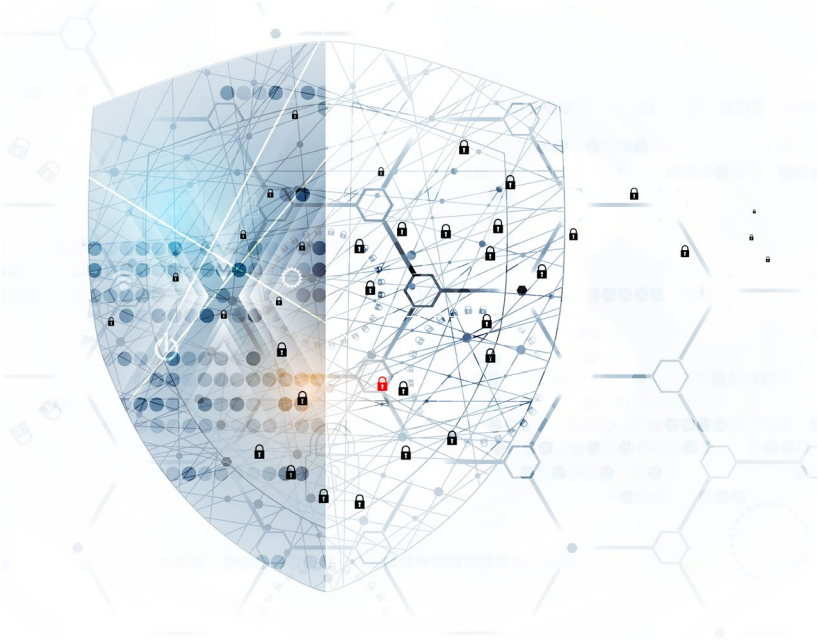
Standards overview in cybersecurity

January 2022



Publication date: 24/01/2021

Version: 1.2

Document history and validation cycle

Version	Description	Author	Reviewer	Document status	Publication date
1.2	Update document to include ENISA, NIST & OWASP standards.	Benoit Poletti	-	Published	24/01/2022
1.1	Update document to reflect recent ISO publications.	Benoit Poletti	-	Published	11/01/2022
1.0	Initial release of the document.	Benoit Poletti	-	Published	30/03/2021

Table of contents

1 Introduction

1.1 Subject

The present document focuses on standardization activities within the **cybersecurity domain**.

1.2 Methodology

This standards overview has been performed based on the following approach:

1. Identification and analysis of international (ISO, IEC and ITU-T), regional (CEN, CENELEC and ETSI) and national standardization activities related to the **cybersecurity domain**; and
2. Assessment and description of relevant standards published or under development.

1.3 Definition of a standard

A standard:

- defines requirements and/or recommendations related to a topic, such as a product, process, method or related results, or a group of topics, or a domain;
- can be used to measure conformance to stated requirements and/or recommendations; and
- provides relevant terminology to facilitate communication and understanding.

A standard:

- is established by consensus, and approved by a recognised body;
- contributes to the achievement of the optimum degree of order in a given context; and
- provides for common and repeated use.

1.4 Standards Developing Organisations ("SDOs")

A SDO is an entity where standards are designed, developed, coordinated, published or revised. It is composed of members which can be countries, private or public organisations.

The main objective of a SDO is to define standards that are harmonizing requirements or recommendations to create uniformity.

A SDO can be:

- International;
- Regional;
- National; or
- An industry consortium.

1.4.1 International SDOs

International Organization for Standardization

International Electrotechnical Commission

International Telecommunication Union

IEEE Standards Association

1.4.2 Examples of regional SDOs

European Committee for Standardization (CEN)

European Committee for Electrotechnical Standardization (CENELEC)

European Telecommunications Standards Institute (ETSI)

European Union Agency for Cybersecurity (ENISA)

1.4.3 Examples of national SDOs

Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (Luxembourg)

National Institute of Standards and Technology (US)

Association Française de Normalisation (France)

1.4.4 Examples of industry consortiums

2 Overview of standards in the cybersecurity domain

2.1 Generic standards that have been published

TITLE	**ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts**
SCOPE	This document provides an overview of cybersecurity. This document: a) describes cybersecurity and relevant concepts, including how it is related to and different from information security; b) establishes the context of cybersecurity; c) does not cover all terms and definitions applicable to cybersecurity; and d) does not limit other standards in defining new cybersecurity-related terms for use. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).
LINK	https://www.iso.org/standard/72434.html
SDO	International Organization for Standardization (ISO)

TITLE	**ISO/IEC 27102:2019, Information security management — Guidelines for cyber-insurance**
SCOPE	This document provides guidelines when considering purchasing cyber-insurance as a risk treatment option to manage the impact of a cyber-incident within the organization's information security risk management framework. This document gives guidelines for: a) considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks; b) leveraging cyber-insurance to assist manage the impact of a cyber-incident; c) sharing of data and information between the insured and an insurer to support underwriting, monitoring and claims activities associated with a cyber-insurance policy; d) leveraging an information security management system when sharing relevant data and information with an insurer. This document is applicable to organizations of all types, sizes and nature to assist in the planning and purchase of cyber-insurance by the organization.
LINK	https://www.iso.org/standard/72436.html
SDO	International Organization for Standardization (ISO)

TITLE	**ISO/IEC TR 27103:2018, Information technology — Security techniques — Cybersecurity and ISO and IEC Standards**
SCOPE	ISO/IEC TR 27103:2018 provides guidance on how to leverage existing standards in a cybersecurity framework.
LINK	https://www.iso.org/standard/72437.html
SDO	International Organization for Standardization (ISO)

TITLE	**ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity**
SCOPE	Provides guidance for improving the state of cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains. It covers the baseline security practices for stakeholders in the cyberspace. This International Standard provides: a) an overview of cybersecurity, b) an explanation of the relationship between cybersecurity and other types of security, c) a definition of stakeholders and a description of their roles in cybersecurity, d) guidance for addressing common cybersecurity issues, and e) a framework to enable stakeholders to collaborate on resolving cybersecurity issues.
LINK	https://www.iso.org/standard/44375.html
SDO	International Organization for Standardization (ISO)

TITLE	**NIST Cybersecurity Framework (CSF)**
SCOPE	The NIST Framework for Improving Critical Infrastructure Cybersecurity is a set of guidelines for mitigating organizational cybersecurity risks, based on existing standards, guidelines, and practices. The framework provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes. This framework is voluntary.
LINK	https://www.nist.gov/cyberframework
SDO	National Institute of Standards and Technology (NIST)
LIFE CYCLE	Version 1.1 (2018-04)

TITLE	**ENISA Cybersecurity for SMEs – Challenges and Recommendations**
SCOPE	In response to the COVID19 pandemic, ENISA analysed the ability of Small and Medium Enterprises (SMEs) within the EU to cope with the cybersecurity challenges posed by the pandemic and determining good practices to address those challenges. This report provides cybersecurity advice for SMEs, but also proposals for actions that Member States should consider in order to support SMEs improve their cybersecurity posture.
LINK	https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
SDO	European Network and Information Security Agency (ENISA)
LIFE CYCLE	Published (2021-06)

2.2 Sector-specific standards that have been published

2.2.1 Automotive

TITLE	**ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering**
SCOPE	This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces. A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk. This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document. This document does not prescribe specific technology or solutions related to cybersecurity.
LINK	https://www.iso.org/standard/70918.html
SDO	International Organization for Standardization (ISO)

2.2.2 Privacy and data protection

TITLE	**ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines**
SCOPE	This technical specification specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations', type, size, or nature.
LINK	https://www.iso.org/standard/72435.html
SDO	International Organization for Standardization (ISO)

2.2.3 Web application security

TITLE	**Application Security Verification Standard (ASVS) Project**
SCOPE	This document provides a basis for testing web application technical security controls and provides developers with a list of requirements for secure development.
LINK	https://owasp.org/www-project-application-security-verification-standard/
SDO	Open Web Application Security Project (OWASP)
LIFE CYCLE	ASVS 4.0.3 released (2021-10)

TITLE	**Web Security Testing Guide (WSTG)**
SCOPE	This document provides: a) a comprehensive guide to testing the security of web applications and web services. b) a framework of best practices used by penetration testers and organizations all over the world.
LINK	https://owasp.org/www-project-web-security-testing-guide/
SDO	Open Web Application Security Project (OWASP)
LIFE CYCLE	Version 4.2 (2020-12). Version 5.0 is under development.

TITLE	**OWASP Top Ten**
SCOPE	This standard awareness document for developers and web application security provides ranking of and remediation guidance for the top 10 most critical web application security risks. The report is based on a consensus among security experts from around the world.
LINK	https://owasp.org/www-project-top-ten/
SDO	Open Web Application Security Project (OWASP)
LIFE CYCLE	Last available version dated from 09 2021.

TITLE	**Software Assurance Maturity Model (SAMM)**
SCOPE	This project provides a usable framework to help organizations formulate and implement a strategy for application security that is tailored to the specific business risks facing an organization. SAMM helps organizations: a) Evaluate existing software security practices, b) Build a balanced software security assurance program in well-defined iterations, c) Demonstrate concrete improvement to a security assurance program, d) Define and measure security-related activities throughout an organization.
LINK	https://owasp.org/www-project-samm/ https://owaspsamm.org/model/
SDO	Open Web Application Security Project (OWASP)
LIFE CYCLE	Version 2.0

2.2.4 Certification body

TITLE	Case for a Trustless Computing Certification Body
SCOPE	Can a new certification body deliver radically unprecedented IT security for all, while at once ensuring legitimate lawful access? In this position paper, we argue that a new cybersecurity certification body can, and should, be created which will be able to reliably and sustainably certify end-to-end IT services with levels of integrity and confidentiality that radically exceed current state-of-the-art, civilian and military, while at once solidly enabling only legitimate and constitutional lawful access. Both can be achieved through uniquely uncompromising “zero trust” security-by-design paradigms down to each critical life-cycle component, including the certification governance itself.
LINK	https://www.trustlesscomputing.org/position-paper
SDO	Trustless Computing Association
LIFE CYCLE	Version 1.0 (04 2018)

2.3 Sector-specific standards that are under development

2.3.1 Automotive

TITLE	**ISO PAS 5112, Road vehicles — Guidelines for auditing cybersecurity engineering**
SCOPE	This document provides guidelines to organizations that contribute to the achievement of road vehicle cybersecurity along the supply chain on managing a cybersecurity management system (CSMS) audit programme, on conducting organizational CSMS audits, on competences of CSMS auditors, and on providing evidence during CSMS audits, in addition to the guidelines in ISO 19011. The elements of the CSMS are based on the processes described in ISO/SAE 21434. This document is applicable to those needing to understand or conduct internal or external audits of a CSMS or to manage a CSMS audit programme.
LINK	https://www.iso.org/standard/80840.html
SDO	International Organization for Standardization (ISO)
LIFE CYCLE	Under development – Expected publication date (03 2022)

2.3.2 Privacy and protection

TITLE	**ISO/IEC TR 27109, Information technology — Information security, cybersecurity and privacy protection — Cybersecurity education and training**
SCOPE	This document provides state of the art information for cyber education and training, useful to those involved in cybersecurity as users, suppliers, certifiers, policy makers and regulators, educationalists, consumers, vendors and manufacturers.
LINK	https://www.iso.org/standard/81556.html
SDO	International Organization for Standardization (ISO)
LIFE CYCLE	Under development

2.3.3 Internet of Things

TITLE	**ISO/IEC DIS 27400 Cybersecurity – IoT security and privacy - Guidelines**
SCOPE	This document will provide guidance on the principles, (information) risks, and corresponding information security and privacy controls to mitigate those risks for the IoT.
STATUS	Final Draft International Standard
LINK	https://www.iso.org/standard/44373.html
SDO	International Organization for Standardization (ISO)
LIFE CYCLE	Under development

Any questions, remarks or suggestions for improvement?

Do not hesitate to contact us!

contact@incert.lu