Information and technology law course

LECTURE 8 – 17 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

Cybersecurity Standardisation

THE CSA IN THE INTERNATIONAL FRAMEWORK

Before getting to the first corr. scheme created through the system, we need to understand what's a standard.

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

↓

Intern. Stand. Org.

Standard is a set of rules. They can be less or more detailed.

(1) Specifications, procedures, guidelines are a bit stricter so there is few room for interpret.

(2) For the 2nd standards are still docs or rules, but are based on general agreement. So experts can write and discuss for the standardization. This is usually what ISO does: They want to reach an agreement. There's a coord. effort for compromise and the standard is validated by legal entity. There needs to be someone that takes the agreement and approves it (like ISO). If there was no validation, there is no care in checking if you comply.

There are usually bodies that can enforce the compliance.

Not compliance will result in being out of the market basically.

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

The type of standards look at them: (1) Helps us to prevent incidents, reduce or mitigate incidents or addressing the problem.
You don't have to think autonomously.
(2) Those who are part of the working group are the ones that work in that sector.
So if they agree, we have common best practices.
(3) ISO works globally: you can use the same standards recognisable by other suppliers in other countries.

Cybersecurity standards – 2

Classification of standards

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

- informazion security governance (1)

NB Cybersecurity standard ≠ cybesecurity framework

DETAILED: "HATE SPEECH IS BANNED ecc" No. "You have to do A to reach B". Very clear and detailed

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

BIGGER PIC: if stand. is one of the elements...

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

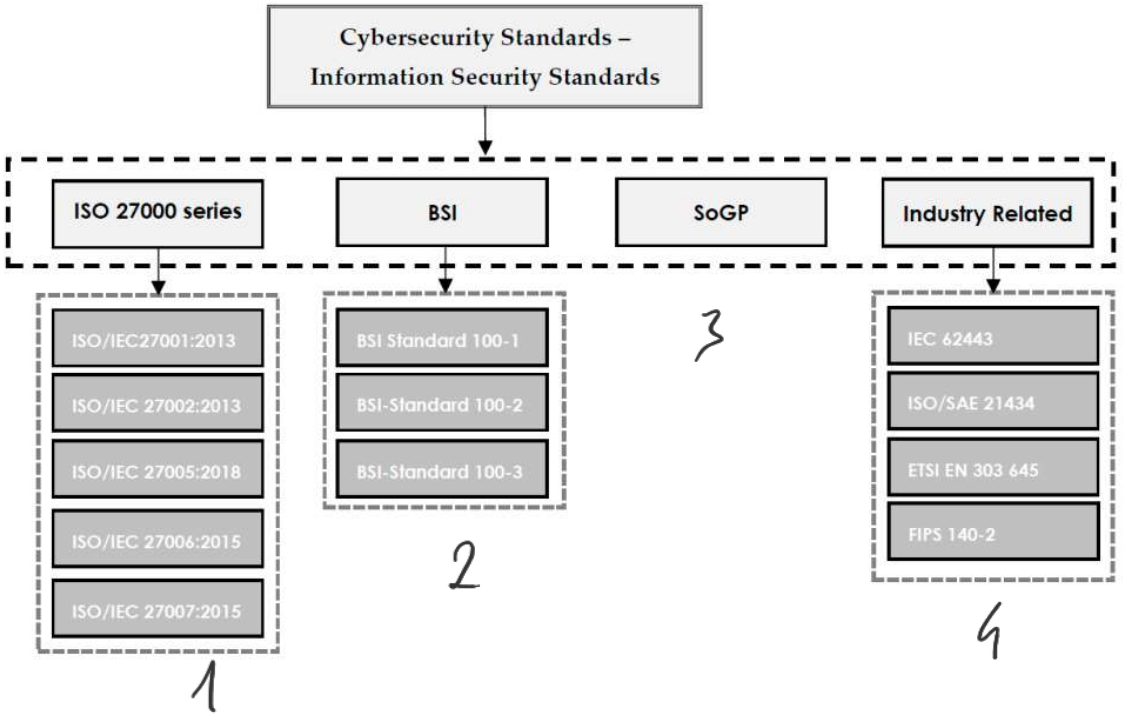
We can have a lot of standards. In info sec. the proc. are quite strict. How the system in a company is set up

(1) Ones dedicated to the structure: who does what, allocation of power and tasks. *
(2) Doesn't allow to understand the specific steps: you have guidelines on how to get to objectives but not how.

* You have a better compliance on who does what specified in a info security standard.

Families of IS standards

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

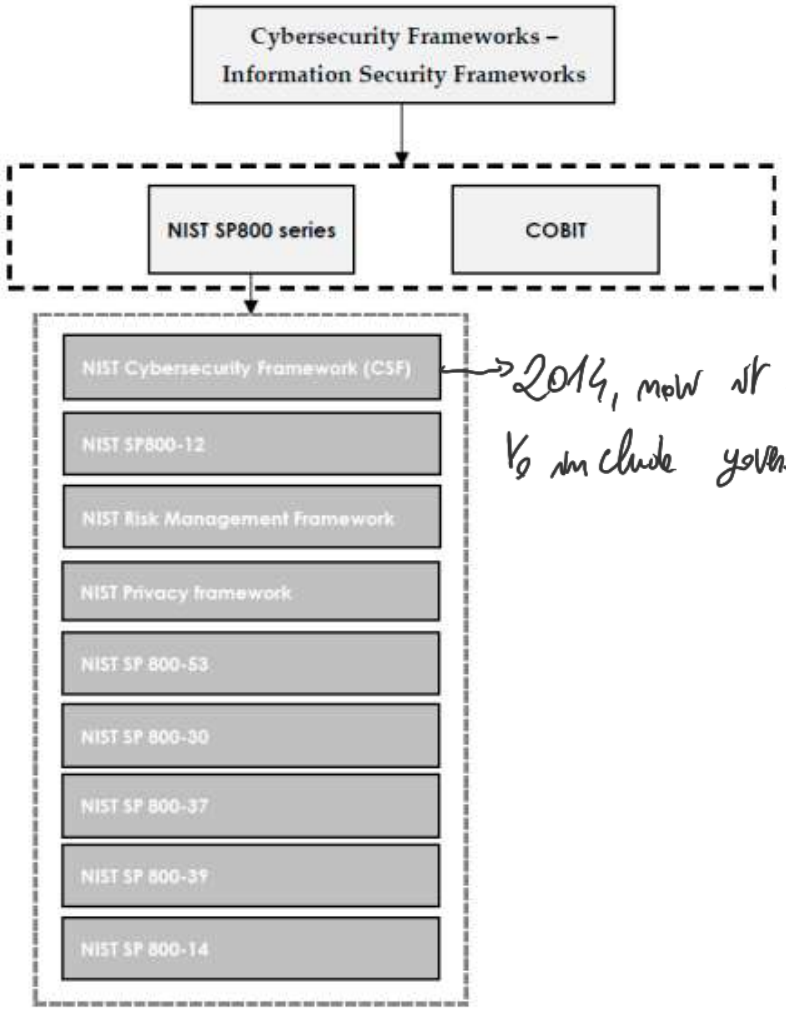


1. Created in US, works globally.
2. BSI is a german organiz. but those standards work globally. The adaptance depends on the market and what others are complying with.
3. SoGP:
4. Industry Related: based sometimes on ISO, sometimes on others.

1. Is usually standards about info security: 1.1. is about a secure info management system, so how to organize data. Provides 7 key elements for steps for installation, recovery, maintaining exc.: they are very specific. 1.2. Code of practice for info security controls, based on best practices for IS sec. management. These standards should facilitate the work of a company.
2. Governmental agency for managing and securing systems, first starting at a national level but then applying to private orgs. Bsp. BSI standard 100-1 is similar to ISO 27001, the difference is that different experts show there opinion. BSI 100-3 is about risk analysis.
4. IR standards are mostly done by an industry and they are build up eventually to ISO for approval.

Families of IS frameworks

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



2014, now it has been updated to include governance framework.

Goes in the direction of increasing security in the org.

EU Common criteria certification scheme

The common criteria standard was created at international level

The common criteria as standard was already existing: document created at international level.
Idea: commission impl. reg. 2024/482: the comm. that has adopted the implementing reg. regarding the EU common criteria based cybers. cert. 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)

Commission has adopted the Regulation of 2019

Understand why a CC cert. should have been an easy task: because before we had the SOG-IS MRA, set up by (1). There was a group of representatives of member states based from the council decision in 1992 addressing for the need of IS (only defence was the main focus). What does MRA mean? (1)

Background – European level

set up by

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

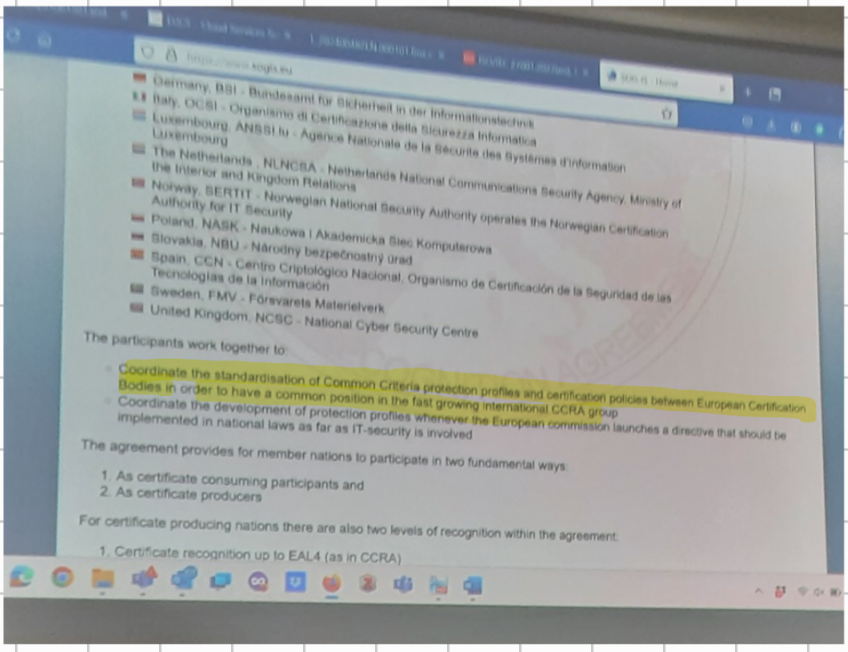
- Then updated in 2010

- The participants work together to:

→ SEC. Req. for a specific type of product

- 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

(1) 1. There was a group with representative of states produced after the 1992 decision.
IDEA: Mutual rec. agree: if I have a standard applying in my country and the standard is similar to other countries', there's the possibility to recognize the standards.



Based on CCRA, an international agreement dedicated to the analysis of common criteria for the standard, divided in Authorizing Members and Consuming Members. It's a standard called common criteria, and at national level there's an agreement. So the EU creates a mutual recog. agreement

(2) In particular, the MRA was looking at many standards; you have countries participating; the idea was to coordinate the standardization of common criteria. The European SOG-IS MRA is the way in which Europe tries to figure out a way to control internally the mutual recognition. It's about a bigger picture though: CC Recog. Agreement is an international agreement; so at national level there is this dedicated to the analysis of the so called CC that are adopted by the countries participating. There's a division between Auth Members and Consuming Members. Here, the products can be evaluated by common and independent licensed laboratories that determine the fulfilment of the rules set out in the standard (set of rules, proc. and processes called CC). At national level there's this agreement. What happens? ASA we have these bright pics the EU was looking for a way to use them internally

for the MS, so they create a MRA, which is a EU agreement.
So what is this CC? MR is based on an ISO standard!
So this SOG-IS uses this version of the CC based on the universal, context based on ISO standard! ISO SR. that has been recognised.

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.

Common criteria are set up for
All the elements in a specific product will have to be evaluated to this standard. This standard has been adopted as the basis for their own activity and control: this is the Bible.

I won't need the SOG-IS system if it is addressing the common criteria if I have a certification scheme once and for all.

The CC defines ① Idea: these type of CC are a set of elements
IDEA: all the elements in a specific product will have to be evaluated according digital
to this CC. In this case, we have this given standard adopted by this CCRA. So there are some countries that adopt this standard as the basis for their own activity at controls? Yh I want to produce something. That's the Bible. So the SOG-IS goes from the ISO level to the european level. So for all these activities, they are an easy task to become a certificate.

PART 1: overview of the principles behind standard, who to methodology used.
2: provides a detailed catalog of security functional requirements that products can be evaluated against (ex. cryptographic support, access control)
3: defines the assurance requirements that are applied during evaluation process (methods and processes that must be followed)
Framework for evaluating security of IT prod. and systems.

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."

What was the process that led to the CScheme?

EUCC certification scheme – step 1

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

Common criteria and already a lot of products comply with the schemes.

Objective

At one point they should see if their previous certification has to be updated.

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)

For the 15 EU states; include the existing Common criteria ISO standards in the certificate rep. But for the rest we need bodies* that release certifications. We want to open market.

* Not only for the consumer, but also the producers I want to include in my chain of supply. I may want to only reach suppliers up to the certifications. It's a tool for consumers, but it's more for the supply chain and manufacturers to look for the best suppliers that have a certificate. Internal market.

*and build their own expertise. They might not have it.

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

there were national schemes that were looking upon CC.
3 possibilities for those already certificated: the certificate issued under the IT scheme just translated into the EU by adding what was missing.
Not easy: bring back the old certs to get the new EU label OR worst case I have to redo everything. The approach for the commission:

Certified manufacturers will need to recertify and only have to bring the documentation without the need for other operations like checks. They have to send docs to prove that they are still compliant.

EUCC certification scheme - step 2

Open consultation

possibility to provide reaction to the proposal

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

Adoption of the cert. scheme. You have 1 year to make sure you have the time to reorganize the system.

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).

Those sectors have high AVA VAN levels, so highly critical

Assurance Vulnerability Analysis Sectors (Vulnerab. Assessment - Vuln. Analysis)

level

Issue: you have to make the doc work to achieve what you are trying to: it can be a burden.

The SOG-IS MRA promoted the adoption and use of CC standard (ISO) among its participating member states, facilitating mutual recognition of certifications based on common criteria.
Each participating member state in the SOG-IS MRA had its own national certification scheme based on CC. They defined specific processes and requirements for performing security evaluations, but all adhered to the CC standard. So they pushed for recognition.
It was a voluntary agreement among participating countries.
The SOG-IS MRA did contribute to fostering a shared approach within the broader CCRA.