  - Part 1: General
  - Part 2: Fundamental mechanisms
- ISO/IEC NP 19989 Competence requirements for information security testers and evaluators
- ISO/IEC NP 27021: Competence requirements for information security management systems professionals
- ISO/IEC NP 18033-6: Encryption algorithms -- Part 6: Homomorphic encryption
- ISO/IEC NP 27034-5-1: Application security -- Par t 5-1: Protocols and application security controls data structure -- XML schemes

Study Periods

- Cloud adapted risk management framework (joint WG 1 /WG 4)
- Information security library (joint WG 1 /WG 4)
- Justification study for revision of ISO/IEC 27010 (WG 1)
- Revision of ISO/IEC 11770-4 (WG 2)
- Suitability of the proposed anonymous entity authentication scheme NAPAKE for possible inclusion in ISO/IEC 20009-4 (WG2)
- Lightweight message authentication codes (WG 2)
- Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

(joint WG 2/WG 3)

- Privacy-respecting identity management scheme using attribute-based credentials (joint WG 2/WG 5)
- Cloud security components (WG 4)
- Cloud security assessment and audit (WG 4)
- Incident response, investigations and e-discovery concepts, terminology and models (WG 4)
- Security architecture framework (WG 4)

Some of the focus areas for Jaipur Event?!

- IOT
  - N15299 SG on security and privacy issues in IOT
- Cloud security
  - N110 SG on Cloud and new data-related technology risk management (CDRM)
  - N134 SG on Cloud security use cases and potential standardisation gaps
  - N090 SG on Code of practice for information security controls based on ISO 27002 for cloud service partners
- Competence
  - N 84 WD2 on Competence requirements for ISMS professionals ISO 27021 WD2
  - N1195 WD2 on IS testers and evaluators WG3N1195_2ndWD_19896-2_20150810
- Governance
  - ISO/IEC 27014 Governance of information security
    - guidance on concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security related activities within the organization
  - ISO/IEC 30121 Governance of digital forensic risk framework
    - for Governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. It applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure

Opportunity to respond now

- Competence – 27021
  - WD 2 (N116)
  - Information security management professionals
- Information Security Management guidelines based on ISO/IEC 27002 for process control systems specific to the energy and utility industry
  - WD1 (N82)
- Guidelines for auditors on information security controls 27008
  - WD2 (N80)
- Guidelines for Information Security management systems auditing 27007
  - WD2 (N78)
- Information security risk management 27005
  - WD4 (N76)
  - New data related risk management
    - Cloud Computing, Big Data, Internet of Things and other 'Data technology (N110 - CfC)
- Cloud security use cases and potential standardisation gaps
  - CfC closes on 5th October (N134)

** Not an exhaustive list

Thank You