Information and technology law course

LECTURE 8 – 17 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

Cybersecurity Standardisation

THE CSA IN THE INTERNATIONAL FRAMEWORK

What are standards?

Standards are represented as documents which define specifications, procedures, and guidelines, aiming to ensure safety, consistency, and reliability of products, services, and systems

- www.standards.org.au

Standards are documents or rules made based on a general agreement and validated by a legal entity, which help to achieve optimal results, as a guideline, model, or sample, in a particular context

- ISO/IEC

Cybersecurity standards – 1

Security features in applications and cryptographic algorithms that mainly provide perspective toward security controls, processes, procedures, guidelines, and baselines.

Objective

Prevent or mitigate cyberattacks and reduce the risk of cyber threats

Advantages

- saving time, decreasing costs, increasing profits, improving user awareness, minimizing risks, and offering business continuity

- facilitate compliance of an organization to industry best practices and procedures

- provide the opportunity to compare a security system on an international level

Cybersecurity standards – 2

Classification of standards

- information security (e.g. ISO 27000 series, NIST, SOX, etc)

- informazion security governance

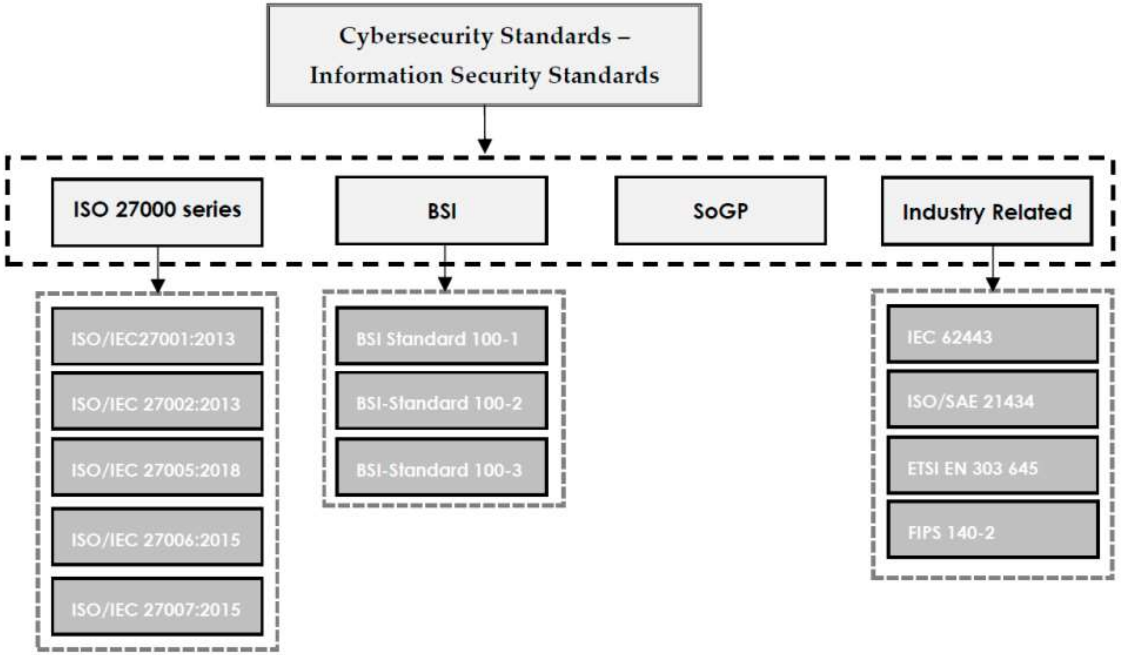
NB Cybersecurity standard ≠ cybesecurity framework

Cybersecurity **standards** explain and provide methods one by one, specify what is expected to be done to complete the process, and clarify methods to coincide with the standard

Cybersecurity **framework** is a general guideline that covers many components or domains that can be adopted by businesses/companies/institutions, which does not specify the steps that are required to be taken

Families of IS standards

Source:Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11, 2181.



Cybersecurity Standards – Information Security Standards

ISO 27000 series

- ISO/IEC27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27005:2018
- ISO/IEC 27006:2015
- ISO/IEC 27007:2015

BSI

- BSI Standard 100-1
- BSI-Standard 100-2
- BSI-Standard 100-3

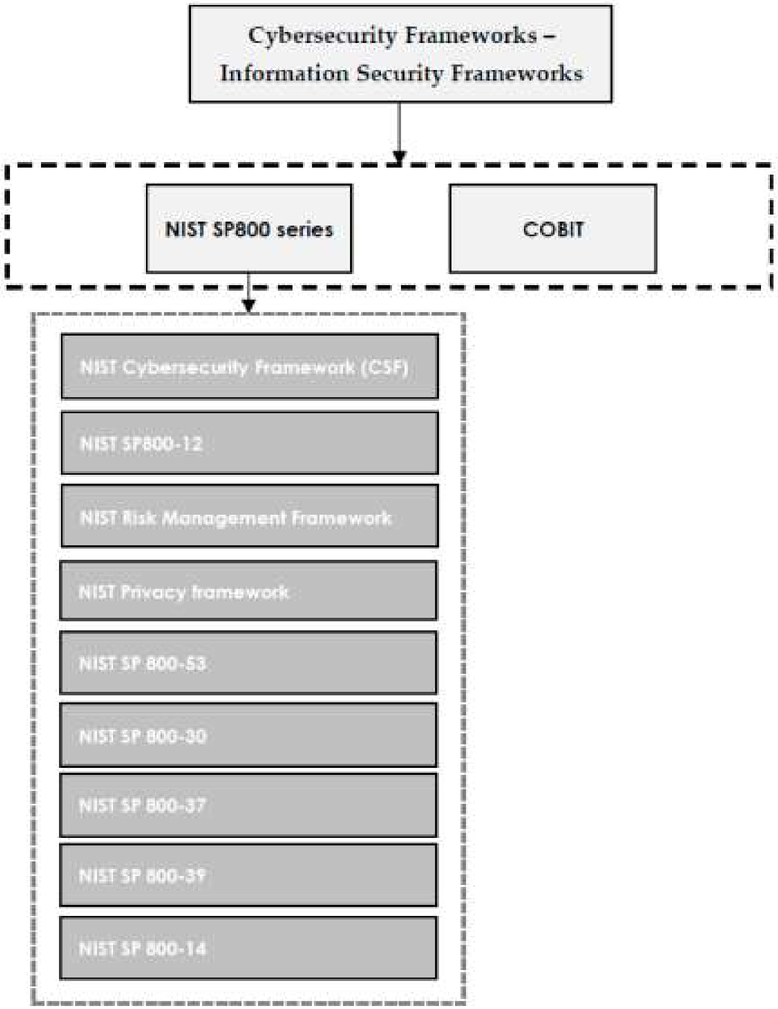
SoGP

Industry Related

- IEC 62443
- ISO/SAE 21434
- ETSI EN 303 645
- FIPS 140-2

Families of IS frameworks

Source:Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11, 2181.



EU Common criteria certification scheme

First Cybersecurity certification scheme

COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

Background – European level

SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement) - produced in response to the EU Council Decision of 31 March 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of 7 April 1995 (1995/144/EC) on common information technology security evaluation criteria

- Then updated in 2010

- The participants work together to:

- Coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies in order to have a common position in the fast growing international *CCRA group*
- Coordinate the development of protection profiles whenever the European commission launches a directive that should be implemented in national laws as far as IT-security is involved

Background – European level

Participants in MRA are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association) which agree

- a) to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;
- b) to improve the availability of evaluated, security-enhanced IT products and protection profiles;
- c) to eliminate the burden of duplicating evaluations of IT products and protection profiles;
- d) to continuously improve the efficiency and cost-effectiveness of the evaluation and certification processes for IT products and protection profiles.

June 2023:

The SOG-IS MRA Management Committee accept the usage of **CC:2022 version of Common Criteria** for issuing CC certificates

Background – International level

ISO/IEC 15408 (Common Criteria)

Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

The standard is composed by three parts:

- Part 1, Introduction and general model: is the introduction to ISO/IEC 15408. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation;
- Part 2, Security functional requirements: establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Targets Of Evaluation);
- Part 3, Security assurance requirements: establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs.

Each part of the standard contains a catalogue of components (mostly functional) tackling different aspects of the cybersecurity functional and assurance requirements. However, as for the others standards analysed so far, this catalogue is instrumental to the specific scope of the Common Criteria, hence it is too specific to be taken as reference for a taxonomy of the cybersecurity knowledge.

Background – International level

Common Criteria Recognition Arrangement (CCRA)

Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance.

Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation

These certificates are recognized by all the signatories of the CCRA.

EUCC certification scheme – step 1

First proposal 1 July 2020 – **CYBERSECURITY CERTIFICATION EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS**

«The EUCC scheme may serve as a successor to the EU national schemes operating under the SOG-IS MRA, identified in Chapter 17, NATIONAL OR INTERNATIONAL SCHEMES.

It may allow to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g., firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, …) as well as of any ICT product embedding a security functionality (i.e., routers, smartphones, banking cards, medical devices, tachographs for lorries, …).

By offering two (2) security assurance levels, 'substantial' and 'high', it shall cover a large variety of demanding security requirements, though not addressing the basic level that may be offered by schemes that are more lightweight and cover less demanding security requirements."

EUCC certification scheme – step 1

Existing CC scheme : recognition by 15 EU countries and +30 countries internationally, and +4500 products certified

Objective

Certification enable consumers to have an impartial assessment of an ICT product, it increases the consumer's level of confidence in and reliance on the security of the certified ICT product.

- the CC include an analysis and testing of the product for conformance to specific security requirements.

Structure

Flexible set of evaluation assurance levels

- two assurance levels of the CSA (medium and high)
- No basic level (thus no possibility to have self-assessment)

EUCC certification scheme – step 1

Following Common Criteria based certification schemes cover the same type or category of ICT products, security requirements, evaluation criteria and methods, and assurance levels:

Within the EU, the:

- French scheme, operated by ANSSI
- German scheme, operated by BSI
- Italian scheme, operated by OCSI
- Dutch scheme, operated by TÜV Rheinland NL and NLNCSA
- Spanish scheme, operated by CCN
- Swedish scheme, operated by FMV
- Norwegian scheme, operated by SERTIT

EUCC certification scheme - step 2

Open consultation

Feedback period: 03 October 2023 - 31 October 2023 (midnight Brussels time)

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en

EU CC certification scheme – step 3

COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

Enjoy ENISA video ☺

https://www.youtube.com/watch?v=vFQht0W-bQg

EUCC certification scheme

The applicant for an EUCC certificate should provide the documentation related to the intended use of the ICT product and the analysis of the levels of risks associated with such usage in order to enable the conformity assessment body to evaluate the suitability of the assurance level selected. Where the evaluation and certification activities are performed by the same conformity assessment body, the applicant should submit the requested information only once.

A technical domain is a reference framework that covers a group of ICT products that have specific and similar security functionality that mitigates attacks where the characteristics are common to a given assurance level.

- A technical domain therefore also fosters harmonisation of the evaluation of covered ICT products.

Two technical domains are currently widely used for certification at levels

- AVA_VAN.4 ‘Smart cards and similar devices’ technical domain, where significant portions of the required security functionality depend on specific, tailored and often separable hardware elements (e.g. smart card hardware, integrated circuits, smart card composite products, Trusted Platform Modules as used in Trusted Computing, or digital tachograph cards)
- AVA_VAN.5 ‘Hardware devices with security boxes’, where significant portions of the required security functionality depend upon a hardware physical envelope (referred to as a ‘Security Box’) that is designed to resist direct attacks (e.g. payment terminals, tachograph vehicle units, smart meters, access control terminals and Hardware Security Modules).