European Standardization Organizations

General Overview of Standards for Conformity Assessment in Cybersecurity

Dr. Walter Fumy, Chairperson CEN-CENELEC JTC 13

Preamble – Standards and Conformity Assessment

- Conformity assessment is the demonstration that specified **requirements** relating to a product, process, service, person, system or body are fulfilled.
- Demonstration may be undertaken by a manufacturer or supplier (first party), a user or purchaser (second party), or an **independent** body (third party).
- Conformity assessment activities can include testing, inspection, evaluation, examination, auditing, declarations, certification, accreditation, peer assessment, verification and validation.
- Mutual recognition agreements on conformity assessment are intended to reduce the costs of testing and certification in other markets.
- Note: In standards the verb **"shall"** indicates a requirement.
- Standards (and other normative SDO deliverables) that do not contain requirements (i.e. do not contain the verb "shall") are not intended to be used for conformity assessment.

Agenda

- Introduction to JTC 13
  - Scope
  - Structure
  - Cooperation
- Roadmap & Achievements
  - Pre-JTC 13
  - International Adoptions
  - Selected Project Highlights
- Activities of Other SDOs

© CEN-CENELEC 2023

CEN-CLC/JTC 13 Cybersecurity and Data Protection

- Joint technical committee (JTC) of CEN and CENELEC
- established November 2017
- 200+ European experts on cybersecurity and data protection
- (currently) 6 dedicated working groups
- 3 plenary meetings per year

- Chairperson: Walter Fumy, Bundesdruckerei (Germany)
- Secretariat: DIN German Institute of Standardization
- Secretary: Martin Uhlherr
- CEN-CENELEC Management Centre Programme Manager: Laurens Hernalsteen

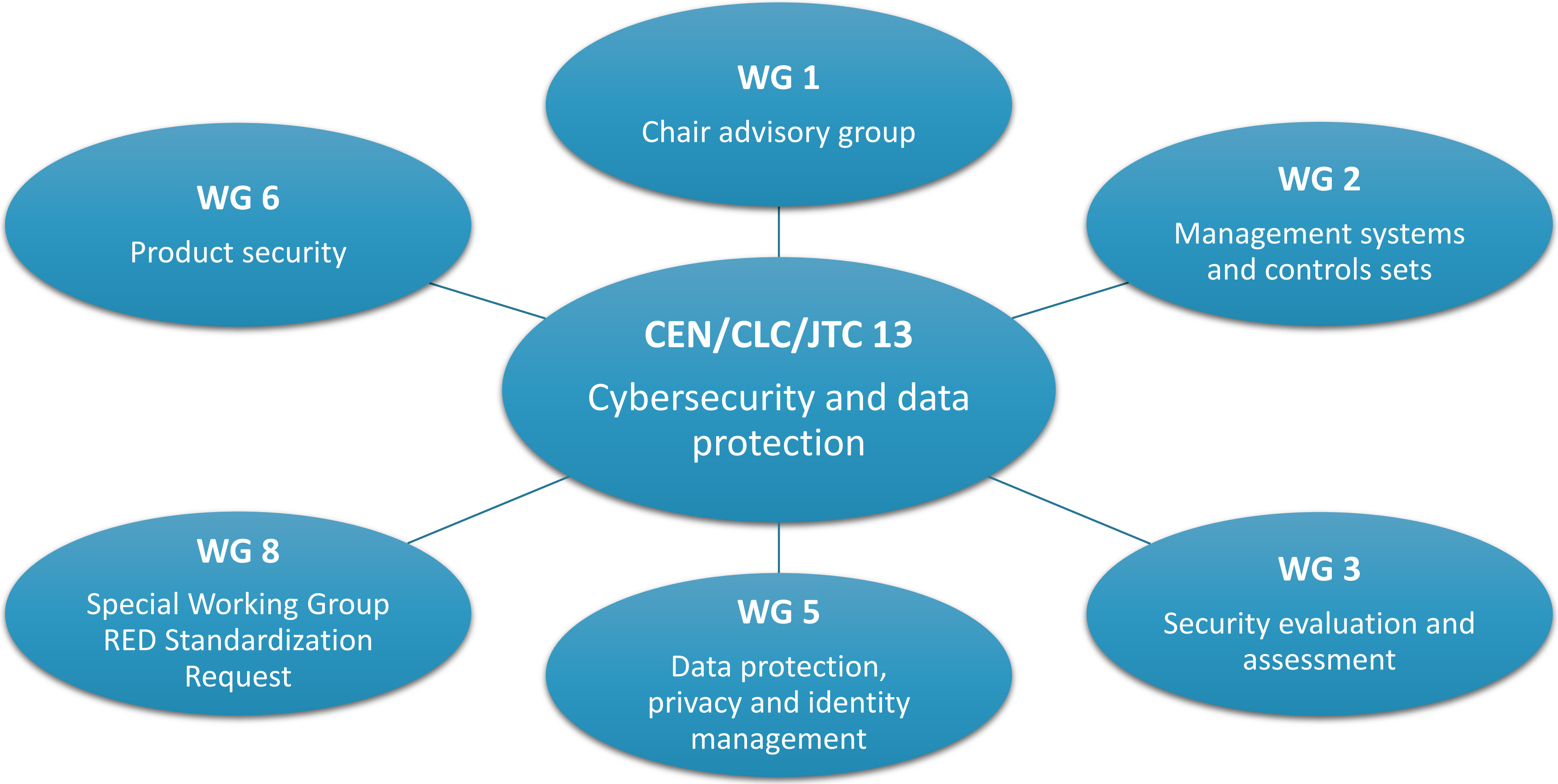
Scope

- Development of horizontal standards in the field of cybersecurity and data protection for vertical application domains such as ICT, eHealth, transport, smart cities, automotive, IoT, …
  - driven by European market needs
- Key areas of work
  - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices
  - Management systems, frameworks, methodologies
  - Data protection and privacy
  - Standards for security assessment and evaluation
  - Competence requirements in the area of cybersecurity and data protection

✓ Identification and adoption of documents published by ISO/IEC JTC 1, other SDOs, international bodies and industrial fora

✓ Development of specific CEN-CENELEC publications

Structure


WG 1
Chair advisory group
WG 6
Product security
WG 2
Management systems and controls sets
CEN/CLC/JTC 13
Cybersecurity and data protection
WG 8
Special Working Group RED Standardization Request
WG 5
Data protection, privacy and identity management
WG 3
Security evaluation and assessment

© CEN-CENELEC 2023

Selected Liaisons and Cooperations I

Standardization Committees

- CEN/CLC/ETSI/SMCG
  Smart Meter Coordination Group
- CEN/CLC/JTC 19
  Blockchain and DLT
- CEN/CLC/JTC 21
  Artificial Intelligence
- CEN/TC 224
  Machine-Readable Cards
- CEN/TC 301
  Road vehicles
- CEN/TC 377/WG 1
  Information security in air traffic management

- CLC/TC 65X
  Industrial-process measurement, control and automation
- CLC/TC 79
  Alarm Systems
- CLC/TC 205
  Home and Building Electronic Systems

- ETSI TC CYBER
- ISO/IEC JTC 1/SC 27
  Information security, cybersecurity and privacy protection

© CEN-CENELEC 2023

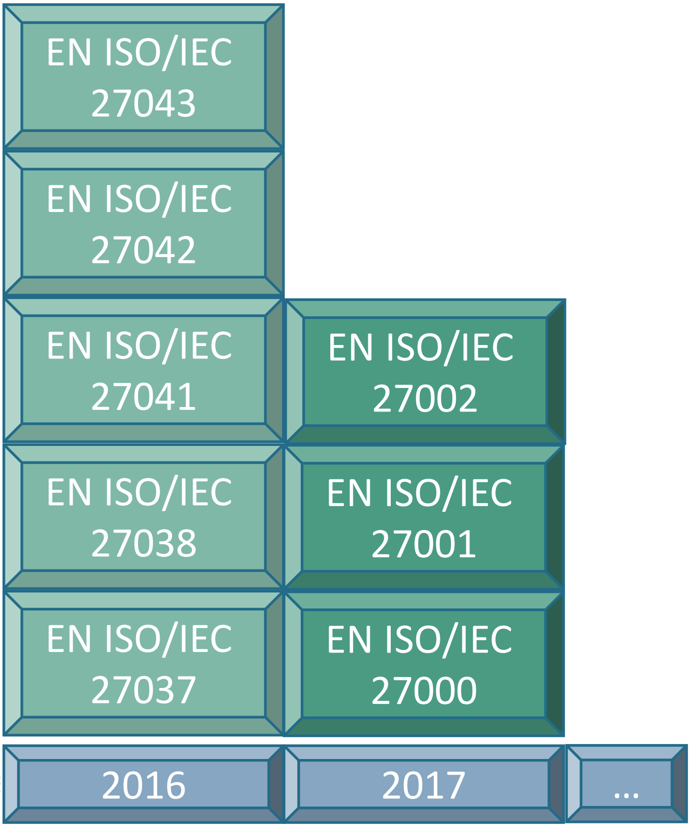
Agenda

- Introduction to JTC 13
  - Scope
  - Structure
  - Cooperation

- Roadmap & Achievements
  - Pre-JTC 13
  - International Adoptions
  - Selected Project Highlights

- Activities of Other SDOs

Achievements – Pre JTC 13

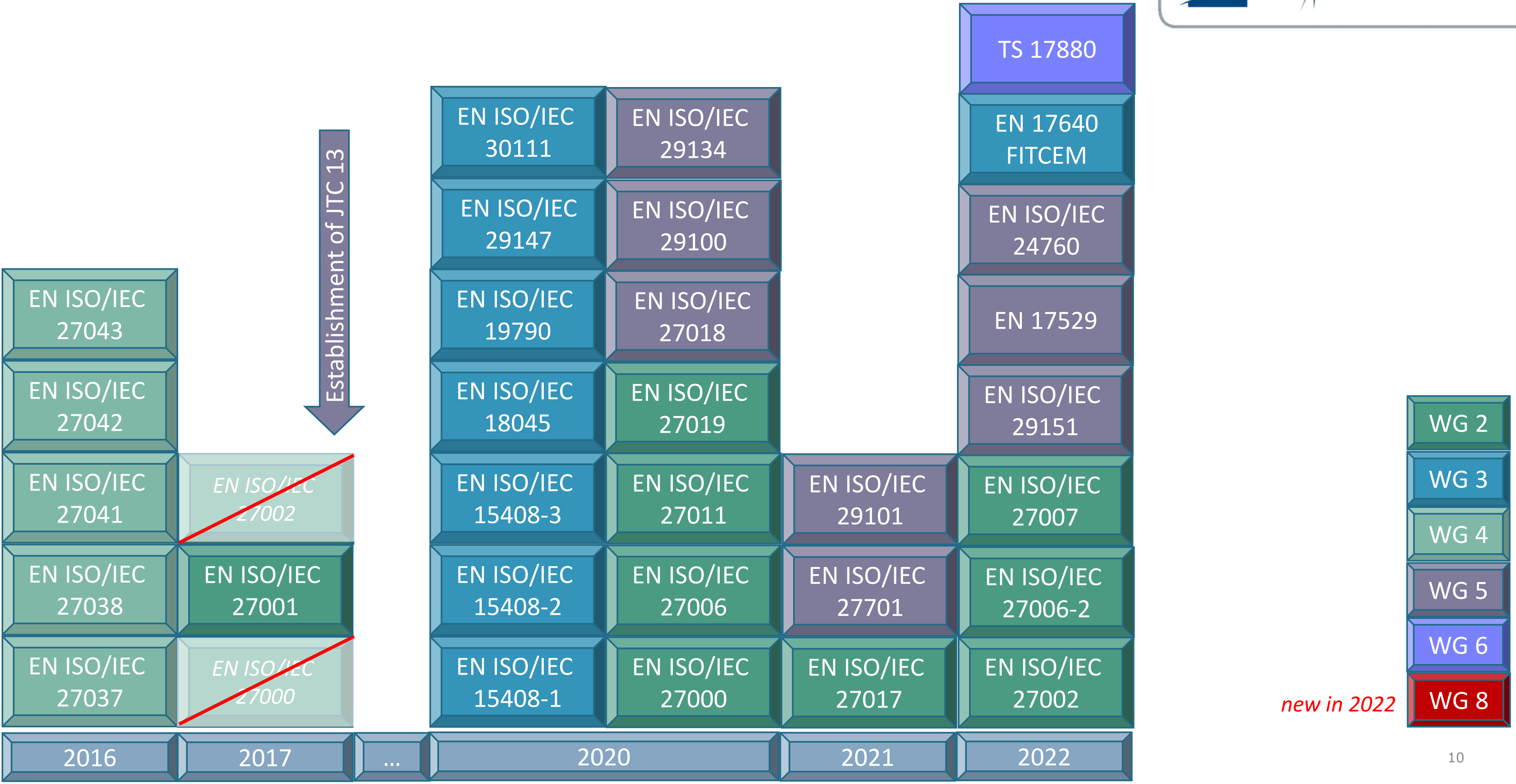


2016	2017	…
EN ISO/IEC 27043		
EN ISO/IEC 27042		
EN ISO/IEC 27041	EN ISO/IEC 27002	
EN ISO/IEC 27038	EN ISO/IEC 27001	
EN ISO/IEC 27037	EN ISO/IEC 27000	

Before JTC 13 was created in November 2017, the *CEN-CENELEC Focus Group on Cybersecurity* has orchestrated the **adoption of international cybersecurity standards** for supporting the EU Digital Single Market.

CEN-CLC/JTC 13

Achievements



2016

EN ISO/IEC 27043

EN ISO/IEC 27042

EN ISO/IEC 27041

EN ISO/IEC 27038

EN ISO/IEC 27037

2017

~~EN ISO/IEC 27002~~

EN ISO/IEC 27001

~~EN ISO/IEC 27000~~

Establishment of JTC 13

…

2020

EN ISO/IEC 30111

EN ISO/IEC 29147

EN ISO/IEC 19790

EN ISO/IEC 18045

EN ISO/IEC 15408-3

EN ISO/IEC 15408-2

EN ISO/IEC 15408-1

EN ISO/IEC 29134

EN ISO/IEC 29100

EN ISO/IEC 27018

EN ISO/IEC 27019

EN ISO/IEC 27011

EN ISO/IEC 27006

EN ISO/IEC 27000

2021

EN ISO/IEC 29101

EN ISO/IEC 27701

EN ISO/IEC 27017

2022

TS 17880

EN 17640 FITCEM

EN ISO/IEC 24760

EN 17529

EN ISO/IEC 29151

EN ISO/IEC 27007

EN ISO/IEC 27006-2

EN ISO/IEC 27002

WG 2

WG 3

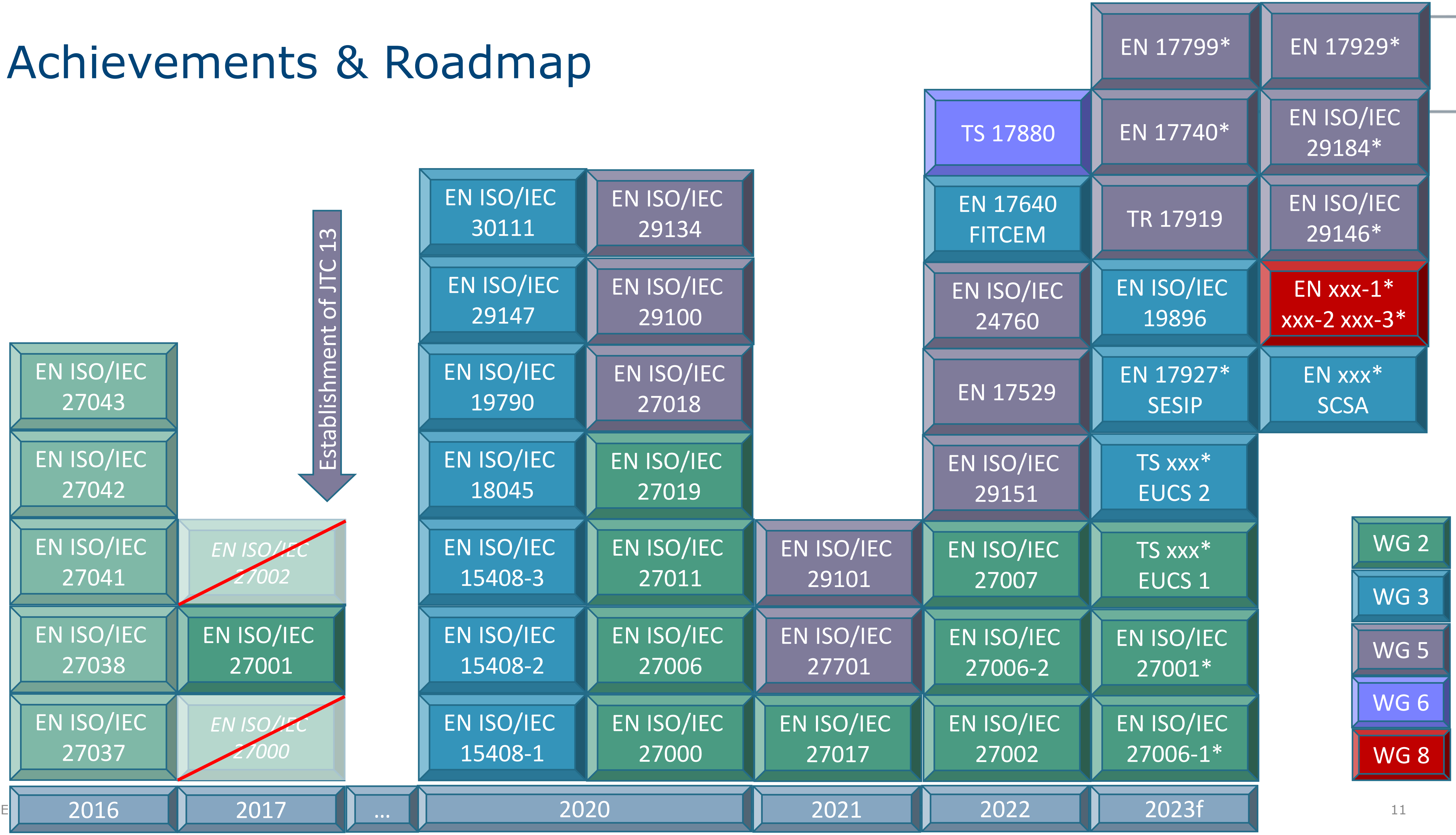
WG 4

WG 5

WG 6

new in 2022 WG 8

Achievements & Roadmap



Establishment of JTC 13

2016
- EN ISO/IEC 27043
- EN ISO/IEC 27042
- EN ISO/IEC 27041
- EN ISO/IEC 27038
- EN ISO/IEC 27037

2017
- ~~EN ISO/IEC 27002~~
- EN ISO/IEC 27001
- ~~EN ISO/IEC 27000~~

…

2020
- EN ISO/IEC 30111
- EN ISO/IEC 29147
- EN ISO/IEC 19790
- EN ISO/IEC 18045
- EN ISO/IEC 15408-3
- EN ISO/IEC 15408-2
- EN ISO/IEC 15408-1
- EN ISO/IEC 29134
- EN ISO/IEC 29100
- EN ISO/IEC 27018
- EN ISO/IEC 27019
- EN ISO/IEC 27011
- EN ISO/IEC 27006
- EN ISO/IEC 27000

2021
- EN ISO/IEC 29101
- EN ISO/IEC 27701
- EN ISO/IEC 27017

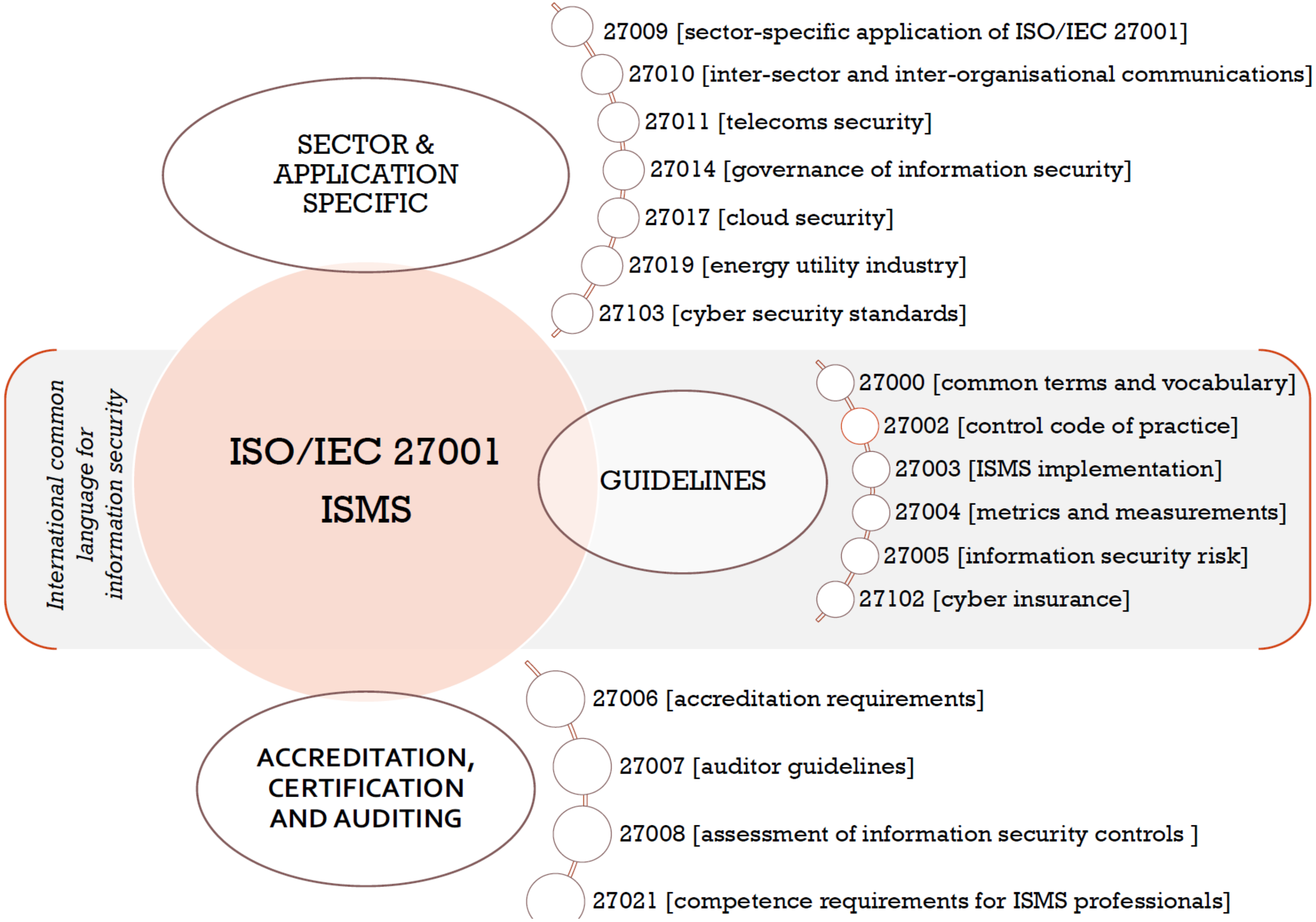
2022
- TS 17880
- EN 17640 FITCEM
- EN ISO/IEC 24760
- EN 17529
- EN ISO/IEC 29151
- EN ISO/IEC 27007
- EN ISO/IEC 27006-2
- EN ISO/IEC 27002

2023f
- EN 17799*
- EN 17740*
- TR 17919
- EN ISO/IEC 19896
- EN 17927* SESIP
- TS xxx* EUCS 2
- TS xxx* EUCS 1
- EN ISO/IEC 27001*
- EN ISO/IEC 27006-1*
- EN 17929*
- EN ISO/IEC 29184*
- EN ISO/IEC 29146*
- EN xxx-1* xxx-2 xxx-3*
- EN xxx* SCSA

- WG 2
- WG 3
- WG 5
- WG 6
- WG 8

ISO/IEC 27000 Family of ISMS Standards

WG 1 ISMS standards


SECTOR & APPLICATION SPECIFIC
International common language for information security
ISO/IEC 27001 ISMS
GUIDELINES
ACCREDITATION, CERTIFICATION AND AUDITING

27009 [sector-specific application of ISO/IEC 27001]

27010 [inter-sector and inter-organisational communications]

27011 [telecoms security]

27014 [governance of information security]

27017 [cloud security]

27019 [energy utility industry]

27103 [cyber security standards]

27000 [common terms and vocabulary]

27002 [control code of practice]

27003 [ISMS implementation]

27004 [metrics and measurements]

27005 [information security risk]

27102 [cyber insurance]

27006 [accreditation requirements]

27007 [auditor guidelines]

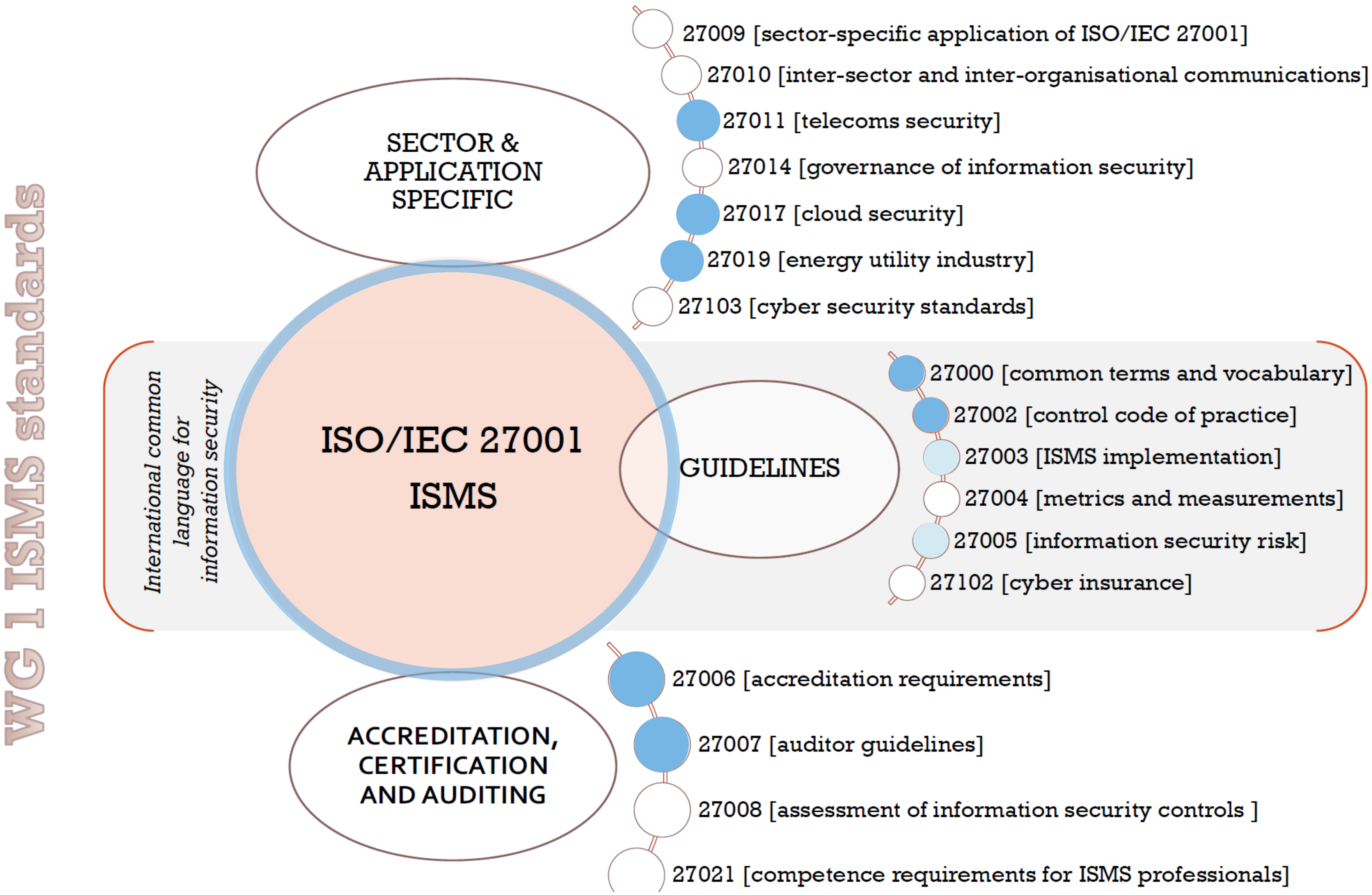
27008 [assessment of information security controls]

27021 [competence requirements for ISMS professionals]

Source: ISO/IEC SC 27/WG 1

©

EN ISO/IEC 27000 Subset of ISMS Standards



WG 1 ISMS standards

ISO/IEC 27001 ISMS

International common language for information security

SECTOR & APPLICATION SPECIFIC

- ○ 27009 [sector-specific application of ISO/IEC 27001]
- ○ 27010 [inter-sector and inter-organisational communications]
- ● 27011 [telecoms security]
- ○ 27014 [governance of information security]
- ● 27017 [cloud security]
- ● 27019 [energy utility industry]
- ○ 27103 [cyber security standards]

GUIDELINES

- ● 27000 [common terms and vocabulary]
- ● 27002 [control code of practice]
- ◌ 27003 [ISMS implementation]
- ○ 27004 [metrics and measurements]
- ◌ 27005 [information security risk]
- ○ 27102 [cyber insurance]

ACCREDITATION, CERTIFICATION AND AUDITING

- ● 27006 [accreditation requirements]
- ● 27007 [auditor guidelines]
- ○ 27008 [assessment of information security controls]
- ○ 27021 [competence requirements for ISMS professionals]

● *adopted as EN*

◌ *adoption initiated*

EN ISO/IEC 27002 –
93 Requirements and Controls in 4 Categories

37
Organizational controls

1: Policies for information security
2: Information security roles and responsibilities
3: Segregation of duties
4: Management responsibilities
[…]
7: Threat intelligence
8: Information security in project management
9: Inventory of information and other associated assets
[…]

8
People controls

1: Screening
[…]
3: Information security awareness training
4: Disciplinary process
5: Responsibilities after termination
[…]

14
Physical controls

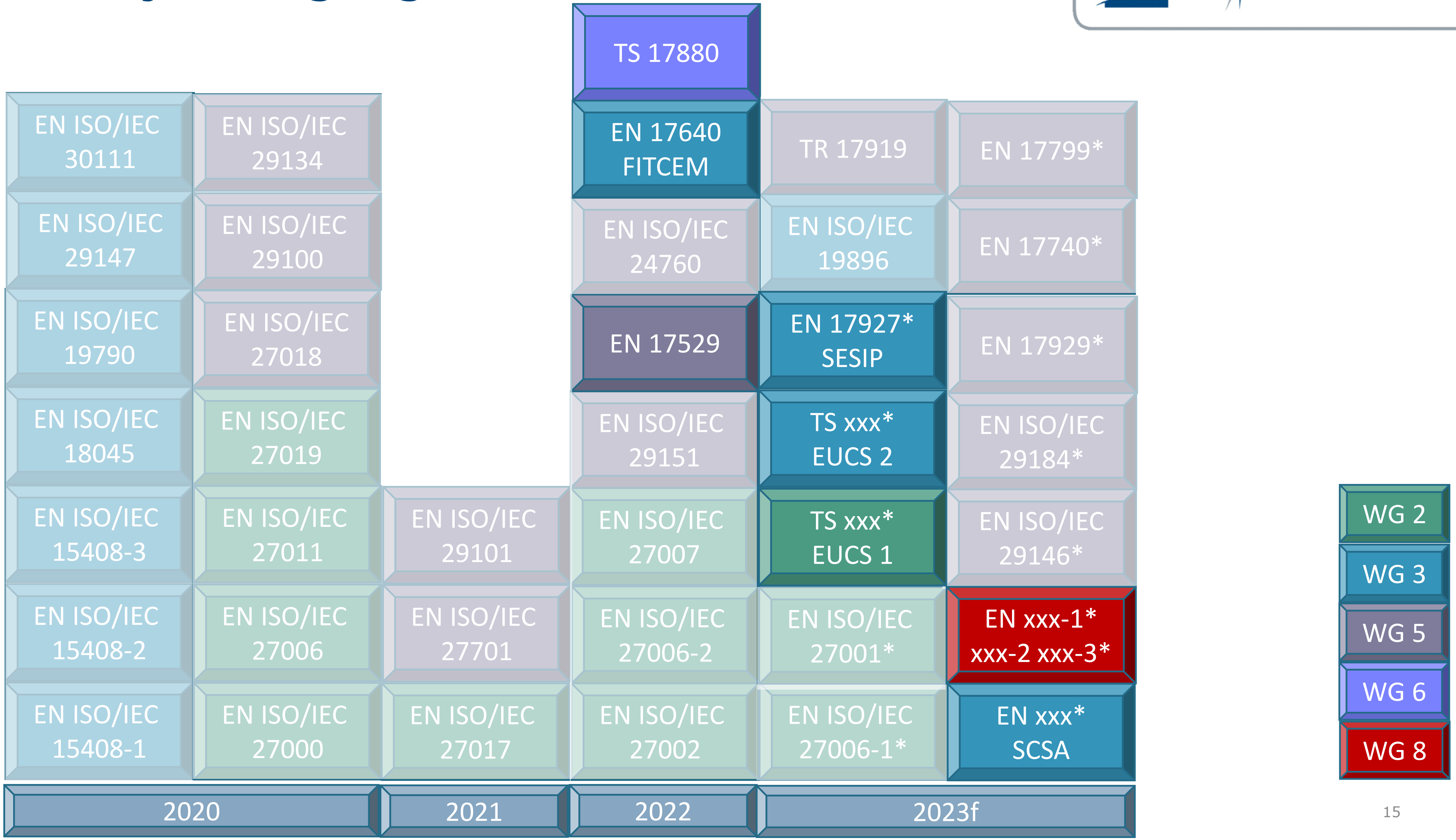
1: Physical security perimeters
2: Physical entry
3: Securing offices, rooms and facilities
4: Physical security monitoring
[…]

34
Technological controls

[…]
20: Networks security
21: Security of network services
22: Segregation of networks
23: Web filtering
24: Use of cryptography
25: Secure development life cycle
26: Application security requirements
[…]

CEN-CLC/JTC 13

Selected Project Highlights



			TS 17880		
EN ISO/IEC 30111	EN ISO/IEC 29134		EN 17640 FITCEM	TR 17919	EN 17799*
EN ISO/IEC 29147	EN ISO/IEC 29100		EN ISO/IEC 24760	EN ISO/IEC 19896	EN 17740*
EN ISO/IEC 19790	EN ISO/IEC 27018		EN 17529	EN 17927* SESIP	EN 17929*
EN ISO/IEC 18045	EN ISO/IEC 27019		EN ISO/IEC 29151	TS xxx* EUCS 2	EN ISO/IEC 29184*
EN ISO/IEC 15408-3	EN ISO/IEC 27011	EN ISO/IEC 29101	EN ISO/IEC 27007	TS xxx* EUCS 1	EN ISO/IEC 29146*
EN ISO/IEC 15408-2	EN ISO/IEC 27006	EN ISO/IEC 27701	EN ISO/IEC 27006-2	EN ISO/IEC 27001*	EN xxx-1* xxx-2 xxx-3*
EN ISO/IEC 15408-1	EN ISO/IEC 27000	EN ISO/IEC 27017	EN ISO/IEC 27002	EN ISO/IEC 27006-1*	EN xxx* SCSA
2020		2021	2022	2023f	

WG 2

WG 3

WG 5

WG 6

WG 8

EU Cybersecurity Act (CSA)

Certification framework includes

- EUCC: Common Criteria based European Cybersecurity Certification
  - Successor of EU national schemes operating under the SOG-IS* Mutual Recognition Agreement
  - Based on (EN) ISO/IEC 15408, (EN) ISO/IEC 18045, ISO/IEC 17065, …
- EUCS: Cloud Services Scheme
  - Standards under development: EUCS1 [WG 2], EUCS2 [WG 3]
  - ISO/IEC 22123: Cloud Computing [ISO/IEC JTC 1/SC 38]
- EU5G: 5G Cybersecurity Certification Scheme
  - JTC 13 adhoc group („WG 7“) under supervision of JTC 13/WG 1
- Guidelines on a sectoral cybersecurity assessment (WG 3, under development)

see also Eric Vetillard presentation

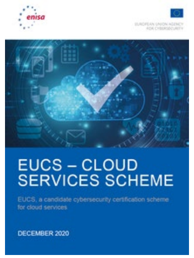
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBERSECURITY CERTIFICATION

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS

V1.1.1 | MAY 2021



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

*) Senior Officials Group - Information Security

EN 17640:2022 - FITCEM

FIxed Time Cybersecurity Evaluation Methodology for ICT products

- flexible methodology comprised of different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA
- designed for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial, high)
- methodology may be applied to both 3rd party evaluation and self-assessment

- p.k.a. „lightweight" evaluation methodology

- Status: Published
  Amendmend under drafting

CEN/CLC TS 17880:2022

Protection Profile for Smart Meter - Minimum Security Requirements

- TOE: Smart supply meter that monitors, and possibly limits, the consumption of electricity, gas, thermal energy or water and communicates with users via local and network interfaces.
- The meter's basic security tasks include to ensure
  - the integrity of its content,
  - the authenticity and integrity of instructions that it acts on,
  - the confidentiality of data used to provide security functions (such as keys), and
  - the confidentiality of sensitive personal and personally identifiable information.
- Further, the meter firmware has to be protected from tampering by a firmware integrity test, and by a secure firmware update.
- Evaluation assurance level EAL3+

- *Based on TR developed and published 2019 by CEN/CENELEC/ETSI Coordination Group on Smart Meters*

© CEN-CENELEC 2023

Special WG RED Standardisation Request

- established July 2022
- to develop the harmonised standards as requested by the Commission Implementing Decision on a standardisation request to CEN and CENELEC as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.

Three approved WG 8 projects:

- NWI Common security requirements for internet connected radio equipment
- NWI Common security requirements for radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- NWI Common security requirements for internet connected radio equipment processing virtual money or monetary value

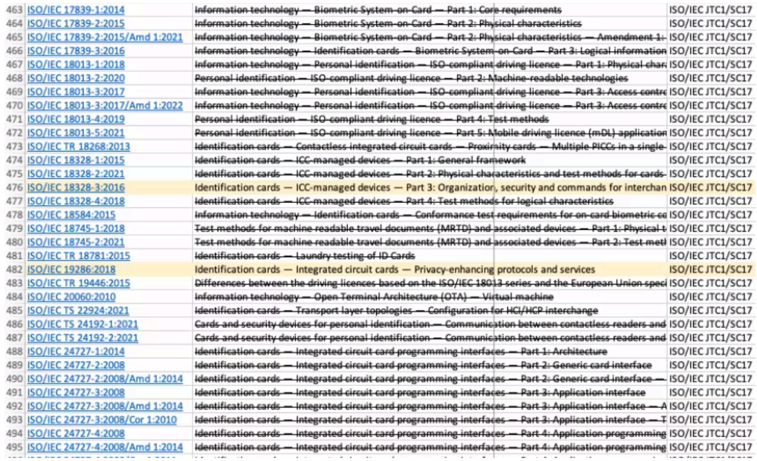
See Samim Ahmadi presentation

EU Cyber Resilience Act (CRA)

- Cybersecurity requirements for placing hardware and/or software on the market
  - Obligations for manufacturers, distributors and importers across the product life cycle
  - Conformity assessment based on risk level (non-critical, critical, or highly critical)

- Applies to „products with digital elements" and includes remote data processing solutions
  - Not covered: non-commercial projects, services, products regulated elsewhere (e.g., cars, medical devices, …)

- Need for standards includes essential requirements, evaluation methodologies, accreditation of conformaty assessment bodies
  - ESOs (and JRC/ENISA) have started preparatory work
    - Mapping of existing standards, gap analysis
  - *new:* JTC 13 decided to establish a Special WG on the CRA



463	ISO/IEC 17839-1:2014	~~Information technology — Biometric System-on-Card — Part 1: Core requirements~~	ISO/IEC JTC1/SC17
464	ISO/IEC 17839-2:2015	~~Information technology — Biometric System-on-Card — Part 2: Physical characteristics~~	ISO/IEC JTC1/SC17
465	ISO/IEC 17839-2:2015/Amd 1:2021	~~Information technology — Biometric System-on-Card — Part 2: Physical characteristics — Amendment 1:~~	ISO/IEC JTC1/SC17
466	ISO/IEC 17839-3:2016	~~Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information~~	ISO/IEC JTC1/SC17
467	ISO/IEC 18013-1:2018	~~Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical chara~~	ISO/IEC JTC1/SC17
468	ISO/IEC 18013-2:2020	~~Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies~~	ISO/IEC JTC1/SC17
469	ISO/IEC 18013-3:2017	~~Information technology — Personal identification — ISO-compliant driving licence — Part 3: Access contre~~	ISO/IEC JTC1/SC17
470	ISO/IEC 18013-3:2017/Amd 1:2022	~~Information technology — Personal identification — ISO-compliant driving licence — Part 3: Access contre~~	ISO/IEC JTC1/SC17
471	ISO/IEC 18013-4:2019	~~Personal identification — ISO-compliant driving licence — Part 4: Test methods~~	ISO/IEC JTC1/SC17
472	ISO/IEC 18013-5:2021	~~Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application~~	ISO/IEC JTC1/SC17
473	ISO/IEC TR 18268:2013	~~Identification cards — Contactless integrated circuit cards — Proximity cards — Multiple PICCs in a single-~~	ISO/IEC JTC1/SC17
474	ISO/IEC 18328-1:2015	~~Identification cards — ICC-managed devices — Part 1: General framework~~	ISO/IEC JTC1/SC17
475	ISO/IEC 18328-2:2021	~~Identification cards — ICC-managed devices — Part 2: Physical characteristics and test methods for cards-~~	ISO/IEC JTC1/SC17
476	ISO/IEC 18328-3:2016	Identification cards — ICC-managed devices — Part 3: Organization, security and commands for interchan	ISO/IEC JTC1/SC17
477	ISO/IEC 18328-4:2018	~~Identification cards — ICC-managed devices — Part 4: Test methods for logical characteristics~~	ISO/IEC JTC1/SC17
478	ISO/IEC 18584:2015	~~Information technology — Identification cards — Conformance test requirements for on-card biometric co~~	ISO/IEC JTC1/SC17
479	ISO/IEC 18745-1:2018	~~Test methods for machine readable travel documents (MRTD) and associated devices — Part 1: Physical t~~	ISO/IEC JTC1/SC17
480	ISO/IEC 18745-2:2021	~~Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test metl~~	ISO/IEC JTC1/SC17
481	ISO/IEC TR 18781:2015	~~Identification cards — Laundry testing of ID Cards~~	ISO/IEC JTC1/SC17
482	ISO/IEC 19286:2018	Identification cards — Integrated circuit cards — Privacy-enhancing protocols and services	ISO/IEC JTC1/SC17
483	ISO/IEC TR 19446:2015	~~Differences between the driving licences based on the ISO/IEC 18013 series and the European Union speci~~	ISO/IEC JTC1/SC17
484	ISO/IEC 20060:2010	~~Information technology — Open Terminal Architecture (OTA) — Virtual machine~~	ISO/IEC JTC1/SC17
485	ISO/IEC TS 22924:2021	~~Identification cards — Transport layer topologies — Configuration for HCI/HCP interchange~~	ISO/IEC JTC1/SC17
486	ISO/IEC TS 24192-1:2021	~~Cards and security devices for personal identification — Communication between contactless readers and~~	ISO/IEC JTC1/SC17
487	ISO/IEC TS 24192-2:2021	~~Cards and security devices for personal identification — Communication between contactless readers and~~	ISO/IEC JTC1/SC17
488	ISO/IEC 24727-1:2014	~~Identification cards — Integrated circuit card programming interfaces — Part 1: Architecture~~	ISO/IEC JTC1/SC17
489	ISO/IEC 24727-2:2008	~~Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface~~	ISO/IEC JTC1/SC17
490	ISO/IEC 24727-2:2008/Amd 1:2014	~~Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface —~~	ISO/IEC JTC1/SC17
491	ISO/IEC 24727-3:2008	~~Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface~~	ISO/IEC JTC1/SC17
492	ISO/IEC 24727-3:2008/Amd 1:2014	~~Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface — A~~	ISO/IEC JTC1/SC17
493	ISO/IEC 24727-3:2008/Cor 1:2010	~~Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface — T~~	ISO/IEC JTC1/SC17
494	ISO/IEC 24727-4:2008	~~Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming~~	ISO/IEC JTC1/SC17
495	ISO/IEC 24727-4:2008/Amd 1:2014	~~Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming~~	ISO/IEC JTC1/SC17

© CEN-CENELEC 2023

CEN-CLC/JTC 13

CRA: Obligations of manufacturers

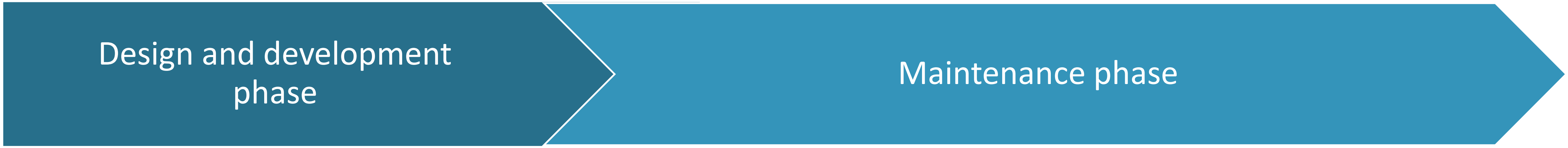
Assessment of risks associated with product

Product-related essential requirements (Annex I.1)
Vulnerability handling essential requirements (Annex I.2)
Documentation requirements (Annex II+V)

Non-critical	Critical Class I	Critical Class II
Word processing Smart speakers Hard drives	Microcontrollers Firewalls Password managers	CPUs Secure elements Operating systems

Annex III product class examples

Declaration of conformity (Annex IV)
- Unclassified products: self-assessment
- Class I products: application of a standard or third-party assessment
- Class II products: third-party assessment



Design and development phase

Maintenance phase

Reporting obligations
- Exploited vulnerabilities
- Incident reporting

© CEN-CENELEC 2023

Agenda

- Introduction to JTC 13
  - Scope
  - Structure
  - Cooperation

- Roadmap & Achievements
  - Pre-JTC 13
  - International Adoptions
  - Selected Project Highlights

- Some Activities of Other SDOs

© CEN-CENELEC 2023

ETSI EN 303 645:2020 – Cybersecurity provisions for consumer IoT

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimise exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data
- Data protection provisions for consumer IoT

- Must implement all 33 requirements (some conditional)
- Should make best effort to implement all 35 recommendations (some conditional)
- Must record rationale if a recommendation is not implemented
- ETSI TR 103 621:2022 provides further guidance

CLC/TC 65X

EN IEC 62443-4-2:2019 – Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

- EN IEC 62443-4-2 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in EN IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component).
- Foundational requirements are
  a) identification and authentication control,
  b) use control,
  c) system integrity,
  d) data confidentiality,
  e) restricted data flow,
  f) timely response to events, and
  g) resource availability.

Targeted Security Level / Protection against …	
SL-1	casual or coincidental violation
SL-2	intentional violation using simple means, low resources, generic skills, low motivation
SL-3	intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL-4	intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

- Defining security capability levels based on these seven FRs for IACS components is the main goal and objective of EN IEC 62443-4-2.

© CEN-CENELEC 2023

Conclusion

- “The good news about (cybersecurity) standards is …
  … there are so many to choose from”   ☺ ☺ ☺

- Conformity to relevant standards, regulations and other specifications underpins trust, confidence and assurance in cybersecurity and cyber eco-systems.

- Given the limited availability of resources for the development of cybersecurity standards, we must avoid duplication of effort and make use of effective cooperation and collaboration.

- Additional information on JTC 13
  - https://standards.cencenelec.eu/

© CEN-CENELEC 2023

Thank you for your kind attention!

Contact: walter.fumy@ry-cyber.de
martin.uhlherr@din.de
lhernalsteen@cencenelec.eu