

ACCREDITATION

CONFIANCE  
NUMÉRIQUE

SURVEILLANCE  
DU MARCHÉ

MÉTROLOGIE

NORMALISATION

ILNAS

*Welcome*  
*Bienvenue*  
*Willkommen*

# ICT technical standardization

—

## Focus on Cloud Computing

Mr. Nicolas Domenjoud

*Responsable secteur « TIC & Normalisation » – ILNAS/OLN*

04 February 2020

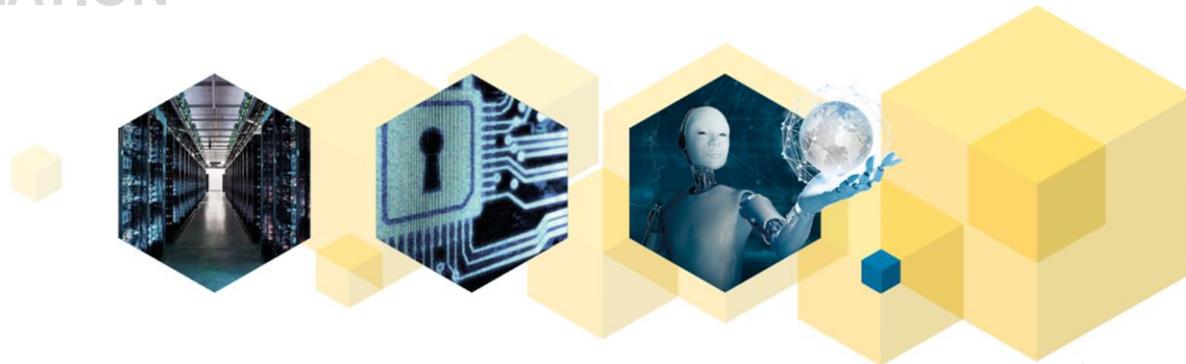


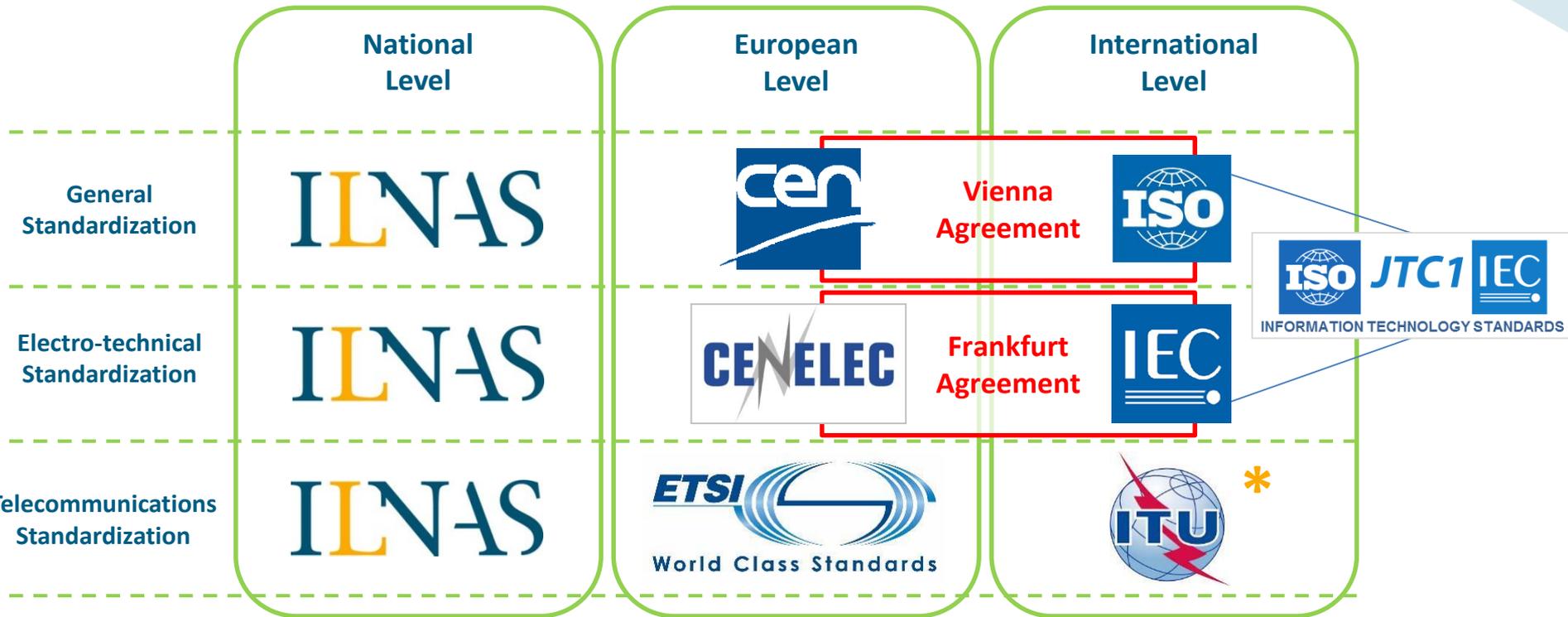


## I – ICT TECHNICAL STANDARDIZATION

## II – STANDARDS ANALYSIS SMART SECURE ICT

## III – FOCUS ON CLOUD COMPUTING TECHNICAL STANDARDIZATION





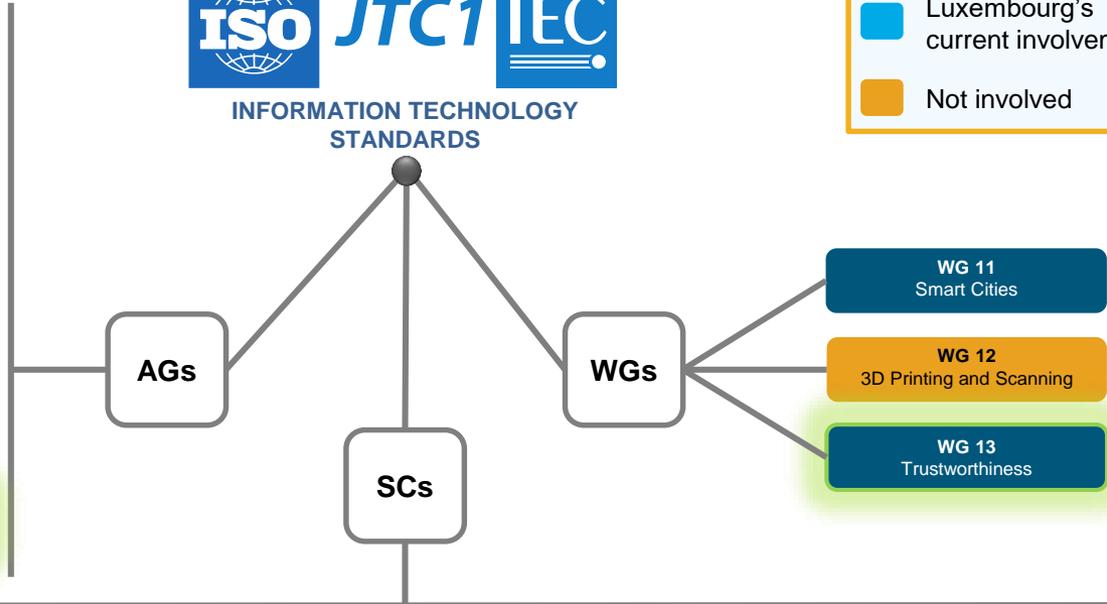
Presidency by ILNAS



INFORMATION TECHNOLOGY STANDARDS

- ILNAS & ANEC Direct involvement
- Luxembourg's current involvement
- Not involved

<b>AG 1</b> - Communications	<b>AG 10</b> - Outreach
<b>AG 2</b> - JTC 1 Emerging Technology and Innovation (JETI)	<b>AG 11</b> - Digital Twin
<b>AG 3</b> - Open Source Software	<b>AG 12</b> - Technical Corrigenda
<b>AG 4</b> - Quantum Computing	<b>AG 13</b> - Use Cases for VR and AR based ICT Integration Systems
<b>AG 6</b> - Autonomous and Data Rich Vehicles	<b>AG 14</b> - Systems Integration Facilitation (SIF)
<b>AG 8</b> - Meta RA and RA for Systems Integration	<b>AG 15</b> - Standards and Regulations
<b>AG 9</b> - Data Usage	<b>AG 16</b> - Brain-computer Interface (BCI)

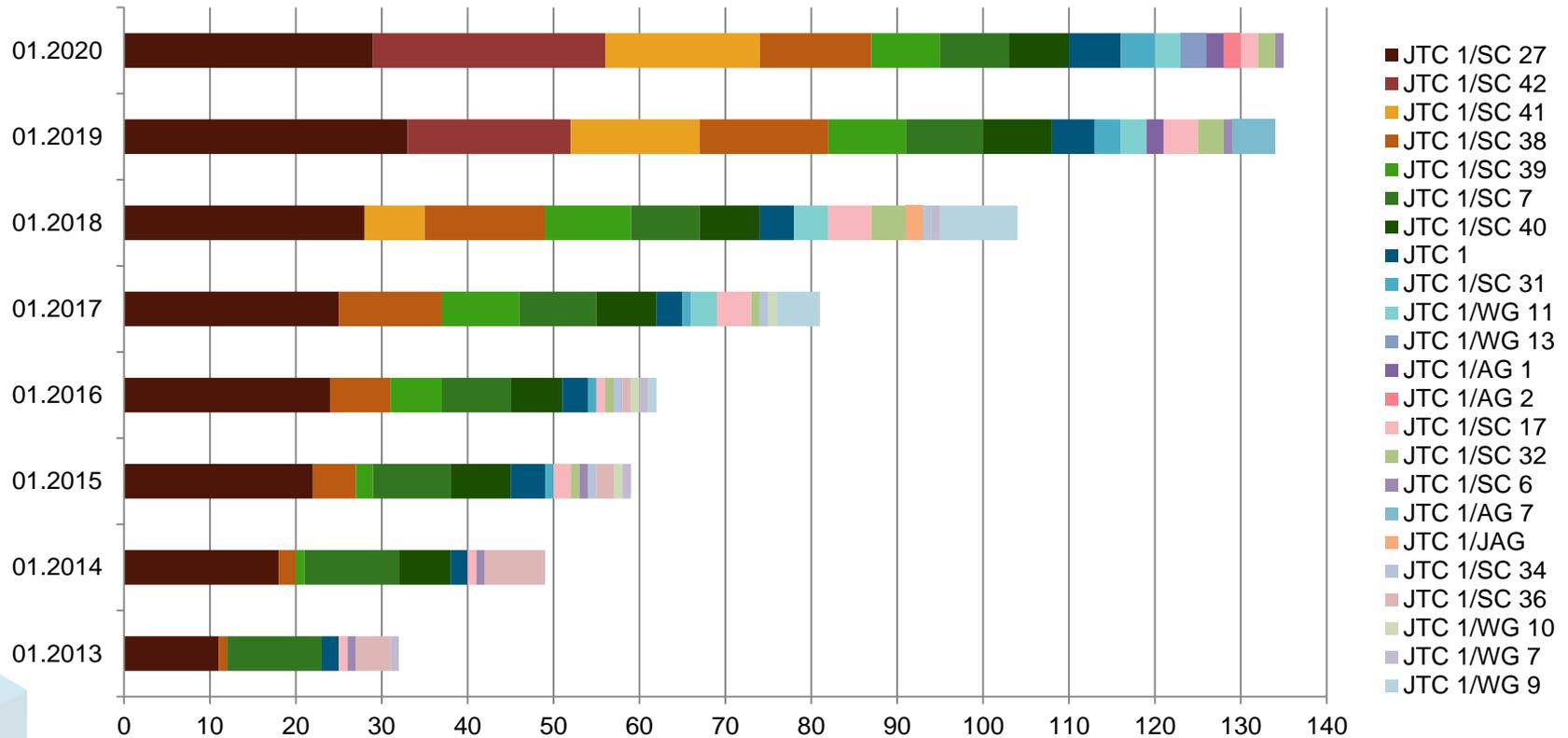


<b>SC 2</b> Coded Character Sets	<b>SC 6</b> Telecommunications and information exchange between systems	<b>SC 7</b> Software and Systems Engineering	<b>SC 17</b> Cards and security devices for personal identification	<b>SC 22</b> Programming languages, their environments and system software interfaces	<b>SC 23</b> Digitally recorded media for information interchange and storage	<b>SC 24</b> Computer graphics, image processing, and environmental data representation	<b>SC 25</b> Interconnection of information technology equipment	<b>SC 27</b> Information security, cybersecurity and privacy protection	<b>SC 28</b> Office equipment	<b>SC 29</b> Coding of audio, picture, multimedia and hypermedia information
<b>SC 31</b> Automatic identification and data captures techniques	<b>SC 32</b> Data management and interchange	<b>SC 34</b> Document description and processing languages	<b>SC 35</b> User interfaces	<b>SC 36</b> Information technology for learning, education and training	<b>SC 37</b> Biometrics	<b>SC 38</b> Cloud Computing and Distributed Platforms	<b>SC 39</b> Sustainability, IT & Data Centres	<b>SC 40</b> IT Service Management and IT Governance	<b>SC 41</b> Internet of Things and related technologies	<b>SC 42</b> Artificial Intelligence

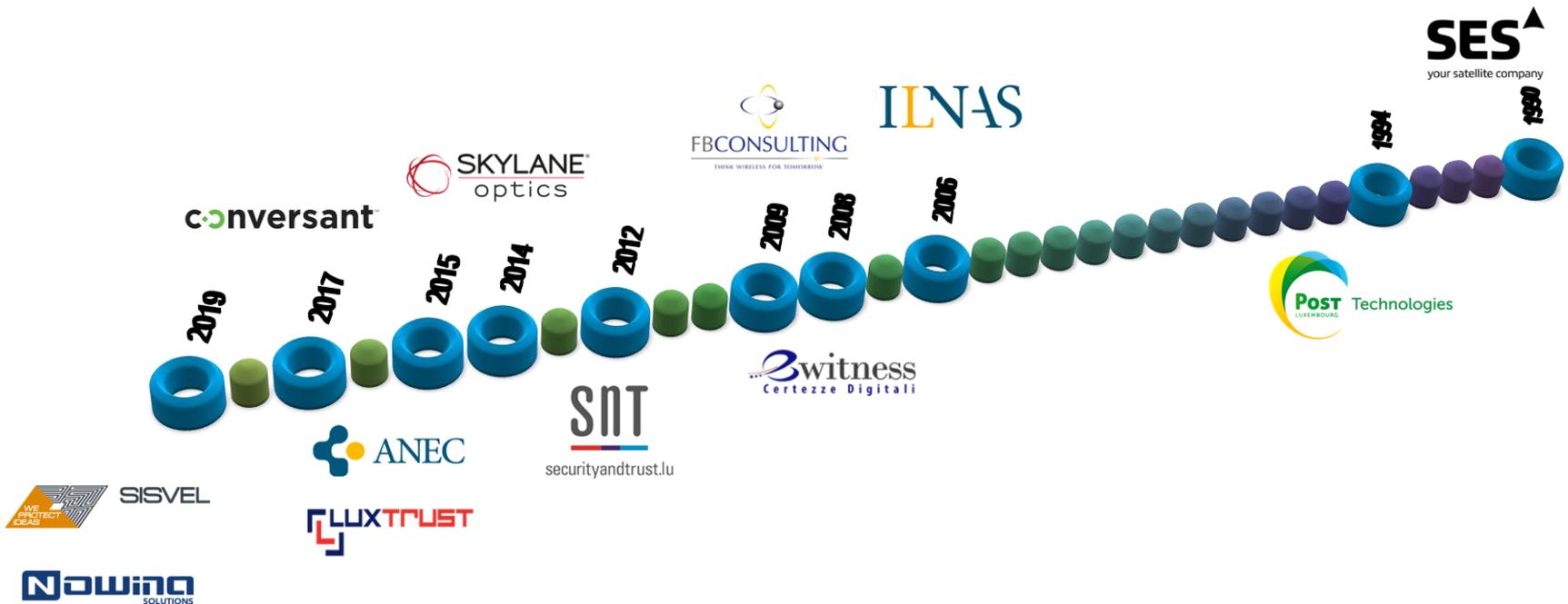
## - Evolution of the number of national standardization delegates in ISO/IEC JTC 1

### ➤ Top representation in JTC 1:

- 29 delegates in the IT security domain (■)
- 18 delegates in the IoT domain (■)
- 13 delegates in the Cloud Computing domain (■)
- 27 delegates in the AI / Big Data domains (■)



- 12 ETSI members in Luxembourg:



- **ILNAS follows some technical areas of particular interest – Examples:**

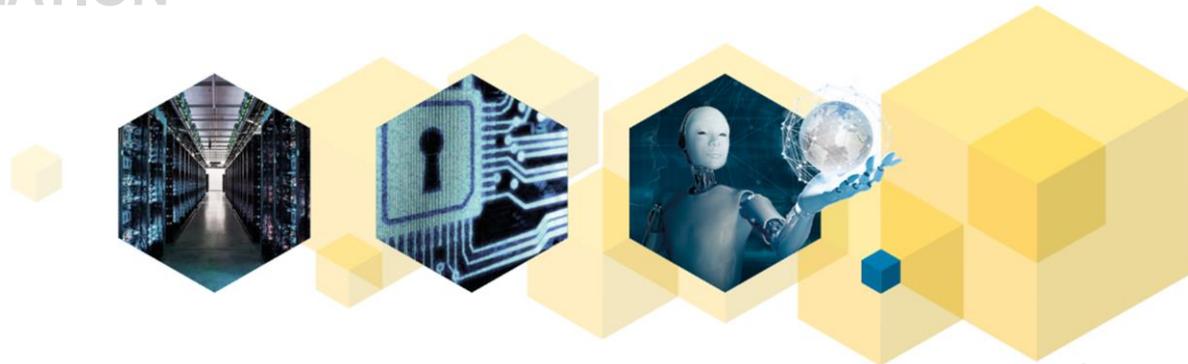
- **ETSI/TC CYBER - Cyber Security**
  - Responsible for standardization in the area of Cyber Security
  
- **ETSI/TC ESI - Electronic Signatures and Infrastructures**
  - Responsible for standardization supporting technology Electronic Signatures and related services (e.g. registered electronic delivery, electronic seals) as well as trust service infrastructures supporting such services
  - Supports regulatory requirements such as the eIDAS Regulation as well as general commercial requirements
  - Standards used by the Digital Trust department of ILNAS to supervise trust service providers



I – ICT TECHNICAL STANDARDIZATION

**II – STANDARDS ANALYSIS SMART SECURE ICT**

III – FOCUS ON CLOUD COMPUTING TECHNICAL  
STANDARDIZATION



- 
- I - Context and objectives of the Standards Analysis Smart Secure ICT
  - II - Results of the Standards Analysis
  - III - Opportunities for the national market

- 
- I - **Context and objectives of the Standards Analysis Smart Secure ICT**
  - II - Results of the Standards Analysis
  - III - Opportunities for the national market

# I. Context and objectives of the Standards Analysis Smart Secure ICT

## A. Context

2010-2020

LUXEMBOURG  
STANDARDIZATION STRATEGY  
2014-2020

"Technical standardization as a service"



**Pillar 1: Information and communication technologies (ICT)**

1

Developing the interest and the involvement of the market

2

Promoting and reinforcing market participation

3

Supporting and strengthening the EaS and related research activities

2020-2030



**ICT IS ONE OF THE GROWTH SECTORS IDENTIFIED**

- <https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-2014-2020.html>
- <https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-TIC-2015-2020.html>
- <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf>

# I. Context and objectives of the Standards Analysis Smart Secure ICT

## A. Context

### 2. GUIDELINES OF THE NATIONAL CYBERSECURITY STRATEGY

#### 2.1. Guideline No. 1: strengthening public confidence in the digital environment

- 2.1.1. **Objective 1 :** Knowledge-sharing between all stakeholders
- 2.1.2. **Objective 2 :** Disseminating information on risks
- 2.1.3. **Objective 3 :** Raising awareness of all the parties concerned
- 2.1.4. **Objective 4 :** Responsible disclosure
- 2.1.5. **Objective 5 :** Combating cybercrime

#### 2.2. Guideline No. 2: digital infrastructure protection

- 2.2.1. **Objective 1 :** Census of essential and critical digital infrastructure
- 2.2.2. **Objective 2 :** Security policies
- 2.2.3. **Objective 3 :** Crisis management
- 2.2.4. **Objective 4 :** Standardization
- 2.2.5. **Objective 5 :** Strengthen international cooperation
- 2.2.6. **Objective 6 :** Cyber defence
- 2.2.7. **Objective 7 :** Strengthening the resilience of the State's digital infrastructure

### OBJECTIVE 4 : STANDARDIZATION

Standardization determines common technical language, both at European and international level. If applied to the field of cybersecurity, this unifying capability allows us to set definitions and needs, the state of the art in this area as well as reference architecture, while establishing by consensus requirements and specifications required to ensure a suitable level of security. This constantly evolving whole facilitates digital ownership, especially for Smart ICT developments (Cloud Computing, Big Data, the Internet of things, Blockchain, etc.).

National monitoring and investment in the development process of standards related to the field of cybersecurity will be strengthened,

specifically in order to convert it into a strategic tool for the development of national digital confidence.

This approach will be carried out for formal technical standardization (ISO, IEC, ETSI, CEN-CENELEC, ITU-T), while taking into account the work developed by relevant fora and consortia identified in the context of cybersecurity.

The ILNAS (Luxembourg standardisation body) will unify and develop this strategic monitoring in order to report it at national level, in the interest of the implementation of a "smart nation".

# I. Context and objectives of the Standards Analysis Smart Secure ICT

## A. Context

- Relies on previous ILNAS Smart ICT publications
- Focuses on **four Smart ICT areas**, considering **related Digital Trust** challenges and developments from a standardization perspective
- Provides a monitoring of **relevant technical committees and standards**
- Introduces **Fora and Consortia** identified as relevant in the cybersecurity context



Internet of Things

Cloud Computing

Artificial Intelligence & Big Data

Blockchain

**DIGITAL TRUST**

# I. Context and objectives of the Standards Analysis Smart Secure ICT

## B. Objectives

### INFORM

about Smart ICT  
standardization  
developments

### IDENTIFY

standardization  
opportunities for the  
national market

### ENCOURAGE

the involvement  
in the standardization  
process

### DEVELOP

“standards-related”  
skills and  
collaborations

For the benefit of all national stakeholders

# I. Context and objectives of the Standards Analysis Smart Secure ICT

## C. Scope of the Standards Analysis

- Introduction of **Smart ICT technologies main characteristics**
- Identification and presentation of **relevant standardization technical committees** as well as identified **Fora and Consortia in the context of cybersecurity**
- Introduction of **basic components of Digital Trust for Smart ICT**
- Identification and presentation of **standards published or in development** in the selected Smart ICT areas as well as **Digital Trust standards developments** related to these areas
- Identification and presentation of **standardization opportunities offered to the national stakeholders in Luxembourg**

	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
International Level			
European Level			
National Level			

- 
- I - Context and objectives of the Standards Analysis Smart Secure ICT
  - II - Results of the Standards Analysis**
  - III - Opportunities for the national market

### A. Smart (Secure) ICT overview

#### - Smart ICT definition

*Smart ICT corresponds to a holistic approach of ICT development, integration and implementation, where a range of emerging or innovative tools and techniques are used to maintain, improve or develop products, services or processes with the global objective to strengthen different societal, social, environmental and economic needs. It includes, through related interconnected ecosystems, advanced ICT such as Cloud Computing, Big Data and Analytics, Internet of Things, Artificial Intelligence, Robotics, and new ways of gathering data, such as social media and crowdsourcing.*

#### - Introduction of fundamental concepts of Smart ICT and related Digital Trust aspects based on standards

- **Internet of Things:**
  - ISO/IEC 20924:2018, Definitions and vocabulary (*new*)
  - ITU-T Y.4000/Y.2060 (06/2012), Overview of the Internet of things
- **Cloud Computing:**
  - ISO/IEC 17788:2014 | ITU-T Y.3500, Overview and vocabulary
- **Artificial Intelligence and Big Data:**
  - ISO/IEC 20546:2019, Big Data -- Definition and Vocabulary (*new*)
  - ISO/IEC 22989, Artificial Intelligence -- Concepts and Terminology (*under development*)
- **Blockchain and Distributed Ledger Technologies:** ISO 22739, Terminology and concepts (*under development*)
- **Basic Components of Digital Trust**

## B. Internet of Things

- **TECHNICAL COMMITTEES (6)**

- ISO/IEC JTC 1/SC 41 “Internet of Things and related technologies”
- ISO/IEC JTC 1/SC 31 “Automatic identification and data capture techniques”
- ISO/IEC JTC 1/SC 25 “Interconnection of information technology equipment”
- CEN/TC 225 “AIDC Technologies”
- ETSI/TC SmartM2M “Smart Machine-to-Machine Communication”
- ITU-T/SG 20 “Internet of Things, smart cities and communities”

- **PUBLISHED STANDARDS (65)**

- ISO/IEC 30141:2018, Internet of Things Reference Architecture (IoT RA)
- ISO/IEC TR 22417:2017, IoT use cases
- ISO/IEC 21823-1:2019, Interoperability for Internet of things systems -- Part 1: Framework (*new*)
- ...

- **STANDARDS UNDER DEVELOPMENT (66)**

- ISO/IEC CD 30161, Requirements of IoT data exchange platform for various IoT services
- ISO/IEC CD 30165, Real-time IoT framework
- ISO/IEC CD 30166, Industrial IoT (*new*)
- ...

## C. Cloud Computing

**- TECHNICAL COMMITTEES (2)**

- ISO/IEC JTC 1/SC 38 “Cloud Computing and Distributed Platforms”
- ITU-T/SG 13 “Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures”

**- PUBLISHED STANDARDS (62)**

- ISO/IEC 19941:2017, Interoperability and portability
- ISO/IEC 19944:2017, Cloud services and devices: Data flow, data categories and data use
- ISO/IEC TR 22678:2019, Guidance for Policy Development (*new*)
- ...

**- STANDARDS UNDER DEVELOPMENT (23)**

- ISO/IEC CD 22123-1, Cloud computing -- Part 1: Terminology
- ISO/IEC CD 22123-2, Cloud computing -- Part 2: Concepts
- ISO/IEC AWI 23751, Data sharing agreement (DSA) framework (*new*)
- ISO/IEC CD TR 23951, Best practices for cloud SLA metrics (*new*)
- ...

## D. Artificial Intelligence and Big Data

**- TECHNICAL COMMITTEES (3)**

- ISO/IEC JTC 1/SC 42 “Artificial Intelligence”
- ISO/IEC JTC 1/SC 32 “Data management and interchange”
- ITU-T/SG 16 “Multimedia coding, systems and applications” (*new*)

**- PUBLISHED STANDARDS (35)**

- ISO/IEC 20546:2019, Big Data -- Overview and Vocabulary (*new*)
- ISO/IEC TR 20547-2:2018, Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
- ISO/IEC TR 20547-5:2018, Big data reference architecture -- Part 5: Standards roadmap
- ...

**- STANDARDS UNDER DEVELOPMENT (43)**

- ISO/IEC CD 22989, Artificial Intelligence -- Concepts and Terminology
- ISO/IEC CD 23053, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/IEC CD TR 24030, Information technology -- Artificial Intelligence (AI) -- Use cases (*new*)
- ...

## E. Blockchain and Distributed Ledger Technologies

- **TECHNICAL COMMITTEES (1)**
  - ISO/TC 307 “Blockchain and distributed ledger technologies”
  
- **PUBLISHED STANDARDS (1)**
  - ISO/TR 23455:2019, Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems (*new*)
  
- **STANDARDS UNDER DEVELOPMENT (10)**
  - ISO/DIS 22739, Terminology
  - ISO/CD TR 23245, Security risks, threats and vulnerabilities
  - ISO/AWI TR 23246, Overview of identity management using blockchain and distributed ledger technologies
  - ISO/CD 23257, Reference architecture
  - ISO/AWI TS 23635, Guidelines for governance
  - ...

## F. Digital Trust in Smart ICT

- **TECHNICAL COMMITTEES (8)**
  - ISO/IEC JTC 1/SC 27 “Information Security, cybersecurity and privacy protection”
  - CEN/CLC/JTC 13 “Cybersecurity and Data Protection”
  - ETSI/TC CYBER “Cyber Security”
  - ...
- **PUBLISHED STANDARDS (32) → Digital Trust aspects of Smart ICT**
  - **IoT:** ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things (*new*)
  - **Cloud Computing:** ISO/IEC 27018:2019, Guidance for the assessment of information security controls (*new*)
  - **AI/Big Data:** ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques
  - ...
- **STANDARDS UNDER DEVELOPMENT (39)**
  - **IoT:** ISO/IEC 30149, Trustworthiness framework
  - **Cloud Computing:** ITU-T Draft X.sgmc, Security guidelines for multi-cloud (*new*)
  - **AI/Big Data:** ISO/IEC CD TR 24028, Overview of trustworthiness in Artificial Intelligence (*new*)
  - ...

### G. Presentation of the results

#### - Presentation of the technical committees using ID-Cards

General information			
<b>Committee</b>	ISO/IEC JTC 1/SC 27	<b>Title</b>	Information Security, cybersecurity and privacy protection
<b>Creation date</b>	1989		
<b>Secretariat</b>	DIN (Germany)		
<b>Committee Manager</b>	Ms. Krystyna Passia		
<b>Chairperson</b>	Dr. Andreas Wolf		
<b>Organizations in liaison</b>	(ISC)2, CalConnect, CCETT, CSA, ECBS, Ecma International, ENISA, EPC, ETSI, Global Platform, IEEE, ISACA, ISSEA, ITU, MasterCard Int., SBS, ABC4Trust, Article 29 Data Protection Working Party, CCDB, CCUF, CREDENTIAL, CSCC, Cyber Security, EUDCA, EuroCloud, FIDO Alliance, FIRST, IFAA, INLAC, Interpol, ISA – Automation, ISCI, ISF, Kantara Initiative, OASIS-PMRM, OECD, OIF, Opengroup – United Kingdom, PICOS, PQCRYPTO, PRIPARE, PRISMACLOUD, SAFECode, SAFEcrypto, TAS3, TCG, TMForum, TRESPASS, WITDOM	<b>MEMBERS</b> 	<b>Participating Countries (48):</b> Germany, Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Cyprus, Denmark, Finland, France, India, Indonesia, Islamic Republic of Iran, Ireland, Israel, Italy, Japan, Republic of Korea, Lebanon, Luxembourg, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Poland, Romania, Russian Federation, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay
<b>Web site</b>	<a href="https://www.iso.org/committee/45306.html">https://www.iso.org/committee/45306.html</a>		
<b>Scope</b>	<p>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:</p> <ul style="list-style-type: none"> <li>- Security requirements capture methodology;</li> <li>- Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls and services;</li> <li>- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;</li> <li>- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;</li> <li>- Security aspects of identity management, biometrics and privacy;</li> </ul>		

<b>Structure</b>	JTC 1/SC 27/AG 1 JTC 1/SC 27/SG 1 JTC 1/SC 27/SG 2 JTC 1/SC 27/SG 3 JTC 1/SC 27/SWG-T JTC 1/SC 27/WG 1 JTC 1/SC 27/WG 2 JTC 1/SC 27/WG 3 JTC 1/SC 27/WG 4 JTC 1/SC 27/WG 5	Management Advisory Group Data Security Trustworthiness Concepts and Terminology Transversal Items Information security management systems Cryptography and security mechanisms Security evaluation testing and specification Security controls and services Identity management and privacy technologies
<b>Standardization work</b>		
<b>Published standards</b>	184	
<b>Standards under development</b>	80	
<b>Involvement of Luxembourg</b>		
<b>27 delegates</b>		
-	Mr. Benoit Poletti (Chairman)	INCERT GIE
-	Mr. Carlo Harpes (Vice-Chairman)	itrust consulting S.à r.l.
-	Mr. Johann Amsenga (Convener WG 4)	INCERT GIE
-	Mr. Matthieu Aubigny	itrust consulting S.à r.l.
-	Mr. Benoit Bertholon	COINPLUS S.A.
-	Mr. Hervé Cholez	LIST
-	Mr. Stéphane Cortina	LIST
-	Mrs. Saharnaz Dilmaghani	University of Luxembourg
-	Mrs. Myriam Djerouni	LUXITH G.I.E.
-	Mr. Nicolas Domenjoud	ILNAS
-	Mrs. Michèle Feltz	ILNAS
-	Mr. Ben Fetter	CTIE
-	Mr. Philippe Germain	PmG SD S.à r.l.
-	Mr. Clement Gort	INCERT GIE
-	Mrs. Carine Grenouillet	INCERT GIE
-	Mrs. Shenplan Hu	POST Telecom PSF S.A.
-	Mr. Ravi Jawhar	PwC
-	Mr. Jean Lancrenon	ANEC G.I.E.
-	Mr. Chao Liu	University of Luxembourg
-	Mr. Michel Ludwig	ILNAS
-	Mr. Alex Mckinnon	SES S.A.
-	Mr. Gaëtan Pradel	INCERT GIE
-	Mr. René Saint-Germain	Certi-Trust S.à r.l.
-	Mr. Nader Samir Labib	University of Luxembourg
-	Mr. Raphaël Taban	CTIE
-	Mr. Qiang Tang	University of Luxembourg
-	Mr. Muhammad Wasim	University of Luxembourg
<b>Comments</b>		
SC 27 is an internationally recognized center of information and IT security standards expertise serving the needs of business sectors as well as governments. Its work covers the development of standards for the protection of information and ICT.		
<b>Working Groups</b>		
-	<b>WG 1:</b> the scope of the WG 1 covers all aspects of standardization related to information security management systems: requirements, methods and processes, security controls, sector and application specific use of ISMS, governance, information security economics and accreditation,	

## G. Presentation of the results

e.g.: Digital Trust for Cloud Computing standards

- **Published standards and standards projects listed in the Appendix**
  - Areas concerned: IoT, Cloud Computing, Artificial Intelligence and Big Data
  - Information provided:
    - Standards (published / under development)
    - **Digital Trust related standards (published / under development)**

SDO	Reference	Title
ISO/IEC JTC 1 / ITU-T	<a href="#">ISO/IEC 27017:2015 / ITU-T X.1631 (07/2015)</a>	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC JTC 1	<a href="#">ISO/IEC 27018:2019</a>	Information technology -- Security techniques -- Guidance for the assessment of information security controls
ISO/IEC JTC 1	<a href="#">ISO/IEC 27036-4:2016</a>	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ISO/IEC JTC 1	<a href="#">ISO/IEC 21878:2018</a>	Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers
ISO/IEC JTC 1	<a href="#">ISO/IEC 19086-4:2019</a>	Information technology -- Cloud computing – agreement (SLA) framework – Part 4: Components of security and protection of PII
ISO/IEC JTC 1	<a href="#">ISO/IEC TR 23186:2018</a>	Information technology -- Cloud computing -- Framework of trust for processing of multi-sourced data
ETSI	<a href="#">ETSI TR 103 304 V1.1.1 (07/2016)</a>	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ETSI	<a href="#">ETSI SR 003 391 V2.1.1 (02/2016)</a>	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing
ETSI	<a href="#">ETSI TS 103 532 V1.1.1 (03/2018)</a>	Attribute Based Encryption for Attribute Based Access Control
ETSI	<a href="#">ETSI TS 103 458 v1.1.1 (06/2018)</a>	Application of Attribute Based Encryption for PII and personal data protection on IoT devices, WLAN, Cloud and mobile services – High-level requirements
ITU-T	<a href="#">ITU-T X.1601 (10/2015)</a>	Security framework for cloud computing (edition 2 under development)
ITU-T	<a href="#">ITU-T X.1602 (03/2016)</a>	Security requirements for software as a service application environments
ITU-T	<a href="#">ITU-T X.1603 (03/2018)</a>	Data security requirements for the monitoring service of cloud computing

## II. Results of the Standards Analysis

### G. Presentation of the results

- A list of relevant Fora and Consortia working in the Digital Trust area (and notably in relation with Smart ICT technologies) is provided (**23 Fora and Consortia identified**)

	IIC	Industrial Internet Consortium
Scope	The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the industrial internet by identifying, assembling, testing and promoting best practices. Members work collaboratively to speed the commercial use of advanced technologies. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations.	
Activities	Standards Development	
Topics	IoT, IIoT, Artificial Intelligence, Blockchain, Cybersecurity, Smart Factory, Smart Cities, Intelligent Transport Systems	
Website	<a href="https://www.iiconsortium.org/">https://www.iiconsortium.org/</a>	

CSA	Cloud Security Alliance
Cloud Security Alliance (CSA) is a global organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, organizations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products.	

The CSA operates a cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. The CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and consultants that offer qualified professional services based on CSA best practices.

	(ISC)2	International Information System Security Certification Consortium
Scope	(ISC) <sup>2</sup> is an international, nonprofit membership association for information security leaders. It provides globally recognized certifications in every aspect of information security (e.g.: CISSP). It is also educating the general public through the support of its Center for Cyber Safety and Education.	
Activities	Education, Certification	
Topics	IT security, Cybersecurity, Application Security, Cloud Computing	
Website	<a href="https://www.isc2.org">https://www.isc2.org</a>	

Certification, Research  
 Cloud Computing, Artificial Intelligence, Blockchain, Internet of Things  
<https://securityalliance.org>



- 
- I - Context and objectives of the Standards Analysis Smart Secure ICT
  - II - Results of the Standards Analysis
  - III - Opportunities for the national market**

#### INFORMATION ABOUT STANDARDIZATION



- Smart ICT workshops
- Awareness sessions
- Smart ICT standards watch
- Publications and disseminations
- Free consultation of the standards
- Smart ICT standardization research results

#### TRAININGS IN STANDARDIZATION



- Trainings on Smart ICT Standardization
- Future professional “*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*” (forecast in September 2020)

#### INVOLVEMENT IN STANDARDIZATION

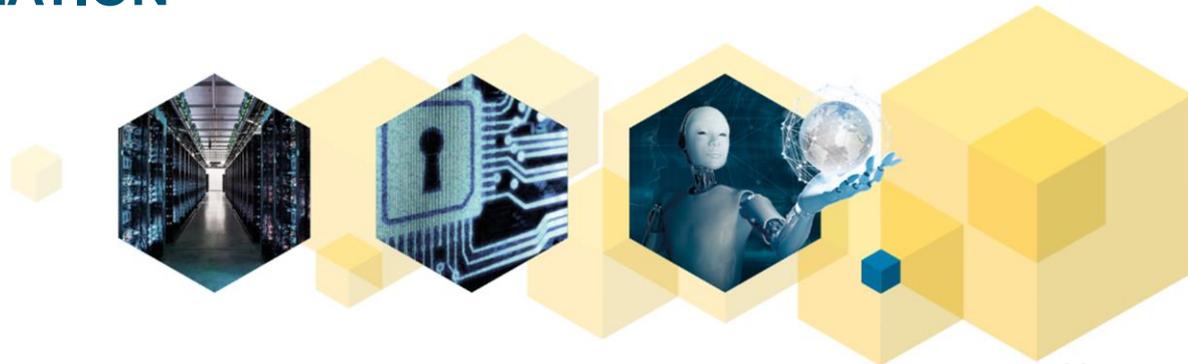


- Become national delegate in standardization
- Comment standards under public enquiry
- Propose new standards projects
- Monitor the standardization work performed by the European Multi-Stakeholder Platform on ICT Standardization (MSP)

I – ICT TECHNICAL STANDARDIZATION

II – STANDARDS ANALYSIS SMART SECURE ICT

**III – FOCUS ON CLOUD COMPUTING TECHNICAL  
STANDARDIZATION**





## ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms

### - Some published standards

- ISO/IEC 17788:2014 - Overview and vocabulary

- ISO/IEC 17789:2014 - Reference architecture

- ISO/IEC 19086 series on Service level agreement (SLA) framework

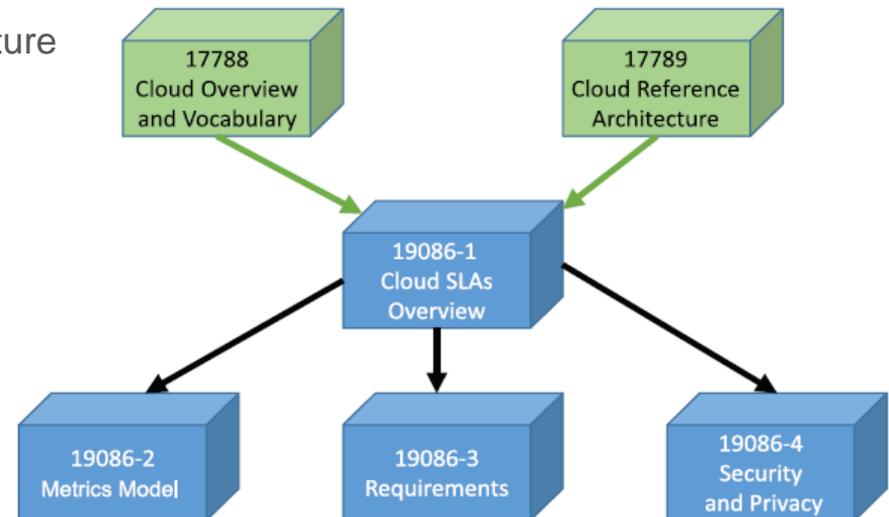
- Part 1: Overview and concepts
- Part 2: Metric model
- Part 3: Core conformance requirements

- ISO/IEC 19941:2017 - Interoperability and portability

- ISO/IEC 19944:2017 - Cloud services and devices: Data flow, data categories and data use

- ISO/IEC TR 22678:2019 - Guidance for policy development

- ISO/IEC TR 23186:2018 - Framework of trust for processing of multi-sourced data



## ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms

### - Current projects

- **ISO/IEC AWI TR 3445 - Guidance and best practices for cloud audits**
  - Surveys aspects and elements specific to cloud audit including:
    - Role and responsibilities of individual(s) conducting audit
    - Approaches and best practice of conducting audits of cloud services
    - Summary of available framework and standards on certification, authorization, and approach
- ISO/IEC DIS 19944-1 - Cloud services and devices: data flow, data categories and data use -- Part 1: Fundamentals
- ISO/IEC 22123-1 - Cloud computing
  - Part 1: Terminology
  - Part 2: Concepts
- ISO/IEC 22624 - Taxonomy based data handling for cloud services
- ISO/IEC TS 23167 - Common technologies and techniques
- ISO/IEC CD TR 23187 - Interacting with cloud service partners (CSNs)

## ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms

### - Current projects

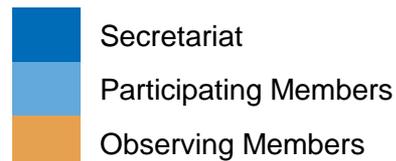
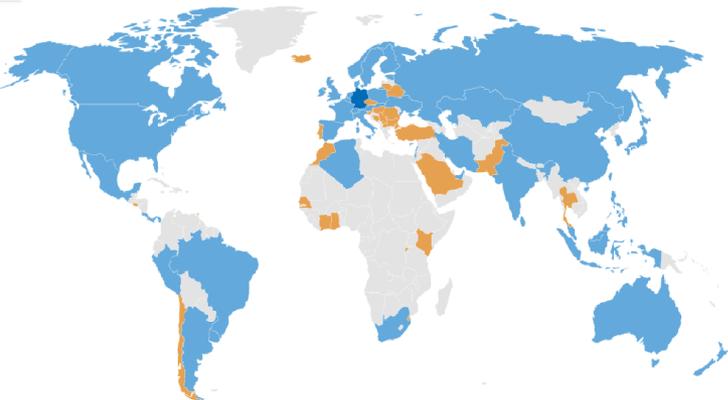
- ISO/IEC TR 23188 - Edge computing landscape
- ISO/IEC CD TR 23613 - Cloud service metering elements and billing modes
- ISO/IEC AWI 23751 - Data sharing agreement (DSA) framework
- **ISO/IEC CD TR 23951 - Guidance for using the cloud SLA metric model**
  - Describe guidance for using ISO/IEC 19086-2 metric model, illustrated with examples

### - Topics under study (Advisory Groups)

- **Multi-Cloud**
  - Identify and classify scenarios where CSCs use multiple cloud services from two or more CSPs
- **Cloud Management**
- **Customer to Cloud Services Connectivity**
  - Provide international standards perspectives regarding the options, best practices and approaches to assure connectivity meets the cloud services customers (CSCs) requirements

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

- **Creation: 1989**
- **Main focus areas**
  - 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 (ISMS, cryptography, security evaluation, security testing, identity management, etc.)
- **Key Indicators:**
  - **188** published standards
  - **76** standards under development
  - **50** Participating members (incl. Luxembourg)
  - **28** Observing members
- **Structure:**
  - **5 WGs** – Working Groups
    - **WG 1:** Information security management systems
    - **WG 4:** Security controls and services
  - **3 SGs:** Study Groups
  - **1 AG:** Advisory Group



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

### - Published standards related to Cloud Computing

- ISO/IEC 19086-4:2019 - Cloud computing -- Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII
- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27036-4:2016 - Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services



# ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10

E-mail: [info@ilnas.etat.lu](mailto:info@ilnas.etat.lu)

[www.portail-qualite.lu](http://www.portail-qualite.lu)