ISO/IEC JTC1 SC27 WG4
“Security Controls & Services”

Use of X.509 within ISO/IEC JTC1 SC 27 / WG 4 “Security controls & services” Projects

ISO/IEC FDIS 27099 **Information Technology — Public key infrastructure — Practices and policy framework**

&

ISO/IEC DIS 27071 **Cybersecurity — Security recommendations for establishing trusted connections between devices and services**

Agenda

- Introduction
- ISO, IEC and JTC1 in a nutshell
- Focus on SC27 « Information security, cybersecurity and privacy protection »
- Focus on SC27 Working Group 4 « Security controls and services »
- Presentation of two WG4 standards using X.509
- Focus on ISO/IEC 27099 « Information Technology — Public key infrastructure — Practices and policy framework »
- Focus on ISO/IEC 27071 « Cybersecurity — Security recommendations for establishing trusted connections between devices and services »

François LOREK

https://www.linkedin.com/in/francoislorek
https://www.linkedin.com/company/trax-solutions

Founder of TRAX, Digital Compliance Agency | Associate director | ISO/IEC JTC1 SC27 WG4 Vice convenor

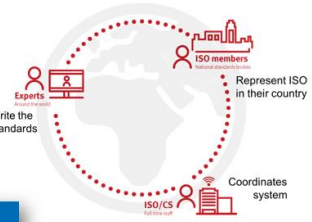
Seasoned expert in Cyber security and risk forecasting with emerging new technologies, relying on strong engineering backgrounds in IT & IT security. His professional career was dedicated to IT consulting activities, including ISO standards lead auditing expertise, whilst dispensing advice to match compliance, business stakes with operational efficiency.

He has been actively involved in standardization work for more than 12 years, at French, European and international level.

Indeed, he is since 2010 member of SC27 french mirror committee as well as 10+ other Afnor's standardization mirror committees. Since 2015, he is vice convenor of ISO/IEC JTC1 SC27 WG4 *"Security Controls & Services"* as well as vice convenor since 2021 for both ad hoc groups *"Internet of Things & Digital Twins"* and *"Artificial Intelligence & Big Data"*. At European level, he is actively involved in CEN-CENELEC JTC013 *"Cybersecurity and Dataprotection"* and CEN-CENELEC JTC021 *"Artificial Intelligence"* since their creation.

ISO/IEC JTC1 overview

International Standard Organization (ISO)



- ISO (International Standard Organization) is an independent, non-governmental international organization with a membership of 167 national standards bodies.

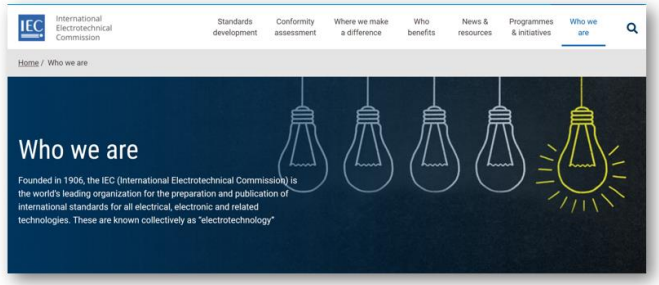
https://www.iso.org/

5

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

+

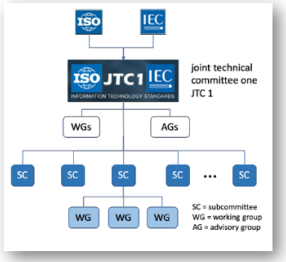
International Electrotechnical Commission



6

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

ISO/IEC Cooperation since JTC1 creation in 1987



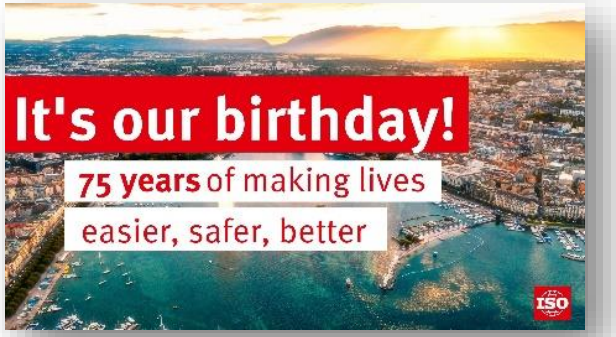
JTC 1 is the environment structured in 22 subcommittees where experts meet to :

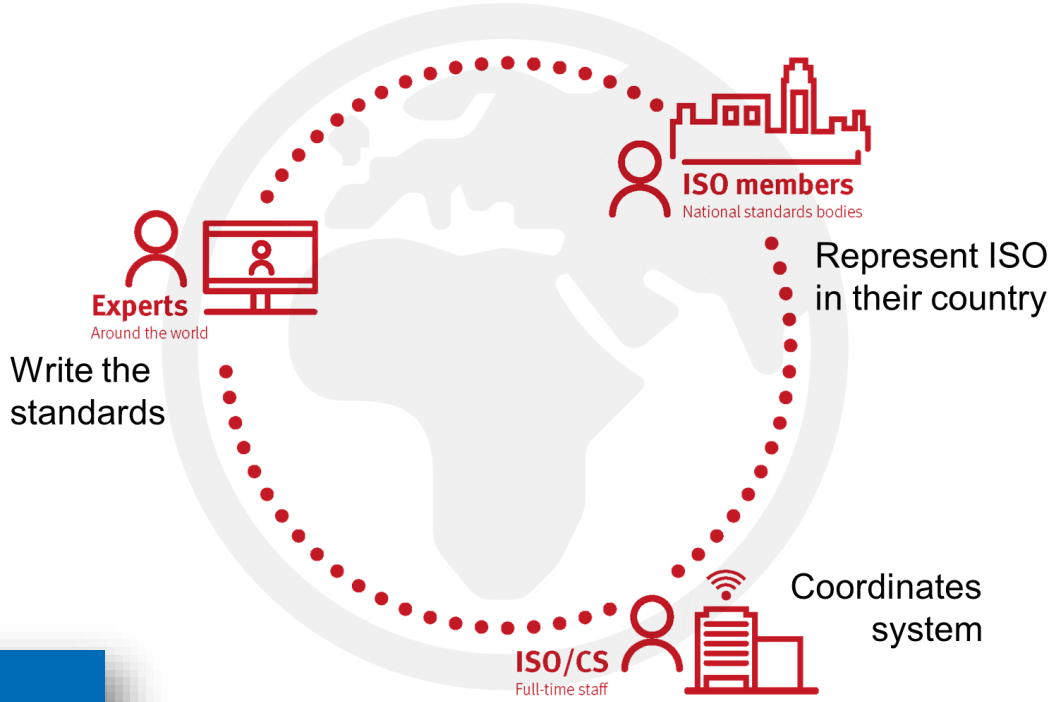
- develop global standards on all information and communication technologies (ICT)
- for both commercial and consumer applications.

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

International Standard Organization (ISO)





- ISO (International Standard Organization) is an independent, non-governmental international organization with a membership of 167 national standards bodies.

ISO TODAY

24265
International Standards covering almost all aspects of technology and manufacturing.

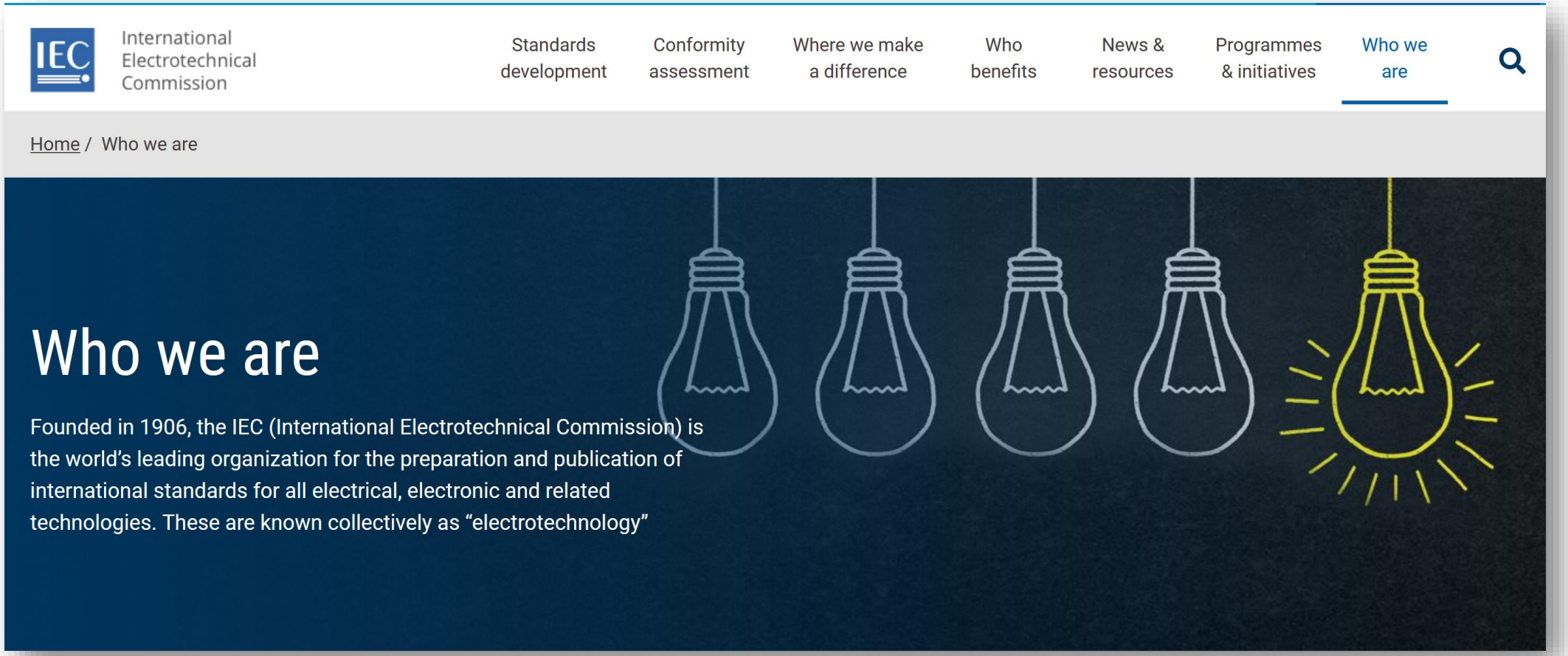
167
Members representing ISO in their country. There is only one member per country.

804
Technical committees and subcommittees to take care of standards development.

https://www.iso.org/

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

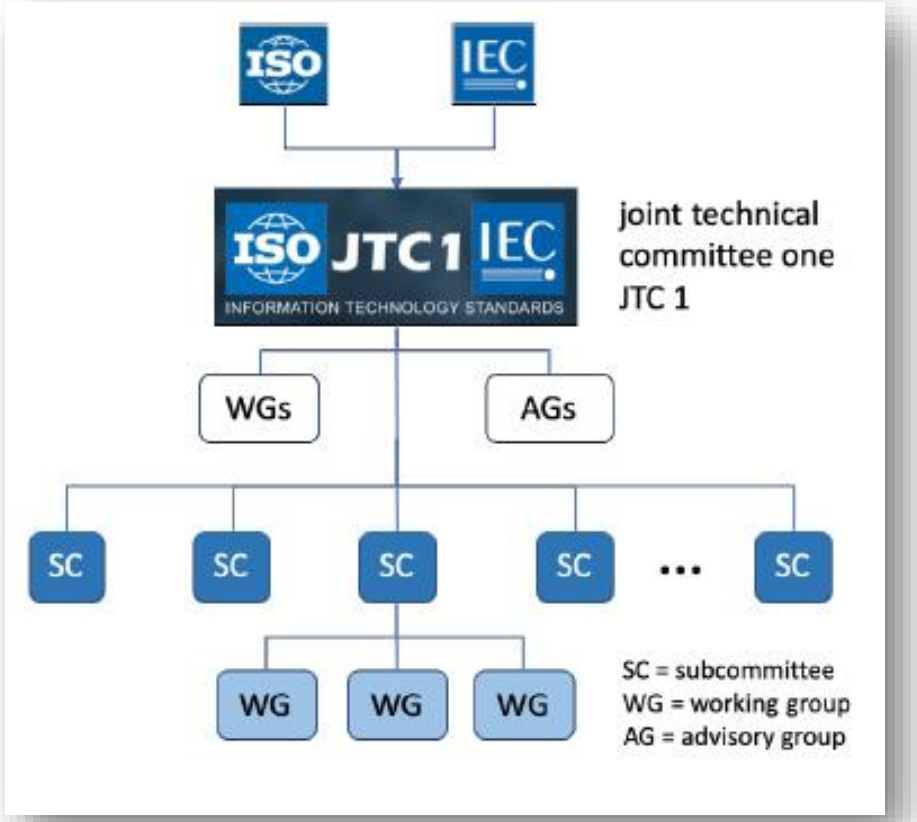
International Electrotechnical Commission



ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

ISO/IEC Cooperation since JTC1 creation in 1987

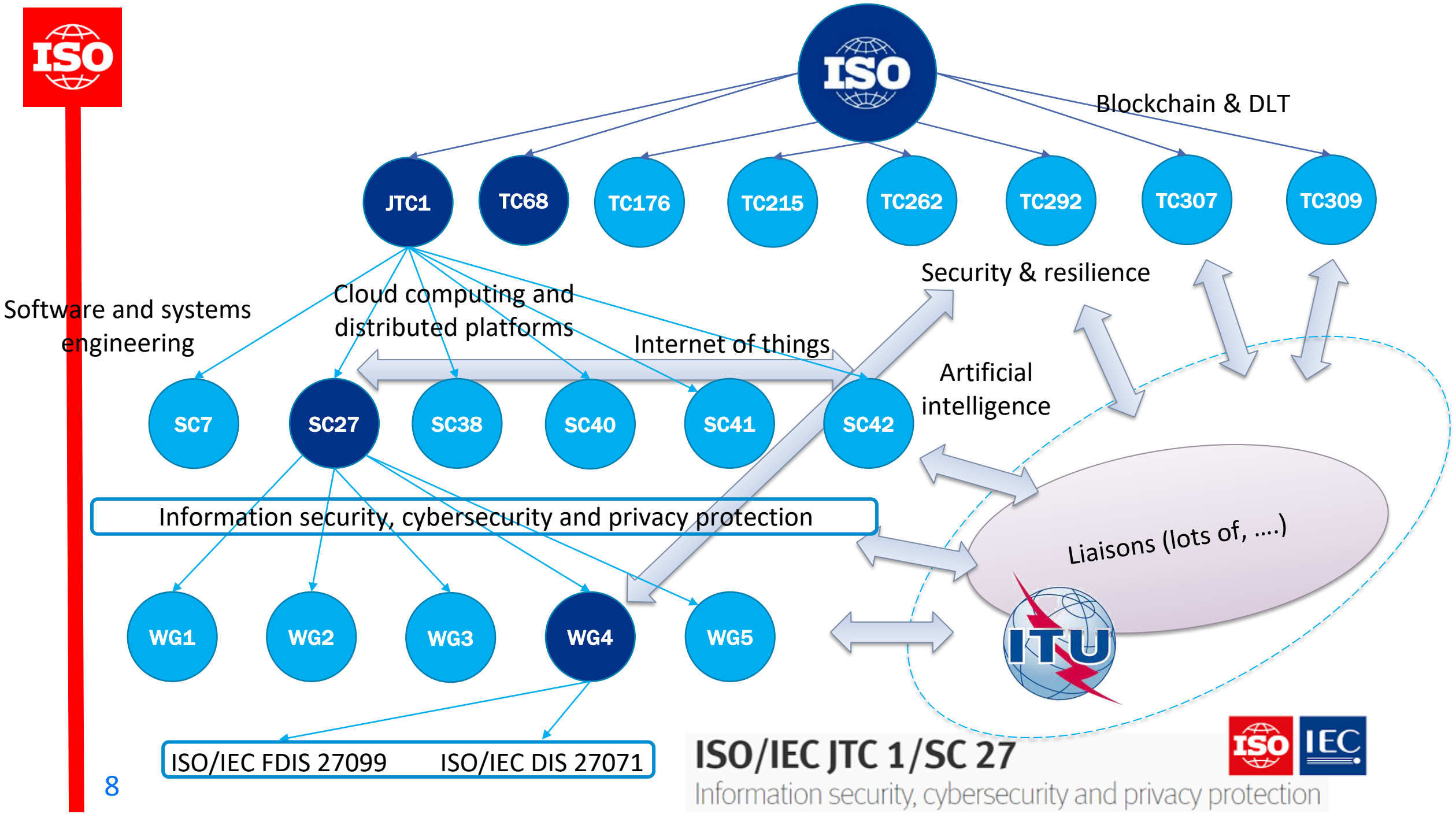


JTC 1 is the environment structured in 22 subcommittees where experts meet to :

- develop global standards on all information and communication technologies (ICT)
- for both commercial and consumer applications.

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection


ISO
Blockchain & DLT
JTC1
TC68
TC176
TC215
TC262
TC292
TC307
TC309
Security & resilience
Software and systems engineering
Cloud computing and distributed platforms
Internet of things
Artificial intelligence
SC7
SC27
SC38
SC40
SC41
SC42
Information security, cybersecurity and privacy protection
Liaisons (lots of, ….)
ITU
WG1
WG2
WG3
WG4
WG5
ISO/IEC FDIS 27099
ISO/IEC DIS 27071
ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection
ISO
IEC

ISO/IEC JTC 1

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

216	73	51	33
PUBLISHED ISO STANDARDS * under the direct responsibility of ISO/IEC JTC 1/SC 27	ISO STANDARDS UNDER DEVELOPMENT * under the direct responsibility of ISO/IEC JTC 1/SC 27	PARTICIPATING MEMBERS	OBSERVING MEMBERS

https://www.iso.org/committee/45306.html

SCOPE

The development of 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, security processes, and security controls and services;
- 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;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

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

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

Working Group 4 : Security controls & services

Aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems.

1. ICT SECURITY OPERATIONS

2. Information life cycle

3. Organizational processess

4. Security aspects of Trusted services

5. Cloud, internet and cyber security related technologies and architectures

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

ISO/IEC FDIS 27099

Information Technology — Public key infrastructure — Practices and policy framework

ISO TC 68 / SC 2 *"Financial Services, security"* has developed a PKI standard, ISO 21188:2018 (2nd edition, 1st edition in 2006)

ISO 21188:2018 *Public key infrastructure for financial services — Practices and policy framework* is financial services industry specific

SC 27 WG 4 decided to take over this existing standard to initiate a new work item aiming to develop a generic PKI standard

- not specific to any sector in particular with a particular effort was done on the controls related to RootCA management.
- Relying on X.509 v3 certificates
- In terms of contribution, liaisons were sent to other ISO groups, e.g: ISO TC68/SC22, ISO TC22/31 which are also maintaining ISO standards related to PKI, but on particular sectors.
- ETSI also was part of the Liaison, and played an active role in the commenting process in order to ensure general alignement with PKI standardisation work done by ETSI, for example on eIDAS.
- Worth noting that one ISO expert actively participating to the standard consistenly is with Google
- 27099 is now reaching FDIS stage

ISO/IEC FDIS 27099

Information Technology — Public key infrastructure — Practices and policy framework

Project leader(s) : GORLT Clément (LU) & SEYMOUR Anthony (GB)

Project stages :

- Proposal for new project proposal (10.00) : 2018-06-26
- New project registered in TC/SC work programme (20.00) : 2018-12-12
- Committee draft (CD) registered (30.00) : 2019-11-27
- DIS registered (40.00) : 2021-05-28
- Full report circulated : DIS approved for registration as FDIS : 2022-01-20
- Close of voting – Proof returned by secretariat (50.60) : target date 2022-06-10
- International Standard published (60.60) : limit date 2022-12-12

ISO/IEC DIS 27071

Cybersecurity — Security recommendations for establishing trusted connections between devices and services

Project leader(s) : ROSS David (AU), WANG Huili (CN) & ZANG Liwu (CN)

Project stages :

- Proposal for new project proposal (10.00) : 2018-11-05
- New project registered in TC/SC work programme (20.00) : 2019-05-09
- Committee draft (CD) registered (30.00) : 2021-06-04
- DIS registered (40.00) : limit date 2022-05-09
- Final texte received or FDIS registered for formal approval : target date 2022-07-01
- International Standard published (60.60) : target date 2023-01-01

ISO/IEC 27070:2021

Information technology — Security techniques — Requirements for establishing virtualized roots of trust

Project leader(s) : CHANDRAMOULI Ramaswamy (IN), GE Xiaoyu (CN), WANG Wuili (CN) & POLETTI Benoit (LU)

Project stages :

- Proposal for new project proposal (10.00) : 2017-06-27
- New project registered in TC/SC work programme (20.00) : 2018-03-26
- Committee draft (CD) registered (30.00) : 2019-12-03
- DIS registered (40.00) : 2020-10-12
- Final texte received or FDIS registered for formal approval : 2021-07-13
- International Standard published (60.60) : 2021-12-06

Thank you !!!
Any questions ?