CERTIFICATIONS

UNICA
UNIVERSITÀ
DEGLI STUDI
DI CAGLIARI

CERTIFICATION

Definition

third-party attestation that specified requirements relating to a person, product, process or service are fulfilled

Kinds of certifications

- professional (attesting qualification)
- product, process and service (attesting the presence of certain features)

Main actors and components

- certification scheme
- accreditation body
- certification body

RELEVANT STANDARDS

ISO/IEC 17000:2020
Conformity assessment – Vocabulary and general principles

ISO/IEC 17024:2012 (reviewed and confirmed in 2018)
Conformity assessment – General requirements for bodies operating certification of persons

ISO/IEC 17065:2012 (reviewed and confirmed in 2018)
Conformity assessment – Requirements for bodies certifying products, processes and services

Informative sections, including terms and definitions, are freely available

PROFESSIONAL CERTIFICATIONS

PROFESSIONAL CERTIFICATIONS LANDSCAPE

Several professional certification bodies, including for-profit companies and non-profit organisations, offer specific programmes for cybersecurity professionals, e.g.

- International Information Systems Security Certification Consortium (ISC2)
- Information Systems Audit and Control Association (ISACA)
- Escal Institute of Advanced Technologies (SANS)
- Computing Technology Industry Association (CompTIA)

There are also **framework** initiatives, e.g.

European Cybersecurity Skills Framework (ECSF)

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)

International Information Systems Security Certification Consortium (ISC2)
not-for-profit organisation founded in 1989

CISSP

- compliant with ISO/IEC 17024:2012
- compliant with the requirements of the US Department of Defense
- over 168,000 certified members

HOW TO OBTAIN THE CISSP CERTIFICATION

Minimum of **5 years** cumulative paid full-time **work experience** (4-year college degree = 1 year of work experience) in two or more domains of the CISSP Common Body of Knowledge; passing an **exam** on all domains

- Security and Risk Management – security, risk, compliance, law, regulations, business continuity
- Asset Security – protecting security of assets
- Security Architecture and Engineering – engineering and management of security
- Communication and Network Security – designing and protecting network security
- Identity and Access Management – controlling access and managing identity
- Security Assessment and Testing – designing, performing, and analyzing security testing
- Security Operations – foundational concepts, investigations, incident management, disaster recovery
- Software Development Security – understanding, applying, and enforcing software security

CISSP IN ITALY

ISC2 Italy chapter

- not-for-profit organization founded in 2011
- over 600 members
- activities include the organization of courses to prepare for the CISSP exam

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF

- a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals, and to support the design of cybersecurity-related training programmes
- EU reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy, a policy initiative by the European Commission (2023)
- governance, implementation and evolution supported by ENISA
- several certifications bodies have already mapped their credentials to the ECSF
  - ISC2
  - ISACA
  - CompTIA
  - SANS

ECSF ROLE PROFILES

The ECSF role profiles document (Sept. 2022) summarises the cybersecurity-related roles into 12 profiles, defined in terms of responsibilities, skills, synergies and interdependencies – competences of each role are

- defined according to the European e-Competence Framework (e-CF)
- organised according to five ICT business areas of the European Qualifications Framework (EQF)

ECSF ROLE PROFILES: EXAMPLE

2.10 CYBERSECURITY RISK MANAGER

Profile Title	Cybersecurity Risk Manager
Alternative Title(s)	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager
Summary statement	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.
Mission	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.
Deliverable(s)	• Cybersecurity Risk Assessment Report • Cybersecurity Risk Remediation Action Plan
Main task(s)	• Develop an organisation's cybersecurity risk management strategy • Manage an inventory of organisation's assets • Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems • Identification of threat landscape including attackers' profiles and estimation of attacks' potential • Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy • Monitor effectiveness of cybersecurity controls and risk levels • Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets • Develop, maintain, report and communicate complete risk management cycle
Key skill(s)	• Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options
Key knowledge	• Risk management standards, methodologies and frameworks • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-related technologies
e-Competences (from e-CF)	E.3. Risk Management E.5. Process Improvement E.7. Business Change Management E.9. IS-Governance	Level 4 Level 3 Level 4 Level 4

PRODUCT CERTIFICATION

PRODUCT AND SECURITY CERTIFICATIONS

Product certification

- outcome of an assessment activity carried out by a certification body, which has to be an independent third party
- certification bodies have to be authorized by specific accreditation bodies
- based on standards and established methodologies

Security certification

- activity which provides a probabilistic (i.e., based on known threats) assurance of the capability of a system to comply with security specifications related to its operation or use

NORMATIVE CONTEXT AND SUBJECTS INVOLVED

Normative context

Reference regulations: what needs to be certified and how

Certification scheme: rules governing the process of applying reference regulations

Scheme manager: local, independent body that

- guarantees the correct application of the scheme by all subjects involved
- negotiates mutual acknowledgment agreements with peer bodies in other countries

Scheme guarantor: independent body (usually, an international one) in charge of settling disputes involving the scheme manager

Subjects involved

Accreditation body: initial accreditation and periodic evaluation of certification bodies

Certification body: issues certifications based on evaluation results, guarantees the correct management of certificates

Evaluator: carries out the security evaluation activities

Client: owner of certification object, recruits the evaluator

Object to be evaluated or certified

Certification's user: the body that will make use of the certification: the client itself (e.g., the manufacturer), a supplier or the final user

CHARACTERISTICS OF PRODUCT CERTIFICATIONS

Impartiality

accreditation body, certification body and evaluator must be an independent third party with respect to the client (no common commercial of financial interests related to the certification outcome)

Objectivity

the evaluation should be based on empirical evidence

Repeatability

the same evaluator should obtain the same results on the same product with respect to the same security requirements

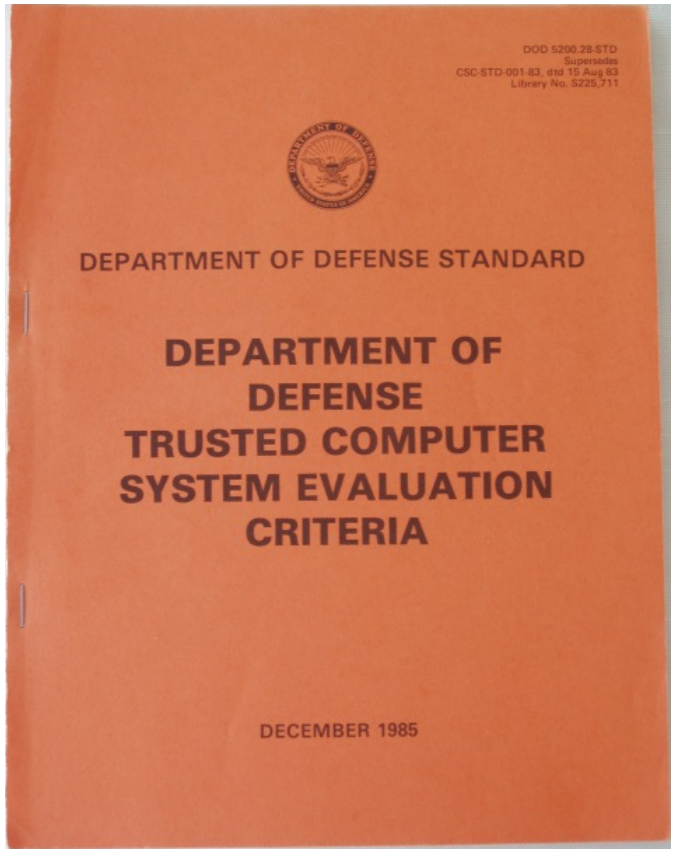
Reproducibility

a different evaluator should obtain the same results on the same product with respect to the same security requirements

TRUSTED COMPUTER SECURITY EVALUATION CRITERIA (TCSEC)

First document on software certification

- also known as "Orange book"
- US Department of Defense, 1983
- focus: operating systems, military applications
- replaced in 2000 by Common Criteria (CC)
- available from NIST



TCSEC SECURITY REQUIREMENTS

Criteria for **probabilistic** evaluation of the **security** of operating systems based on fundamental **requirements**

Policy
- security policy definition
- marking (access control labels to objects)

Accountability (of users)
- identification
- accountability (logging)

Assurance
- assurance (independent evaluation)
- continous protection

Outdated categorization, but still valid principles: early stage of ISO 27001 security domains

Security of operating systems is evaluated into four main classes, labelled from D (lowest) to A (highest)

TCSEC SECURITY CLASSES

D – Minimal Protection

OSs that fail to meet the requirements for a higher evaluation class, e.g.: MS-DOS, Windows 95/98/ME

C – Discretionary Protection

- administrators **can** apply protection mechanisms to objects
- the OS provides some basic **logging** capabilities
  - C1 – Discretionary Security Protection, e.g.: users and data separation in early UNIX versions
  - C2 – Controlled Access Protection: fine-grained access control enforcing accountability, e.g., IBM OS/400, Win NT/2000/XP, Novell Netware

B – Mandatory Protection

protection levels to each object are required

- B1 – Labeled Security Protection: sensitivity labels, access control to objects such as processes, files and devices; e.g.: HP-UX, Cray Research Trusted Unicos 8.0, Digital SEVMS
- B2 – Structured Protection: formal security policy model, e.g.: Honeywell Multics, Cryptek VSLAN, trusted XENIX
- B3 – Security Domains: mediation of accesses of subjects to objects, e.g.: Getronics/Wang Federal XTS-300

A (A1) – Verified Protection

trustworthiness of the OS is verified through formal methods, e.g.: Boeing MSL LAN, Honeywell SCOMP

INFORMATION TECHNOLOGY SECURITY EVALUATION (ITSEC)

European scheme analogous to TCSEC

- originally developed by France, Germany, The Netherlands and the United Kingdom (1991)
- main objective: defining internationally harmonised criteria to provide a compatible basis for certification by the national certification bodies, possibly permitting international mutual recognition of evaluation results
- the "father" of modern evaluation criteria for IT products and systems
- widely used in the **military** sector and for **digital signature**
- later replaced by **Common Criteria** (CC)
- available from the EU Senior Officials Group Information Systems Security (SOGIS)

COMMON CRITERIA (CC)

CC: a common set of criteria for evaluating the security of computer systems

Developed by the national security authorities of USA, Canada and Europe (France, Germany, Netherlands, United Kingdom) in the mid-90's

- first version: CC 1.0 (1994)
- current version: CC:2022 Release 1 (2022)

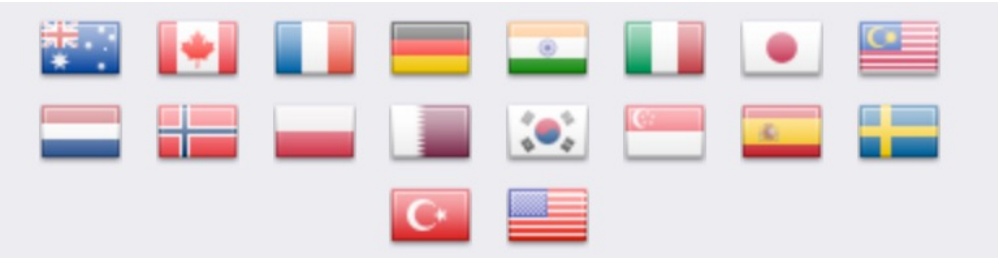
Common Criteria Recognition Agreement (CCRA)

- product evaluation by independent, licensed laboratories
- documents defining the certification process
- certifications issued by Certificate Authorizing Schemes (a **subset** of CCRA members)
- certifications recognised by **all** CCRA members

COMMON CRITERIA MEMBERS

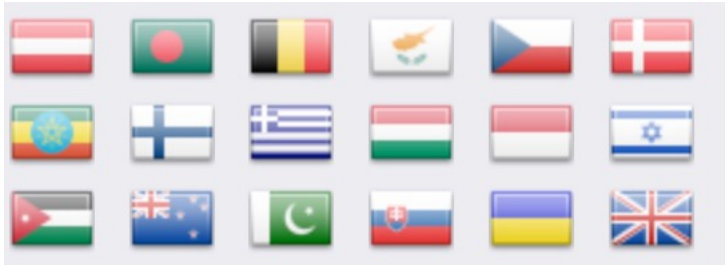
18 Certificate Authorizing Members (schemes), allowed to issue certifications

Australia, Canada, France, Germany, India, **Italy** (since 5 October 2009), Japan, Malaysia, Netherlands, Norway, Poland, Qatar, Republic of Korea, Singapore, Spain, Sweden, Turkey, USA



18 Certificate Consuming Members that recognise, but cannot issue, CC certifications

Austria, Bangladesh, Belgium, Cyprus, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Indonesia, Israel, Jordan, New Zealand, Pakistan, Slovakia, Ukraine, United Kingdom



COMMON CRITERIA: ITALIAN MEMBER

Organismo di Certificazione della Sicurezza Informatica (OCSI)

OCSI is in charge of maintaining the National Scheme for the evaluation and certification of the security of systems and products in the ICT sector (DPCM 30.10.2003 - G.U. n. 98 27.04.2004)

OCSI is within the Italian Agency for National Cybersecurity (ACN)

Seven licensed laboratories provide system and product evaluation services

COMMON CRITERIA: DOCUMENTS STRUCTURE

Current version: CC:2022 Release 1 (November 2022)

Part 1 – Introduction and general model: general concepts and principles

Part 2 – Security functional requirements: standard templates upon which to base functional requirements

Part 3 – Security assurance components

- standard templates upon which to base assurance requirements
- evaluation criteria
- Evaluation Assurance Levels (EALs)

Part 4 – Framework for the specification of evaluation methods and activities

Part 5 – Pre-defined packages of security requirements

PROTECTION PROFILES

Documents describing

- the elements subject to evaluation
- the security requirements for a category of products

Typically defined by three different kinds of actors

- a user community seeking consensus on the requirements for a given product type
- a developer or group of developers of similar products wishing to establish a minimum baseline for that product type
- a government or a large corporation specifying its requirements as part of its acquisition process

PROTECTION PROFILES BY CATEGORY

- Access Control Devices and Systems (8 PP)
- Biometric Systems and Devices (6 PP)
- Boundary Protection Devices and Systems (14 PP)
- Data Protection (18 PP)
- Databases (1 PP)
- ICs, Smart Cards and Smart Card-Related Devices and Systems (87 PP)
- Key Management Systems (4 PP)
- Mobility (5 PP)
- Multi-Function Devices (2 PP)
- Network and Network-Related Devices and Systems (16 PP)
- Operating Systems (2 PP)
- Other Devices and Systems (82 PP)
- Products for Digital Signatures (21 PP)
- Trusted Computing (10 PP)

EVALUATION ASSURANCE LEVELS (EAL)

Levels of confidence established by the evaluation process that the security functionality of an IT product and the applied assurance measures meet the stated requirements

Greater assurance results from a greater evaluation effort, based upon

- scope (portion of the IT product evaluated)
- depth (level of design and implementation detail considered)
- rigour (how much structured and formal the evaluation is)

EAL1: functionally tested (lower level)

EAL2: structurally tested

EAL3: methodically tested and checked

EAL4: methodically designed, tested and reviewed

EAL5: semiformally designed and tested

EAL6: semiformally verified design and tested

EAL7: formally verified design and tested (upper level)

LIMITATIONS OF COMMON CRITERIA

Complex evaluation process

- time
- cost

Product evaluation through the CC schema is suitable to

- equipment for military forces
- critical infrastructures (nuclear and chemical plants, etc.)

The "connection of everything" to the network requires novel certification schemes

- fast enough to cope with the release of new versions
- larger base of certification laboratories

EUROPEAN UNION CYBERSECURITY CERTIFICATION

EU cybersecurity certification schemes

- required by the EU Cybersecurity Act (2019), defining a framework for their development
- developed by ENISA

Main actors:

Product vendors and service providers

National Cybersecurity Certification Authorities (NCCAs)

Conformity Assessment Bodies (CABs)

Users of Certificates

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN UNION CERTIFICATION FRAMEWORK

Up to three levels of assurance in schemes are foreseen to tackle different levels of risk associated with the intended use of ICT solutions

Basic

Minimising the known basic risks of incidents and cyberattacks

Substantial

Minimising the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

High

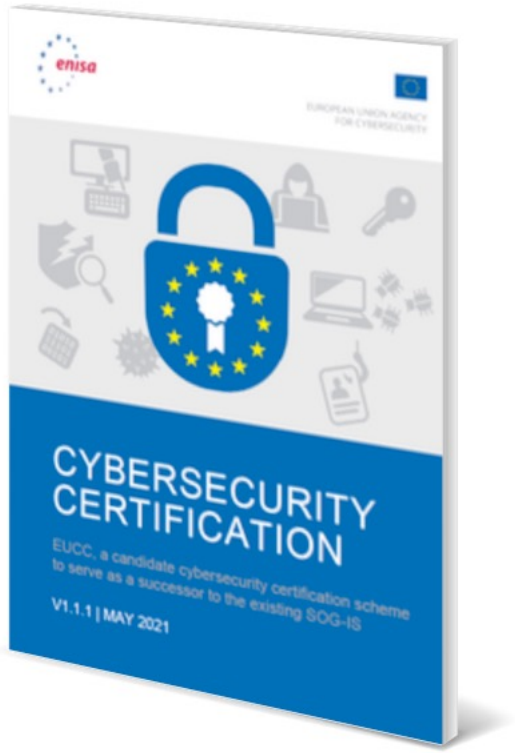
Minimising the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources

EU CYBERSECURITY CERTIFICATION SCHEME

Current version: V1.1.1 – May 2021

Based on

- Common Criteria (ISO/IEC 15408)
- Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)



OTHER CERTIFICATIONS

SERVICE PROVIDERS AND ORGANISATIONS

CYBER ESSENTIALS

Cyber Essentials

- UK Government-baked scheme (2014)
- main goals
  - helping organisations to protect against the most common cyber threats
  - demonstrating commitment to cyber security
- required by some central UK government contracts that involve
  - handling sensitive and personal information
  - provision of certain technical products and services

Two kinds of certifications

- Cyber Essentials: **self** certification
- Cyber Essentials Plus: certified by an **external** organization

Essential requirements

- boundary firewalls and internet gateways
- secure configuration
- access control
- malware protection
- patch management