FIRST ARTICLE OF LICORICE'S BLOG !

Led by Antonio Kung (Trialog), François Zamora (Orange), and Jean Caire (RATP)

The Evolution of Standardization in Cybersecurity

This document was initiated by Antonio Kung (FR – Trialog), François Zamora (FR – Orange), and Jean Caire (FR – RATP), following the publication of a French paper by SEE in October 2024. Building on discussions with Norbert Bensalem (FR, JTC 1 SIF facilitator), the French national body has graciously made it available to ISO/IEC JTC 1/SC 27. Through LICORICE, the document is now accessible to a broader international audience, showcasing the bridge that LICORICE has built as one of the project's key achievements.

The paper offers a comprehensive overview of existing standards, both at the domain and conformance assessment levels.

Cybersecurity for Information and Communication Technologies (ICT)

Standardization of cybersecurity for ICT mainly managed by the ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) committee1. The committed includes five main working groups:

WG1: Information security management systems | WG2: Cryptography and security mechanisms | WG3: Security evaluation, testing and specifications | WG4: Security Controls and Services | WG5: Identity management and privacy technologies

SC 27 has published 253 standards, and is currently developing 74 standards. While it is not possible to describe all of them, we can cluster them according to the following topics:

Standards on organizational aspects of information security management systems, with ISO/IEC 27001 on requirements, ISO/IEC 27002 on information security measures, or ISO/IEC 27005 on recommendations for risk management linked to information security information.
Standards on organizational aspects of related to life cycles, with ISO/IEC 27110 on the development of cybersecurity frameworks, the ISO/IEC 27035 series on incident management, or ISO/IEC 6114 on security considerations throughout the product life cycle.
Standards on technology such as

- Blockchains and distributed ledger technologies (DLT), with ISO/IEC 23249 on identity management mechanisms using DLTs, ISO/IEC 23649 on trust anchors in DLT-based identity management systems, ISO/IEC 23244 and ISO/IEC 24946 on privacy, and ISO/IEC 25126 on security controls for DLTs.
- Internet of Things, with ISO/IEC 27400 on security and privacy guidelines, ISO/IEC 27402 on baseline device requirements, ISO/IEC 27403 on IoT domotics, or ISO/IEC 27404 on a framework for cybersecurity labels of consumer products.
- Artificial intelligence with ISO/IEC 27563 on use cases, ISO/IEC 27090 on security, ISO/IEC 27091 on privacy.

The SC27 is also responsible for standards on privacy. We can also present them according to similar topics:

Standards on essential aspects with ISO/IEC 29100 which describes the principles, and ISO/IEC 29134 which provides the guidelines for the privacy impact study.
Standards on organizational aspects of privacy management systems, with ISO/IEC 27701 on requirements and guidelines.

[1] https://www.iso.org/committee/45306.html

Standards on operational aspects relating to privacy engineering, often called "privacy-by-design", with the ISO 31700 series on requirements for consumer products, the ISO/IEC 27550 on the life cycle, the ISO/IEC 27561 on the operationalization of the principles, or ISO/IEC 27564 on recommendations on the use of models. Further note that the creation of a new committee, ISO/IEC JTC 1/SC44 (consumer protection in the field of privacy-by-design) which is taking over the ISO 31700 series.
Standards on data de-identification such as ISO/IEC 20889 (terminology and classification of data de-identification techniques for the protection of privacy) or ISO/IEC 27559 (Framework for data de-identification for the protection of privacy).
Standards on consent and preference management with ISO/IEC 29184 (notices on privacy protection and online consent) or ISO/IEC 27556 (user-centered framework for managing privacy preferences).
Finally, we will cite the standards relating to age assurance like ISO/IEC 27566 which can be used for instance to help protect minors from adult sites.

Cybersecurity in Vertical Domains

While ICT cybersecurity standards can be considered as common to all vertical domain, they are not sufficient. This is why specific standards have been developed at the vertical level:

- In the industrial field, standards of the IEC 62443 series2, developed with the help of association such as ISA (International society of automation)3 or WIB (user's association of instrumentation and process control)4 cover the cybersecurity of industrial automation and control systems or IACS. This series is guided by functional safety concerns, takes into account the diversity of systems and associated consequences in the event of incident, organizational (maturity levels) and technical (security levels) aspects.

  IEC 62443 takes a system engineering vision with:

  - the concept of defense in depth which aims to distribute security measures according to security levels, and
  - a description of systems in zones and conduits: zones constitute domains with common security requirements, and conduits group interactions between two necessary zones and provide secure communication.

- Further to using the IEC 62443 series, the energy utility industry has also published ISO/IEC 27019 to provide guidance on the use of ISO/IEC 27002 applied to process control systems.
- In the automotive field, the United Nations UNECE R155 regulation published in 20215 calls for car manufacturers to certify their cybersecurity management systems. This certification is mandatory for vehicle approval. In order to support this certification, ISO and SAE worked on standards,

[2] https://www.iec.ch/blog/understanding-iec-62443

[3] https://www.isa.org/

[4] https://www.wib.nl/

[5] https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

initially starting from the context of functional safety standards6, to develop ISO/SAE 21434 which focuses on cybersecurity engineering. Two other standards are under development, ISO/SAE 8475 which addresses cybersecurity assurance levels and target attack feasibility, and ISO/SAE 8477 on verification and validation of cybersecurity.

- the railway sector is currently developing IEC 63452 (Railway applications - cybersecurity) which aims to apply the principles of IEC 62443 to railway applications, by relying on a high-level life cycle of operational safety or railways applications as defined in EC 62278 (Railway applications - Specification and demonstration of reliability, availability, maintainability and safety), and by identifying the interplay and necessary exchanges of information between the cybersecurity process and the railway safety process.

Conformity Assessment

Conformity assessment is carried out by CASCO7, the ISO committee that develops policy guidance and publishes standards on conformity assessment. Many of the published document are common to ISO and IEC. In short, conformity assessment focuses on verifying that requirements specified in a standard are met. It starts with an object of conformity assessment, which is the entity to which the specified requirements apply. Conformity assessment activities aim to provide confidence in the object of conformity.

CASCO provides strict rules on the principle of separation between requirements to be evaluated, and requirements of the evaluation process itself8.

In terms of ICT cybersecurity, we can cite the following standards:

- For compliance with ISO/IEC 27001 on information security management systems, ISO/IEC 27006 on the requirements for bodies providing audit and certification of information security management systems.
- For compliance with ISO/IEC 27701 on privacy management systems, ISO/IEC 27706 on the requirements for bodies providing audit and certification of privacy information management systems.
- For information technology security compliance, ISO/IEC 15408 series on evaluation criteria for IT security, and ISO/IEC TS 27115 on cybersecurity assessment of complex systems.

At the level of business areas

- For compliance with IEC 62443 in the industrial field, evaluation standards have been added with part 6-1 on the evaluation of requirements of part 2-4 concerning IACS service providers and part 6-2 on the evaluation of requirements of Part 4-2 relating to IACS components.
- For compliance with ISO/SAE 21434 in the automotive field, ISO 5112 which provides guidelines for auditing cybersecurity engineering

---

6 Supported by the ISO 26262 standard (Road vehicles – Functional safety) published in 2011.

7 https://www.iso.org/fr/casco.html Reference may be made to clause 33 of part 2 of the ISO directives:

8 https://www.iso.org/sites/directives/current/part2/

These standards are used as references for the implementation of certification programs such as those of AFNOR for ISO/IEC 27001 certifications.9 or ISO/IEC 2770110, that of ANSSI for common criteria (ISO/IEC 15408)11, that of the IECEE12 for IEC 62443, or that of TÜV NORD13 for ISO/SAE 21434.

Cybersecurity Frameworks

Moves towards the creation of a cybersecurity community can be traced back to the 2000s with a focus on prevention:

- The NIST (National Institute of Standards and Technology) in the United States published the report NIST SP 800-53 in 2005.14 which can be considered as the security controls reference catalog. From 2010, NIST added controls on privacy. The latest version is revision 5 published in 2020. It contains no less than 450 pages and will continue to evolve in the future.
- The cybersecurity community published the Common Vulnerability Scoring System (CVSS) in 2003.15, a system for evaluating the criticality of vulnerabilities according to a score between zero and ten. Version 4 of this system was published in 2023.

In 2014, NIST published its cybersecurity framework (CSF)16. This framework changed the landscape by integrating the management of cybersecurity incidents, thus completing a vision of risk management based on the two phases (risk assessment and risk treatment) with five functions: Identify (corresponding to risk assessment), Protect, Detect, Respond, Recover (corresponding to treatment of risk). A list of activities is associated with each function, and the concept of organizational profile is defined, allowing organizations to select relevant activities. NIST released version CSF 2.0 in 2024. It adds an additional function (Govern), and explains the correspondence between activities in version 2.0 and controls in the NIST SP 800-53 controls catalog. Since 2018, NIST has also been leading an equivalent initiative on a privacy framework17.

NIST further published SP 800-160 vol.2 in 2019 and 202118 on the engineering of resilient cyber systems, and SP 800-160 vol.119 in 2022, on the engineering of trusted secure systems.

---

9 https://certification.afnor.org/numerique/certification-iso-27001

10 https://certification.afnor.org/numerique/iso-27701-protection-vie-privee

11 https://cyber.gouv.fr/comprendre-la-certification

12 IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components: https://www.iecee.org/certification

13 https://www.tuev-nord.de/en/company/certification/services/isosae-21434/

14 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

15 https://www.first.org/cvss/

16 https://www.nist.gov/cyberframework

17 https://www.nist.gov/privacy-framework

18 https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

19 https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

Note also contributions of MITRE20 to the work of NIST, with the provision of two online sites. The first, published in 2013, is a knowledge base that categorizes and describes cyber attacks21. The second is the "cyber resilience engineering framework".22, which accompanies SP 800-160 vol.2 by visualizing the correspondences between the controls of the NIST SP 800-53 catalog and the activities of CSF 2.0.

Standardization follows this evolution, with ISO/IEC 27100 (concepts and overview of cybersecurity), with ISO/IEC 27110 (guidelines for the development of a cybersecurity framework) which is directly influenced by the cybersecurity framework of the NIST. We will also note the ISO/IEC 27035 series on incident management, as well as the start of the ISO/IEC 9138 series on systems resilience, the first part of which on concepts and vocabularies will be published shortly.

In our coming blog on standardization evolution of cybersecurity standards, LICORICE will cover topics such: Ecosystems, Regulations and the evolution of standardization Practices.

[20] https://www.mitre.org/

[21] https://attack.mitre.org/

[22] https://crefnavigator.mitre.org/