



# CORAL

cybersecurity Certification based On Risk evALuation and treatment

## Cybersecurity standards in support of the Cybersecurity Act

Presented by Natalia Vinogradova, ANEC GIE

18/10/2023





# CORAL

## Cybersecurity standards

### *Article 54*

#### **Elements of European cybersecurity certification schemes**

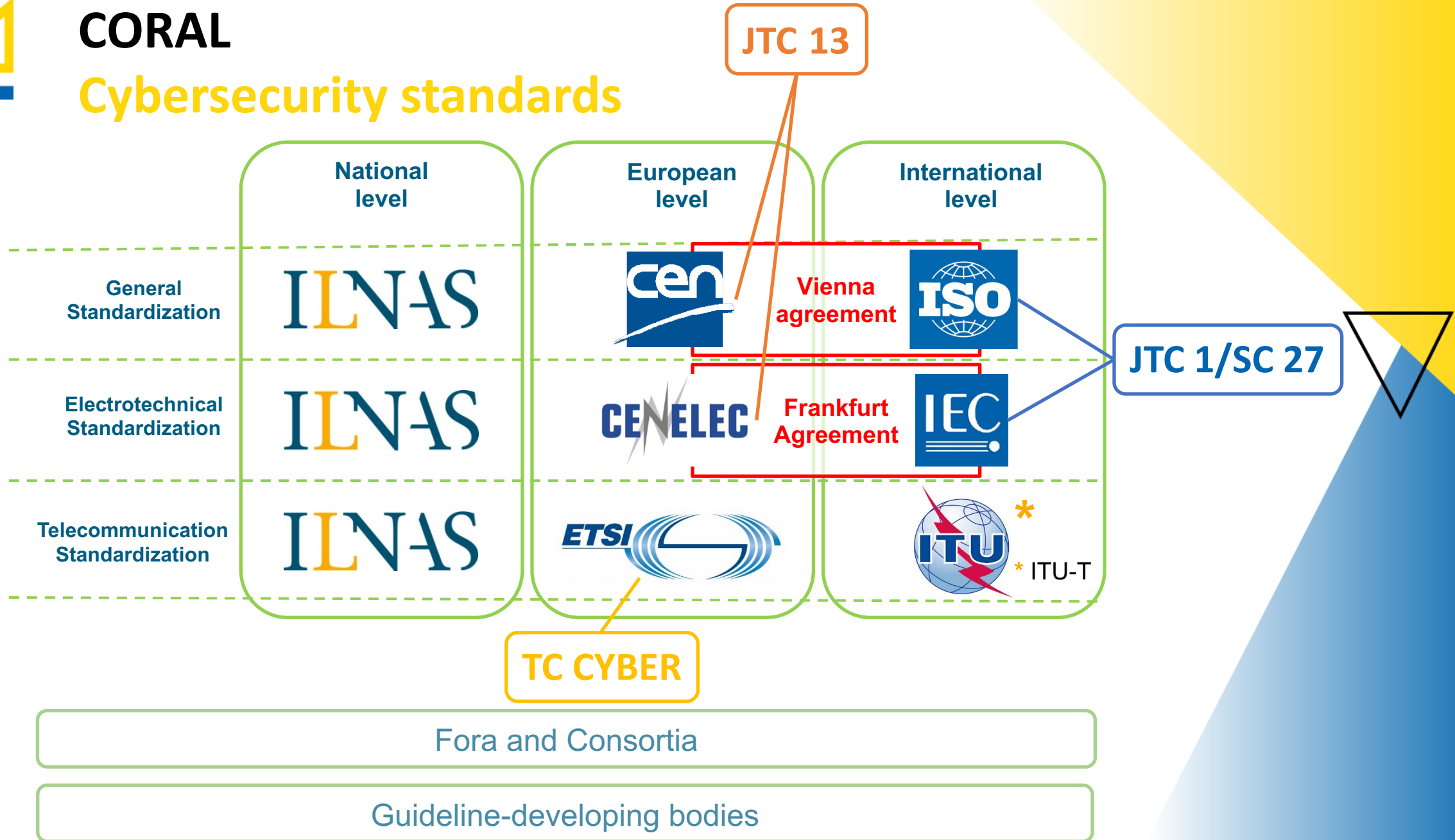
1. A European cybersecurity certification scheme shall include at least the following elements:
  - (a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;
  - (b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;
  - (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

- **Collaboration between the European standardization organizations and ENISA in order to identify potential needs and gaps for cybersecurity certification schemes**
- **Most relevant technical committees**
  - *CEN/CLC/JTC 13 “Cybersecurity and Data Protection”*
  - *ETSI/TC CYBER “Cybersecurity”*
  - *ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection”*



**CORAL**

# Cybersecurity standards





# CORAL

## Cybersecurity standards



### CEN/CLC JTC 13 “Cybersecurity and Data Protection”

#### Scope:

- Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to:
  - Management systems, frameworks, methodologies
  - Data protection and privacy
  - **Services and products evaluation standards suitable for security assessment** for large companies and small and medium enterprises (SMEs)
  - Competence requirements for cybersecurity and data protection
  - **Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices**
- Included in the scope is the **identification and possible adoption of documents already published or under development by ISO/IEC JTC 1 and other SDOs and international bodies** such as ISO, IEC, ITU-T, and industrial fora. Where not being developed by other SDO's, the development of cybersecurity and data protection CEN/CENELEC publications for safeguarding information such as organizational frameworks, management systems, techniques, guidelines, and products and services, including those in support of the EU Digital Single Market.



Working group	Title
<a href="#">CEN/CLC/JTC 13/WG 1</a>	Chair's Advisory Group
<a href="#">CEN/CLC/JTC 13/WG 2</a>	Management systems and controls sets
<a href="#">CEN/CLC/JTC 13/WG 3</a>	Security evaluation and assessment
<a href="#">CEN/CLC/JTC 13/WG 5</a>	Data Protection, Privacy and Identity Management
<a href="#">CEN/CLC/JTC 13/WG 6</a>	Product security
<a href="#">CEN/CLC/JTC 13/WG 7</a>	Adhoc group EU 5G Certification scheme support group
<a href="#">CEN/CLC/JTC 13/WG 8</a>	Special Working Group RED Standardization Request
<a href="#">CEN/CLC/JTC 13/WG 9</a>	Special Working Group on Cyber Resilience Act



**CORAL**

## Cybersecurity standards



**CENELEC**

### CEN/CLC JTC 13 “Cybersecurity and Data Protection”

#### Standards in support of the CSA

- EN 17640:2022 “Fixed time cybersecurity evaluation methodology for ICT products”
  - This document **describes a cybersecurity evaluation methodology that can be implemented using pre-defined time and workload resources, for ICT products. It is intended to be applicable for all three assurance levels defined in the CSA (i.e. basic, substantial and high).**
  - The methodology comprises different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the mentioned three assurance levels. Where appropriate, it can be applied both to third-party evaluation and self-assessment.
- prEN XXXX “Guidelines on a sectoral cybersecurity assessment”
  - This document contains **guidelines to be used in the process of drafting requirements of cybersecurity certification schemes for sectoral ICT services and systems.** It includes all steps necessary to define, implement and maintain such requirements.
  - Note: Standard proposed by ENISA based on their own publication (<https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>)





**CORAL**

## Cybersecurity standards



**CENELEC**

### CEN/CLC JTC 13 “Cybersecurity and Data Protection”

#### Standards in support of the CSA (EUCS)

- FprCEN/CLC/TS 18026 “Three-level approach for a set of cybersecurity requirements for cloud services”
  - This Technical Specification (TS) **provides a set of information security requirements for information/cyber security controls for Cloud Services.**
  - This TS is applicable for organizations providing cloud services and their subservice organizations.
- prCEN/CLC/TS XXX “Requirements for Conformity Assessment Bodies certifying Cloud Services”
  - This TS **provides requirements and ISO/IEC 17065 interpretations for Conformity Assessment Bodies (CABs) assessing Cloud Services.**
  - This TS is intended to be used by the National Accreditation Bodies (NABs), as well as CABs.





**CORAL**

## Cybersecurity standards



**CENELEC**

### CEN/CLC JTC 13 “Cybersecurity and Data Protection”

#### Standards in support of the CSA

- EN 17927 “Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.”
  - This document **describes a cybersecurity evaluation methodology, named SESIP, for components of connected ICT products.** Security claims in SESIP are made based on the security services offered by those components. Components can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of components which apply to the foundational components of devices that are not application specific. The methodology describes the re-use of evaluation results.





**CORAL**

## Cybersecurity standards



**ETSI/TC CYBER “Cybersecurity”**

### Scope:

- To act as the **ETSI centre of expertise in the area of Cyber Security**
- Advise and assist all ETSI Groups with the development of Cyber Security requirements
- To develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI
- To collect and specify Cyber Security requirements from relevant stakeholders
- To identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects
- To ensure that appropriate Standards are developed within ETSI in order to meet these requirements
- To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects
- **To coordinate work in ETSI with external groups such as ENISA**
- **To answer to policy requests related to Cyber Security, and security in broad sense in the ICT sector**







# CORAL

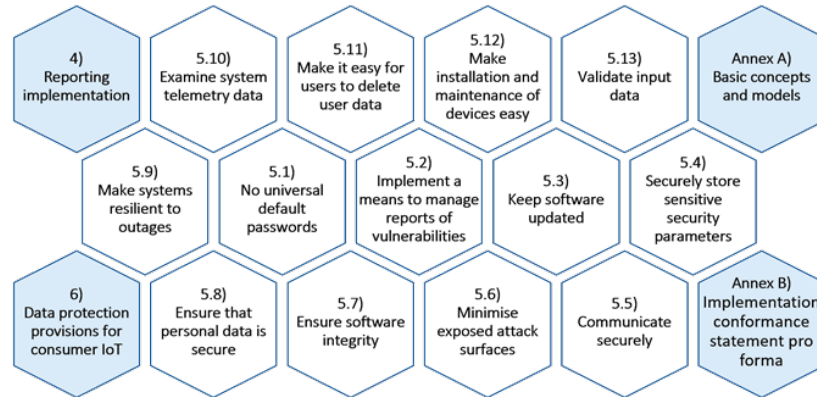
## Cybersecurity standards



### ETSI/TC CYBER “Cybersecurity”

#### Standards in support of the CSA

- EN 303 645 “CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”
  - The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope.



- EN 303 645 and its complementary assessment specification and implementation guide **could be used in a certification scheme** if the EC request ENISA to prepare a cybersecurity certification scheme for IoT under the Cybersecurity Act
- This work on security and evaluation requirements for consumer mobile device **could be also of use for certification of 5G mobile devices**





**CORAL**

## Cybersecurity standards



**ETSI/TC CYBER “Cybersecurity”**

### Standards in support of the CSA

- TS 103 701 “CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements”
  - The present document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645/ETSI EN 303 645, addressing the mandatory and recommended provisions as well as conditions and complements of ETSI TS 103 645/ETSI EN 303 645 by defining test cases and assessment criteria for each provision.
- TR 103 621 “Guide to Cyber Security for Consumer Internet of Things”
  - The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.
  - The present document is complementary to ETSI EN 303 645 and ETSI TS 103 701. It explains the relationship between these specifications and how they can be used together. It also provides a non-exhaustive set of example implementations that can be used to meet the provisions of ETSI EN 303 645 and ETSI TS 103 645, noting that not all possible implementations are included. Where relevant, pointers to supporting specifications are provided. Usage by industry players as well as future development of standards, such as specialisation into precise use cases, or certification aspects, are being given consideration.





# CORAL

## Cybersecurity standards

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



#### 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/JWG 6	Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies



**CORAL**

## Cybersecurity standards

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



#### Standards in support of the CSA (EUCC)

Evaluations shall be based on the following standards:

- Common Criteria for Information Technology Security Evaluation, under their applicable ISO/IEC 15408 version or under their applicable version published on <https://www.commoncriteriaportal.org/cc/>, and composed of:
  - CC Part 1: Introduction and general model;
  - CC Part 2: Security functional components;
  - CC Part 3: Security assurance components;
- and simply referred to as the Common Criteria or the CC into this candidate scheme;
- Common Methodology for Information Technology Security Evaluation, under its applicable ISO/IEC 18045 version or under its applicable version published on <https://www.commoncriteriaportal.org/cc/>, simply referred to as the CEM into this candidate scheme.

Certificates issued shall indicate which version/release of the CC and CEM have been used for the evaluation and certification.





# CORAL

## Cybersecurity standards


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



#### Standards in support of the CSA (EUCC)

- 13 references to ISO standards
- 9 standards from ISO/IEC JTC 1/SC 27

Reference	Title
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 18045	Information technology - Security techniques - Methodology for IT security evaluation
ISO/IEC 17000	Conformity assessment - Vocabulary and general principles
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services
ISO/IEC 17025	Testing and calibration laboratories
ISO/IEC 19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
ISO/IEC WD TS 23532-1	IT Security Techniques — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Testing and evaluation for ISO/IEC 15408
ISO/IEC 27001	Information technology - Security techniques - Information security management systems – Requirements
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management controls
ISO/IEC 27005	Information technology - Security techniques - Information security risk management
ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure
ISO/IEC 30111	Information technology - Security techniques - Vulnerability handling processes
ISO/IEC 7816-4	Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange



CYBERSECURITY CERTIFICATION  
V1.1.1 | MAY 2021

### 26. REFERENCES

CSA (Cybersecurity Act)  
REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

SOG-IS MRA  
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates VERSION 3.0, MANAGEMENT COMMITTEE, January 2010.

CCRA  
ARRANGEMENT on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

**REFERENCED STANDARDS**

Table 6: Standards references

Reference	Title
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 18045	Information technology - Security techniques - Methodology for IT security evaluation
ISO/IEC 17000	Conformity assessment - Vocabulary and general principles
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services
ISO/IEC 17025	Testing and calibration laboratories
ISO/IEC 19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
ISO/IEC WD TS 23532-1	IT Security Techniques — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Testing and evaluation for ISO/IEC 15408
ISO/IEC 27001	Information technology - Security techniques - Information security management systems – Requirements
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management controls
ISO/IEC 27005	Information technology - Security techniques - Information security risk management
ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure
ISO/IEC 30111	Information technology - Security techniques - Vulnerability handling processes
ISO/IEC 7816-4	Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

76



# CORAL

## Cybersecurity standards

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



#### Standards in support of the CSA (EUCS)

The scheme relies on a number of standards and technical specifications:

- International standards ISO/IEC 17788 and ISO/IEC 17000, and to a lesser extent ISO/IEC 9000 and ISO/IEC 27000, are being used as references for the terminology used through the scheme, with input from all the schemes listed below when required.
- The security controls used in the scheme, together with the associated security requirements, are defined in an Annex of the present scheme (see Annex A.: Security Objectives and requirements for Cloud Services), and they are based on international standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and on documents previously issued by Member States to define the security controls in their respective National Schemes [C5, SecNumCloud].
- The definition of the assurance levels reuses some concepts defined in the ISO/IEC 15408-3 standard.
- The conformity assessment methodology defined in the scheme is based on the ISO/IEC 17065 international standard.

The scheme also leverages several security assessment methods and standards:

- International standards ISO/IEC 17021 and ISO/IEC 27006.
- International auditing standards ISAE3402 and ISAE3000.
- One method defined in an Annex to the present scheme (see Annex D.: Assessment for level Basic).

The security controls and other annexes also reference a number of standards:

- The ISO/IEC 29147 and ISO/IEC 30111 standards are referenced about vulnerability handling
- The ISO/IEC 27005 standard is referenced about risk management





# CORAL

## Cybersecurity standards

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



#### Standards in support of the CSA (EUCS)

- 22 references to ISO standards
- 11 standards from ISO/IEC JTC 1/SC 27

 EUCS – CLOUD SERVICES SCHEME  
December 2023

## 26. REFERENCES

**STANDARDS AND TECHNICAL SPECIFICATIONS**

**ISO Standards**

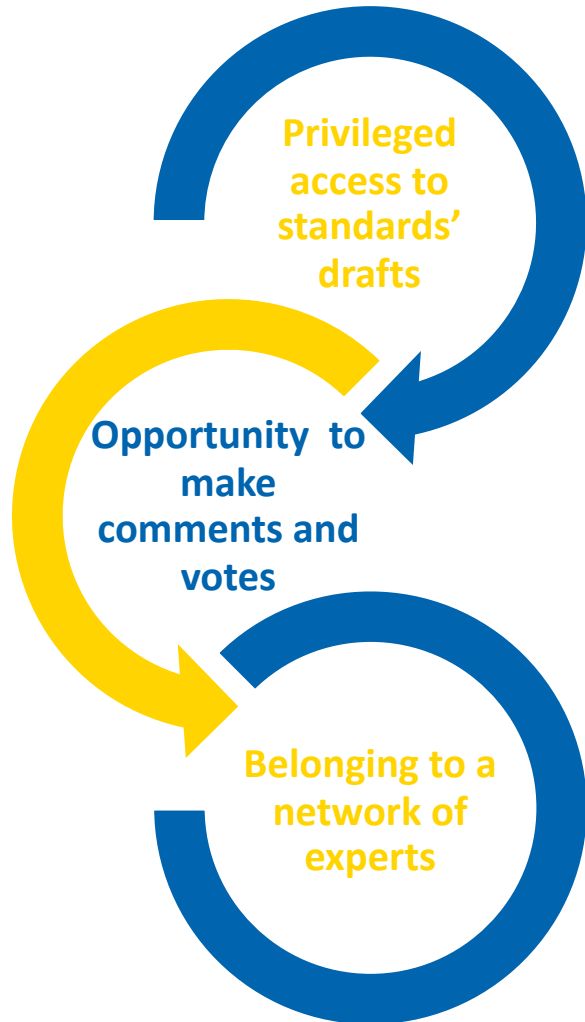
[ISO Supplement]	ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedures specific to ISO (in particular, Annex SL)
[ISO Guide 73]	ISO Guide 73:2009, Risk management — Vocabulary
[ISO9000]	ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
[ISO15408-3]	ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
[ISO17000]	ISO/IEC 17000:2020, Conformity assessment — Vocabulary and general principles.
[ISO17021]	ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
[ISO17025]	ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories
[ISO17029]	ISO/IEC 17029:2019, Conformity assessment — General principles and requirements for validation and verification bodies
[ISO17065]	ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services
[ISO17067]	ISO/IEC 17067:2013, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
[ISO17788]	ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary.
[ISO19011]	ISO 19011:2018, Guidelines for auditing management systems
[ISO20000-10]	ISO/IEC 20000-10:2018, Information technology — Service management — Part 10: Concepts and vocabulary
[ISO24765]	ISO/IEC/IEEE 24765:2017, Systems and software engineering — Vocabulary
[ISO27000]	ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[ISO27001]	ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
[ISO27002]	ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls
[ISO27005]	ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management
[ISO27006]	ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
[ISO27007]	ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
[ISO27017]	ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[ISO27032]	ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity
[ISO29147]	ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure
[ISO30111]	ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes

 79



**CORAL**

## Cybersecurity standards – Getting involved



- *Live monitoring of the development of standardization projects*
- *Analyze the ongoing projects*
- *Anticipate future rules and best practices*
  
- *Defend the interests of your business*
- *Spread and promote your innovations*
- *Value your know-how as best practices which could become a reference in the sector*
  
- *Learn about your competitors and their positions during the meetings*
- *Collaborate in order to defend common interests*
- *Promote your business and your competencies at national and international level*

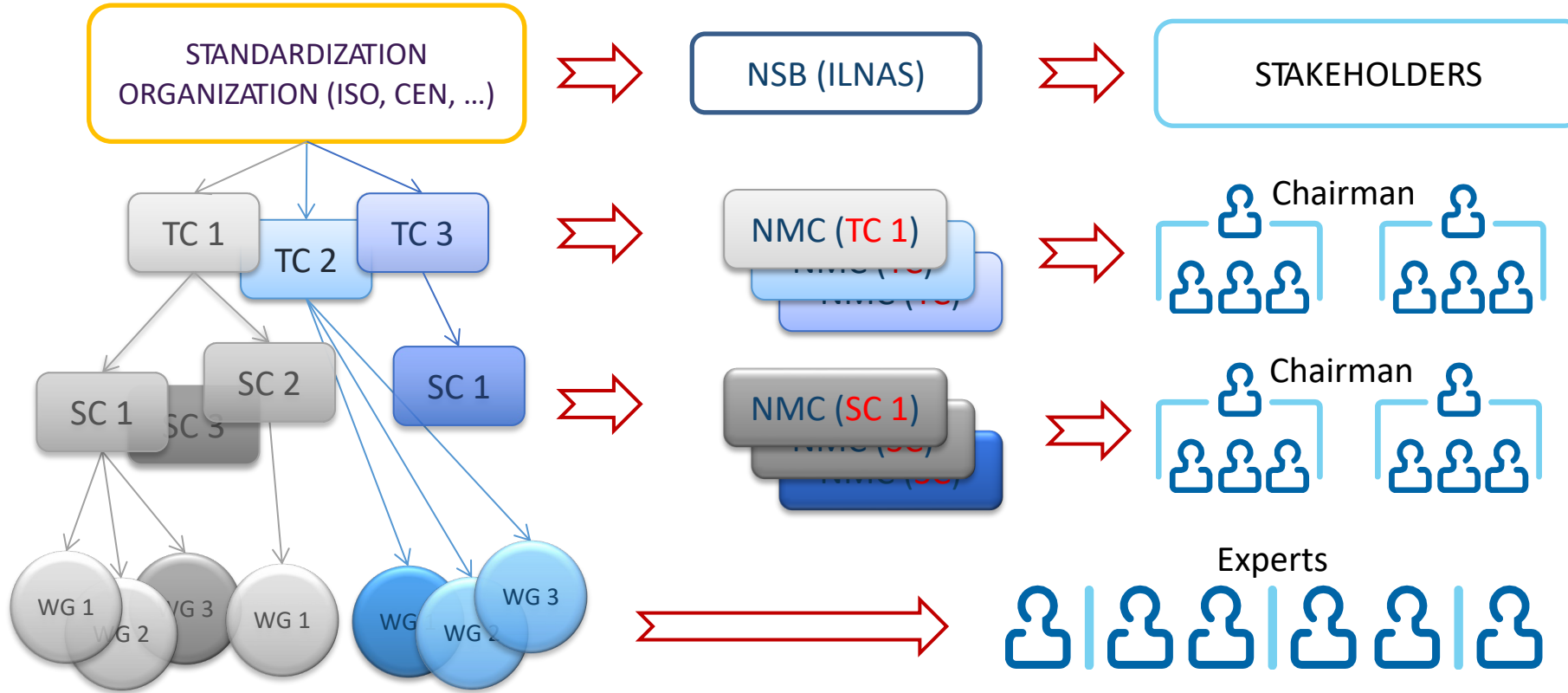






# CORAL

## Cybersecurity standards – Getting involved



NSB: National Standards Body

TC: Technical Committee

SC: Subcommittee - Entity established within a TC responsible for a large work program (focuses on an area of interest of the TC)

WG: Working Group - Group established by a TC or SC that develops standards project(s) within the scope of activity of the TC/SC

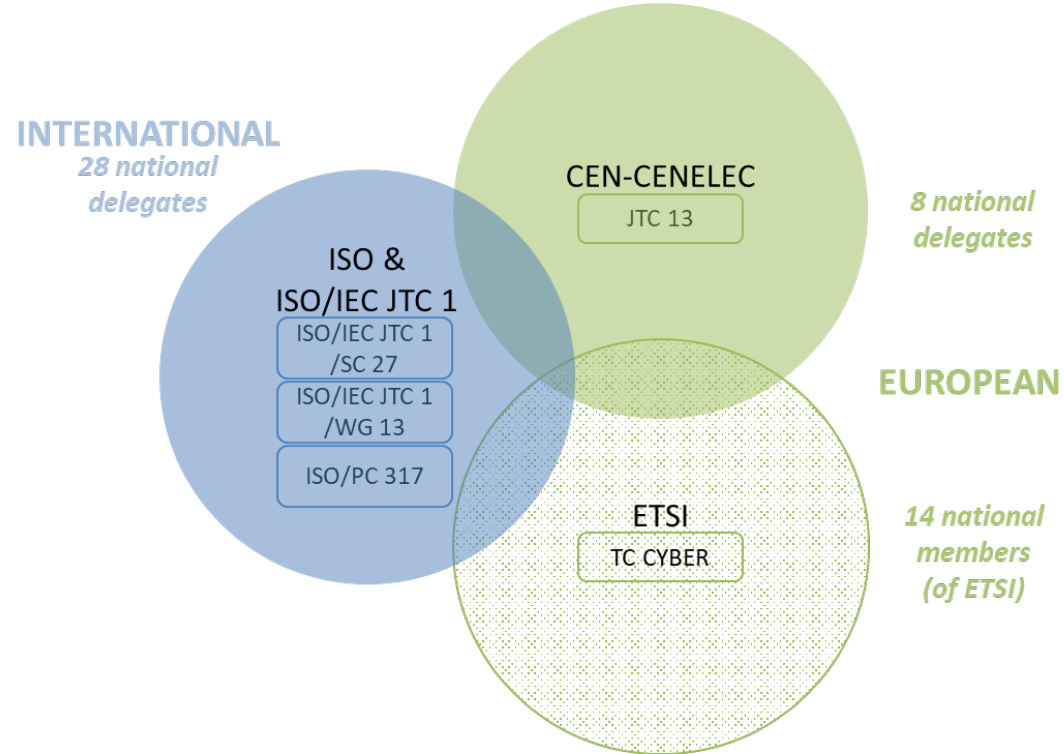
NMC: National Mirror Committee



# CORAL

## Cybersecurity standards – Getting involved

Multiple technical committees dealing with similar or complementary projects



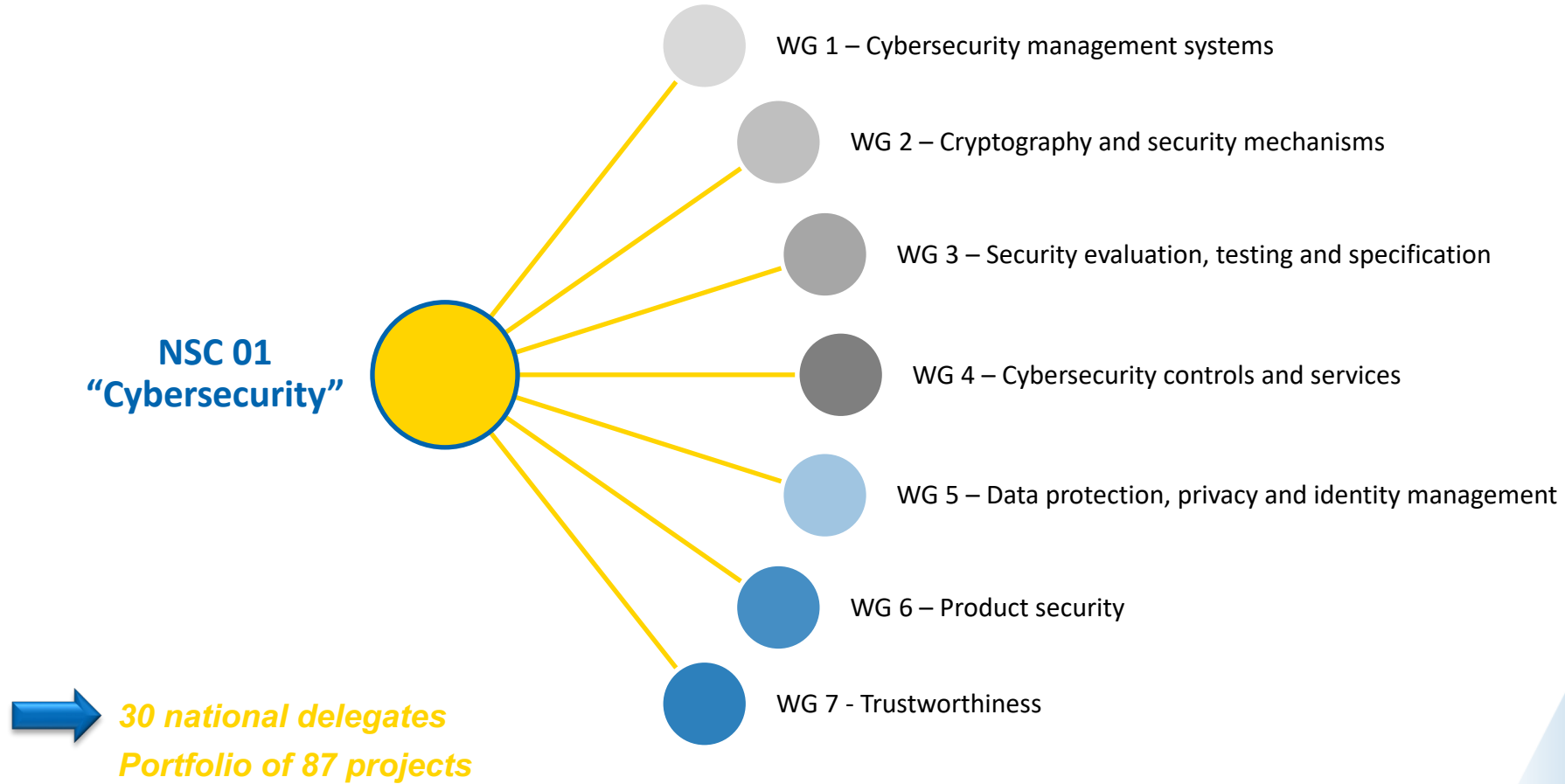
- *CEN/CLC/JTC 13 “Cybersecurity and Data Protection”*
- *ETSI/TC CYBER “Cybersecurity”*
- *ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection”*
- *ISO/IEC JTC 1/WG 13 “Trustworthiness”*
- *ISO/PC 317 “Consumer protection: privacy by design for consumer goods and services”*



**CORAL**

# Cybersecurity standards – Getting involved

National Standardization Commission (NSC 01) “Cybersecurity”





# CORAL

## Cybersecurity standards – Getting involved

### Who can participate ?

- *Every socio-economic actor with a certain expertise in the domain treated by the technical standardization committee*

### Application form for registration to a technical standardization committee

- *Form ILNAS/OLN/F001*
- Available on <https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html>

### National register of delegates

- 285 experts registered (September 2023)
- 1044 registrations in technical committees
- Link: <https://gd.lu/cCN7qg>

→ More information available on: <https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>



Registre national des délégués en normalisation - Septembre 2023

Nombre d'inscriptions aux comités techniques :	
ILNAS/OLN	97
CEN	261
CENELEC	12
CEN/CLC	53
CEN/CLC/ETSI	2
ECISS	0
ISO/IEC	313
ISO	295
IEC	11
Total	1044
Nombre de personnes inscrites : 285	

**ILNAS**

1, av du Swing - L-4367 Belvaux - Tél. : (+352) 24 77 43 40 - Fax : (+352) 24 79 43 40 - Email : normalisation@ilnas.etat.lu - www.portail-qualite.lu



**Project website:**

<https://coral-project.org/>

**Test Fit4CSA:**

<https://fit4csa.nc3.lu/survey/>

**Contacts:**

General: [coral@lhc.lu](mailto:coral@lhc.lu)

Dr. Gabriela Gheorghe (LHC): [gabriela.gheorghe@lhc.lu](mailto:gabriela.gheorghe@lhc.lu)

Ms. Natalia Vinogradova (ANEC GIE): [natalia.cassagnes@ilnas.etat.lu](mailto:natalia.cassagnes@ilnas.etat.lu)

Dr. Jean Lancrenon (ILNAS): [jean.lancrenon@ilnas.etat.lu](mailto:jean.lancrenon@ilnas.etat.lu)



Co-financed by the Connecting Europe Facility  
of the European Union