SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M7 - Certification of products and technologies

Contents

7. Certification of products and technologies

- Common Criteria (ISO/IEC 15408) and FIPS 140 for cryptography
- Italian law on certification of products and technologies
- Payment Card Industry Data Security Standard (PCI) - Data Security Standard (DSS)

Effective security system

DEFINED BY FISP 140-2

*“The primary goal in designing an effective security system is to make the cost of any attack **greater** than the possible **payoff**”*

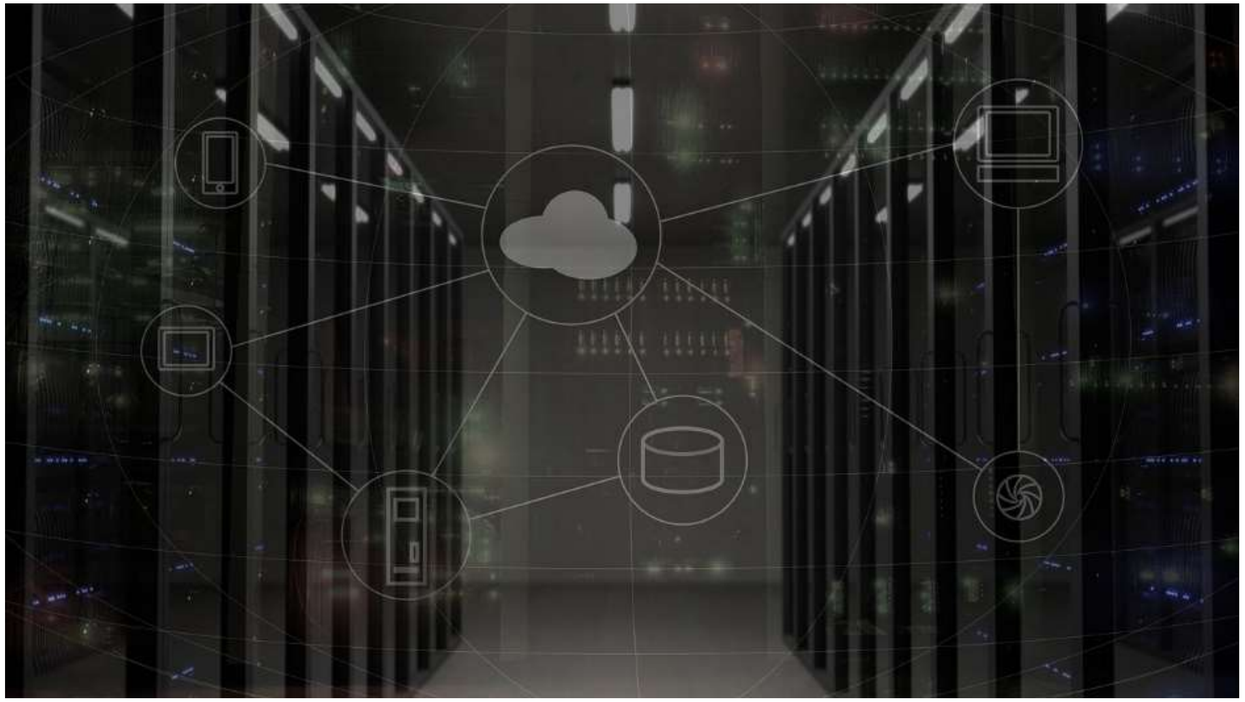
[Source: FIPS PUB 140-2]

Common Criteria

ISO / IEC 15408

Technology assessment and certification

The evaluation of technologies and IT products (hardware, software or firmware) is a difficult problem to solve, as it is not easy to find universal rules.
However, there are methods to demonstrate reliability that can be placed in the security measures of an IT product. One of the best known refers to the so-called **Common Criteria**, currently considered the most reliable. (they are also known as “**CC**” and the ISO / IEC 15408 standard has transposed them).



Actual version of CC: April 2017, V. 3.1, Revision 5

Common Criteria

ISO / IEC 15408

Structure of CC

Part 1, Introduction and general model is the introduction to the CC. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.

[Source: www.commoncriteriaportal.org]

Common Criteria

ISO / IEC 15408

Part 2, Security functional components establishes a set of functional components that serve as standard *templates* upon which to base functional requirements for TOEs.
CC Part 2 catalogues the set of functional components and organises them in **families** and **classes**.

[Source: www.commoncriteriaportal.org]

Common Criteria

ISO / IEC 15408

Part 3, Security assurance components establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs. CC Part 3 catalogues the set of assurance components and organises them into **families** and **classes**.

CC Part 3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance **packages** which are called the Evaluation Assurance Levels (EALs).

[Source: www.commoncriteriaportal.org]

Common Criteria

ISO / IEC 15408

The standard provides for seven increasing levels of assurance, from EAL1 (Evaluation Assurance Level) to EAL7, which depend on the **extent** and **formality** of the documentation used during the analysis and development phases, but also on the development **methods**.

The Common Criteria contain a grouping of 60 security functional requirements in 11 classes. This grouping allows specific classes of requirements to be evaluated in a standard way in order to arrive at an Evaluation Assurance Level.

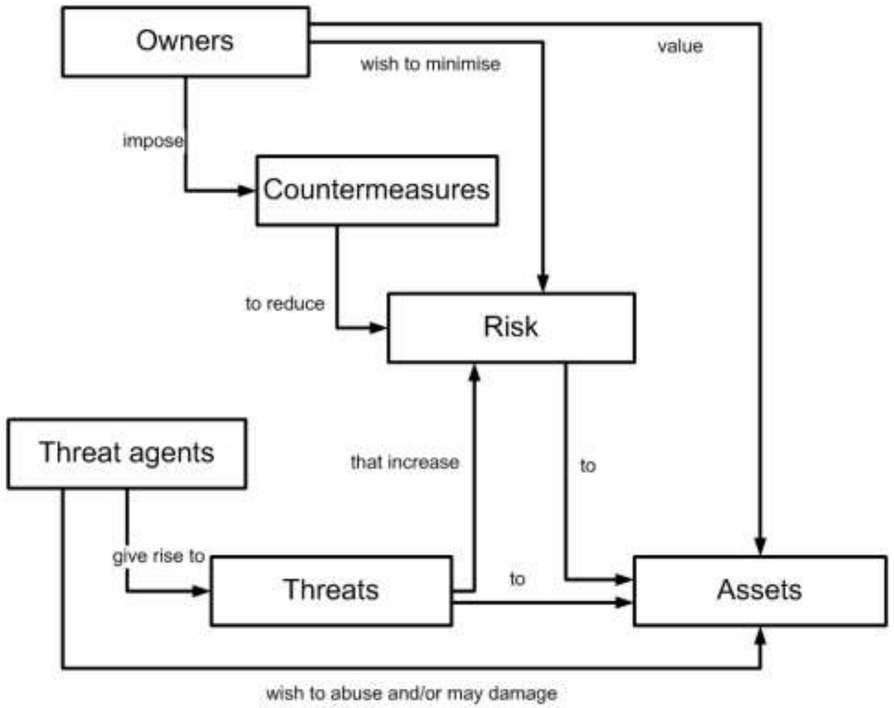
[Source: www.cisa.gov]

Common Criteria

ISO / IEC 15408

General model

assets are protected from threats by countermeasures. Figure 2 illustrates these high level concepts and relationships.



[Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model]

Common Criteria

ISO / IEC 15408

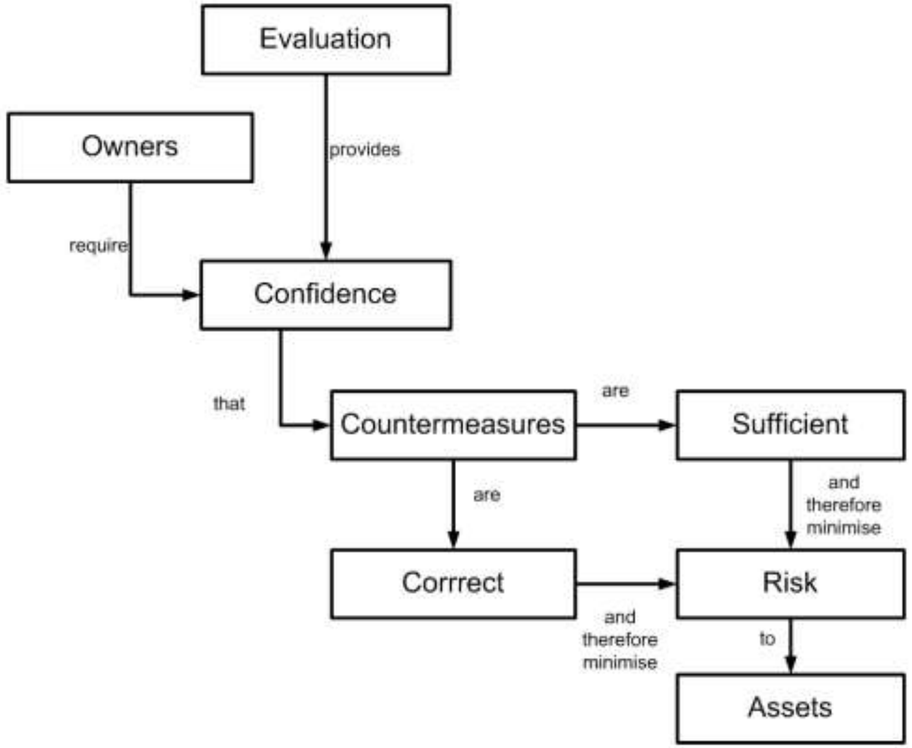
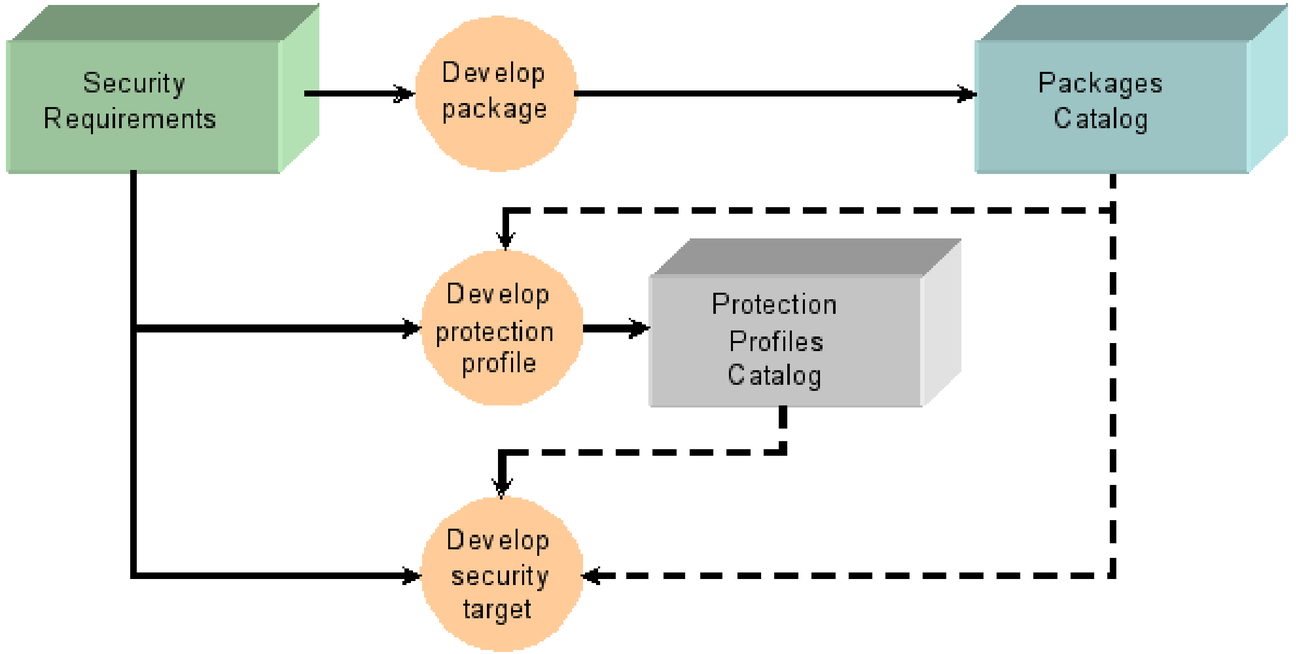


Figure 3 - Evaluation concepts and relationships

[Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model]

Common Criteria

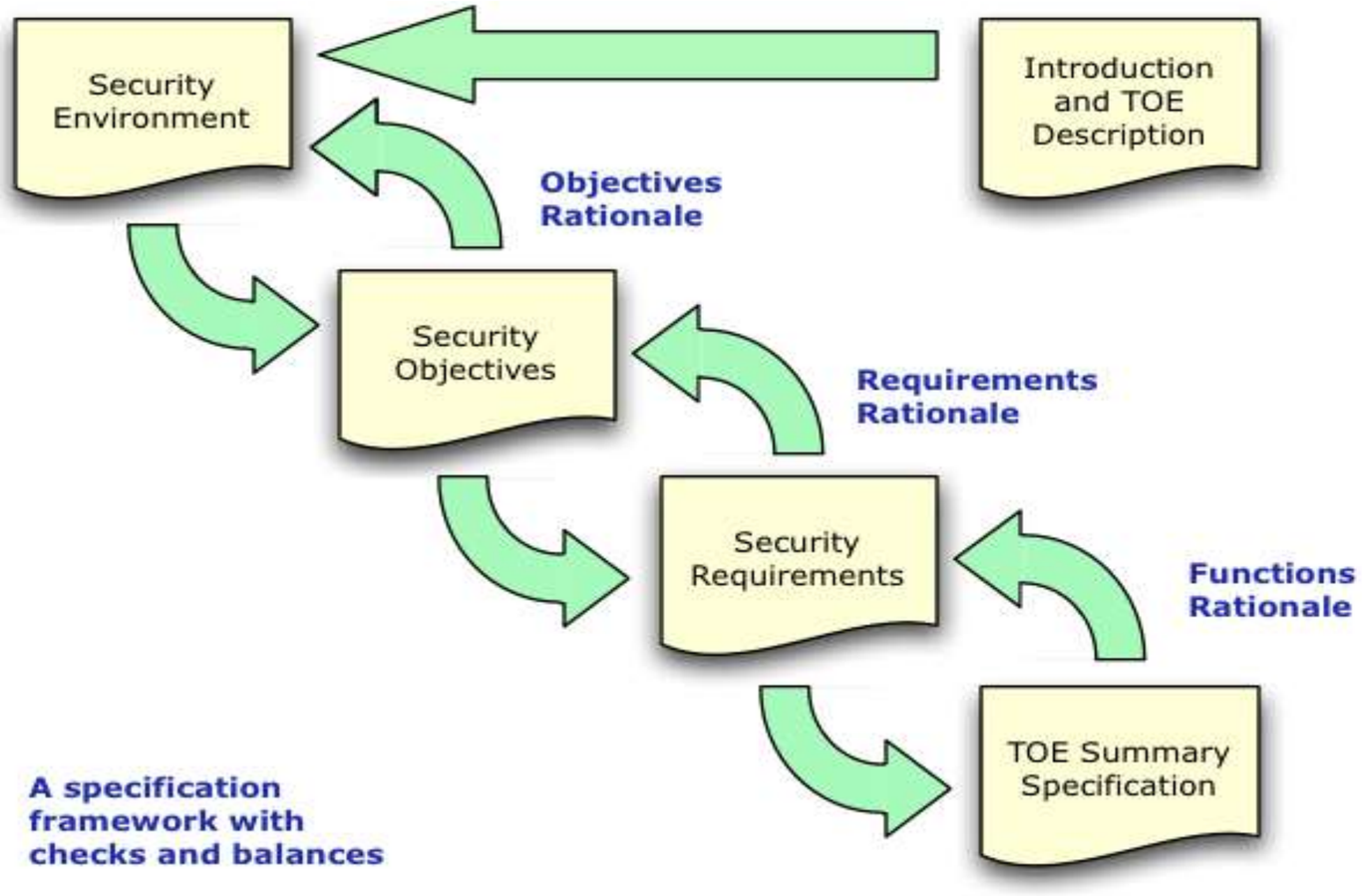
ISO / IEC 15408



[Source: www.cisa.gov]

Common Criteria

ISO / IEC 15408



[Source: www.cisa.gov]

Common Criteria

ISO / IEC 15408

Something to be careful about:

The *onerousness* of the *assessment* can lead a manufacturer to choose to certify only part of the security functions of their product. A dishonest seller, however, could use the same system to *mask* the presence of security functions for some reason "*weak*", by having only the functions evaluated sufficiently robust.

Common Criteria

ISO / IEC 15408

For instance, if for some reason a specific function of some device *has not been included* in the evaluated configuration (perhaps because it is vulnerable to some type of attack or because it is deliberately obsolete for backward compatibility reasons), the enabling of one of these functions would pose a serious risk to the system. The sense of trust that is placed in the certification may lead us not to consider its actual '**perimeter**'. This is not always known.

It is necessary to have trained personnel who adopt the **appropriate procedures** to configure the product correctly even at the cost of limiting its functionality.

Common Criteria

ISO / IEC 15408

ISO/IEC 15408-5 called “*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*” is under development and the release date should be 05-2022.

Federal Information Processing Standard (FIPS) 140-2

Federal Information Processing Standard (FIPS) 140-2 is one of the main standard for validating the effectiveness of cryptographic **modules**. If a product has a FIPS 140-2 certificate, you know it has been formally tested and validated by the **governments** of the United States and Canada.

Although FIPS 140-2 is a US / Canadian federal standard, FIPS 140-2 compliance has been widely adopted around the world

in both government and non-government sectors as a practical safety benchmark and realistic best practice.

Federal Information Processing Standard (FIPS) 140-2

This standard requires specialized **laboratories** to identify and test a particular *hardware, software* or *firmware* module.

Cryptographic modules can be produced by the private sector (also by open source community) or public for use by particular sectors (e.g. health, finance) and in general the critical infrastructures that make use of these modules to process **sensitive** information.

Federal Information Processing Standard (FIPS) 140 - 11 areas of control

- *Cryptographic module specification* (what must be documented)
- *Cryptographic module ports and interfaces* (what information flows in and out, and how it must be segregated)
- *Roles, services and authentication* (who can do what with the module, and how this is checked)
- *Finite state model* (documentation of the high-level states the module can be in, and how transitions occur)
- *Physical security* (tamper evidence and resistance, and robustness against extreme environmental conditions)
- *Operational environment* (what sort of operating system the module uses and is used by)
- *Cryptographic key management* (generation, entry, output, storage and destruction of keys)
- *EMI/EMC*
- *Self-tests* (what must be tested and when, and what must be done if a test fails)
- *Design assurance* (what documentation must be provided to demonstrate that the module has been well designed and implemented)
- *Mitigation of other attacks* (if a module is designed to mitigate against, say, TEMPEST attacks then its documentation must say how)

Federal Information Processing Standard (FIPS) 140-2

Organizations use the FIPS 140-2 standard to ensure that selected hardware meets specific security requirements. The FIPS certification standard defines **four** increasing quality security levels:

Level 1: Requires production-grade equipment and externally tested algorithms.

Federal Information Processing Standard (FIPS) 140-2

Level 2: Adds requirements for physical tamper evidence and role-based authentication. Software implementations must run on an EAL2 level Common Criteria approved operating system.

Federal Information Processing Standard (FIPS) 140-2

Level 3: Adds requirements for physical tamper resistance and identity-based authentication. There must also be a physical or logical separation between the interfaces according to which "critical safety parameters" enter and exit the module. Private keys can enter or exit only in encrypted form.

Federal Information Processing Standard (FIPS) 140-2

Level 4: This level makes physical security requirements more stringent, requiring the ability to be tamper-proof, wiping the contents of the device if it detects various forms of environmental attack.

Federal Information Processing Standard (FIPS) 140-2

Internationally, the equivalent of FIPS 140-2 is ISO / IEC 19790: 2012 with the title ‘Security requirements for cryptographic modules’. ISO / IEC 24759: 2014 (Information technology - Security techniques - Test requirements for cryptographic modules) is the equivalent of the NIST Derived Test Requirements document.

Federal Information Processing Standard (FIPS) 140-3

FIPS 140-3 approved

On March 22, 2019, the Secretary of Commerce approved **Federal Information Processing Standards Publication (FIPS) 140-3**, ***Security Requirements for Cryptographic Modules***, which supersedes FIPS 140-2. This was announced in the Federal Register on May 1, 2019. FIPS 140-3 aligns with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the Cryptographic Module Validation Program (CMVP), as a validation authority. The testing for these requirements will be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2. Major changes in FIPS 140-3 are limited to the introduction of non-invasive physical requirements.

[source: csrc.nist.gov]

Federal Information Processing Standard (FIPS) 140-3

While FIPS 140-2 continues on through 2026, **development** to **support** and **validate** FIPS 140-3 modules must be in place by September **2020**.

This project addresses questions concerning the process of migrating from FIPS 140-2 to FIPS 140-3. The transition process includes organizational, documentation and procedural changes necessary to update and efficiently manage the ever increasing list of security products that are tested for use in the US and Canadian governments.

Changes also support the migration of internally developed security standards towards a set of standards developed and maintained by an international body, while also referencing government standards.

[source: csrc.nist.gov]

Italian National ICT Security Assessment Scheme

National ICT Security Assessment Scheme (“*Schema Nazionale di Valutazione della Sicurezza ICT*”)

The National Scheme collects all the procedures and rules necessary for the evaluation and certification of ICT systems or products or Protection Profiles , in compliance with the European ITSEC or Common Criteria. The National Scheme does not apply to systems and products that handle classified information.

[Source: atc.mise.gov.it]

Italian National ICT Security Assessment Scheme

The procedures relating to the National Scheme, described in detail in the Guidelines, must be observed by the Certification Body (OCSI), by the Laboratories for Safety Assessment (LVS), as well as by all those (individuals, legal entities and any other subject) that operate within the national scheme.

[Source: atc.mise.gov.it]

Italian National ICT Security Assessment Scheme

The figures that operate in the scheme

In addition to the OCSI, the following entities operate within the National Scheme:

- **Safety Assessment Laboratories (LVS**): carry out assessment activities under the control of the OCSI
- the **Client** : is the person who commissions the evaluation and can coincide with the Supplier
- the **Supplier** : is the person who provides the Object of the Assessment (ODV)
- the **Assistant** : is a person trained, trained and authorized by OCSI to provide technical support to the Client or Supplier

[Source: atc.mise.gov.it]

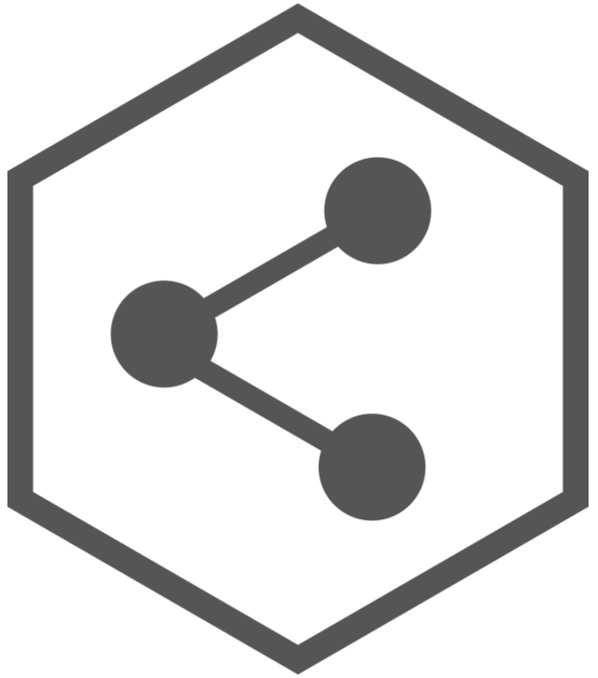
CVCN - Centro di Valutazione e Certificazione Nazionale

With the decree-law n. 105 of 2019, converted into law no. 133 of the same year - which defines the national cyber security perimeter - the National Evaluation and Certification Center (CVCN) - set up at the Ministry of Economic Development - was entrusted with the task of carrying out the assessment of ICT **goods**, **systems** and **services** intended to be used on ICT infrastructures that support the provision of **essential services** or **essential functions** for the State.

[Source: atc.mise.gov.it]

CVCN - Centro di Valutazione e Certificazione Nazionale

the subjects included in the national security perimeter, pursuant to article 1, paragraph 6, of law decree no. 105/2019 are required to **communicate** to the CVCN **their intention to acquire ICT goods**, **systems** and **services** to be used on their "*strategic*" assets belonging to certain categories identified on the basis of specific technical criteria. The CVCN, within a maximum time of 60 days from the communication, indicates to the subject included in the perimeter *any conditions to which the suppliers must comply and hardware and software tests that must be carried out*.



[Source: atc.mise.gov.it]

CVCN - Centro di Valutazione e Certificazione Nazionale

Any conditions and tests are **included** in the calls for tenders and contracts with clauses that condition the contract on compliance with the conditions and the favorable outcome of the tests ordered by the CVCN. The tests can be carried out in the CVCN laboratories or in *test laboratories* accredited by the CVCN itself and must be completed within sixty days.

Since the Ministry of Defense and the Ministry of the Interior can make use of their own Assessment Centers - CVs - for acquisitions destined for their networks, information systems and IT services, the CVCN will have to liaise with these Assessment Centers to prevent the supplier from carrying out several times the tests on the same product.

[Source: atc.mise.gov.it]

CVCN - Centro di Valutazione e Certificazione Nazionale

With the Decree of the President of the Republic February 5, 2021, n. 54, the procedures, methods and terms of operation of the CVCN have been **defined**, as well as the procedures for verifying compliance with the provisions of decree-law no. 105/2019, as well as the technical criteria for identifying the categories of **goods**, **systems** and **ICT services** (to be carried out with DPCM) that will be subject to the evaluation of the CVCN in the event that they are intended for "strategic" assets. These categories were identified with the Prime Ministerial Decree of 15 June 2021

[Source: atc.mise.gov.it]

CVCN - Centro di Valutazione e Certificazione Nazionale

Recently the regulatory scenario in the field of cybersecurity was revisited with the issue of the decree-law of 14 June 2021, no. 82 converted into law no. 109, which defined the national cybersecurity architecture and established the **National Cybersecurity Agency**. In the new context, the National Assessment and Certification Center (CVCN) is transferred to the Agency and its operation is ensured from *30 June 2022*.

In the coming months, the regulatory framework will be completed with the approval of the Prime Ministerial Decree which defines the procedures for the accreditation of the test laboratories and the methods of linking the CVCN with the CVs.

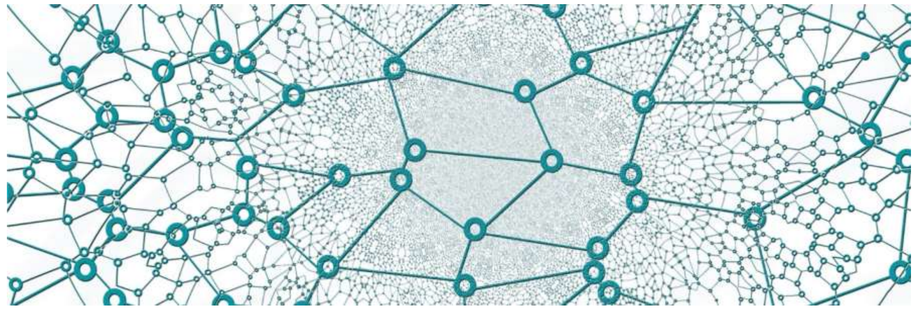
[Source: atc.mise.gov.it]

ACN and CVCN

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

National Assessment and Certification Center

The CVCN is the technical structure that, together with a network of accredited laboratories, will be responsible for verifying the **security** and **absence of known vulnerabilities** in ICT goods, systems and services, with the aim of raising the level of cybersecurity and resilience of the infrastructures on which the country's essential functions and services depend.



Currently being transferred from the Ministry of Economic Development (MiSE), it will enter into operation from **30 June 2022**.

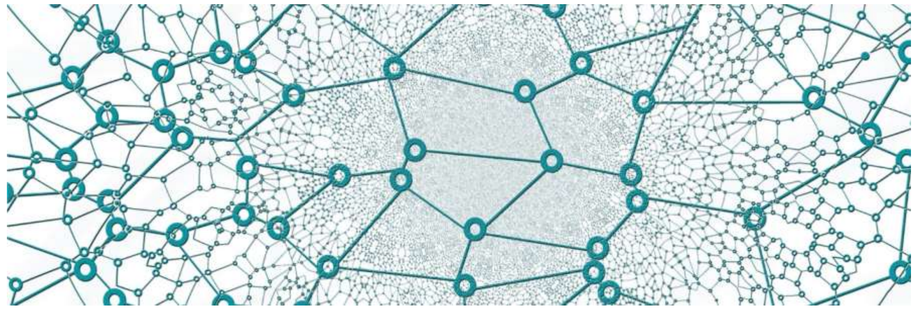
ACN and CVCN

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Tasks and functions

The CVCN will have the task of carrying out **preliminary** checks on the assignment procedures and may impose *conditions* and *tests* aimed at the security analysis of hardware or software on some components of the supply that may be particularly sensitive if compromised by a cyber attack.

[Source: acn.gov.it]



PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI Security Standards are developed specifically to protect **payment account data** throughout the payment **lifecycle** and to enable technology solutions that **devalue this data** and **remove the incentive** for criminals to steal it.

They include standards for *merchants*, *service providers*, and *financial institutions* on security practices technologies and processes, and standards for *developers* and *vendors* for *creating secure payment products* and *solutions*.

[Source: it.pcisecuritystandards.org]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI DSS is a cybersecurity standard born in **2006** when the world leading card issuers formed the ***Payment Card Industry Security Standards Council*** . Developed to prevent data theft of payment card holders and make transactions through these cards safer, it is a very important tool.

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

About the PCI DSS

PCI DSS stands for *Payment Card Industry Data Security Standard* and is a proprietary standard for cybersecurity managed by the **PCI Security Standards Council** (PCI SSC). This standard applies to organizations that store, process or transmit data relating to credit card holders, such as merchants, buyers, issuers and service providers. **PCI DSS** is the gold **standard** for consumer protection and helps reduce fraud and data breaches across the payments ecosystem. It applies to all organizations that accept or process payment cards, therefore, also to structures in the hospitality sector. When implemented correctly, **PCI DSS** can help these organizations secure their own and their customers' data.

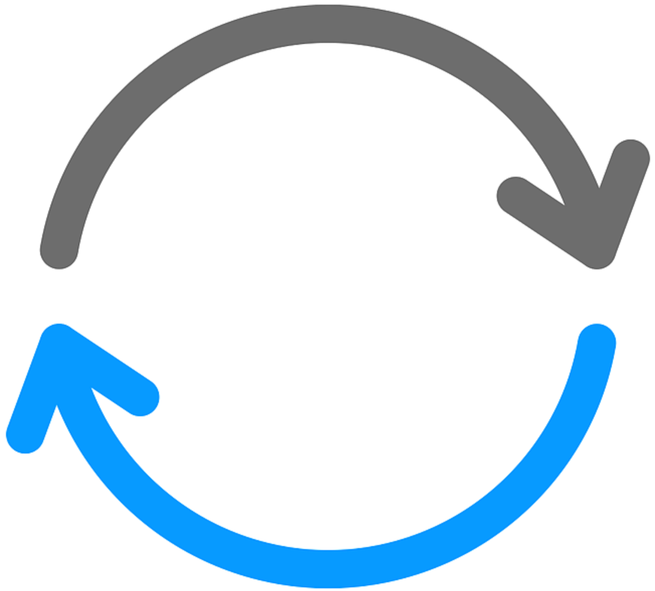
PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

WHO ISSUES THE CERTIFICATE AND HOW TO OBTAIN THE PCI DSS

The **Payment Card Industry Security Standards Council** is the body that issues the PCI DSS certificate. But **how to get PCI DSS certification** ? It can be done in two ways:

- Through self -certification , by completing an SAQ (Self Assessment Questionnaire) form and an AOC (Attestation of Compliance) form.
- By contacting a QSA (Qualified Security Assessor) company that issues the certification.



PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

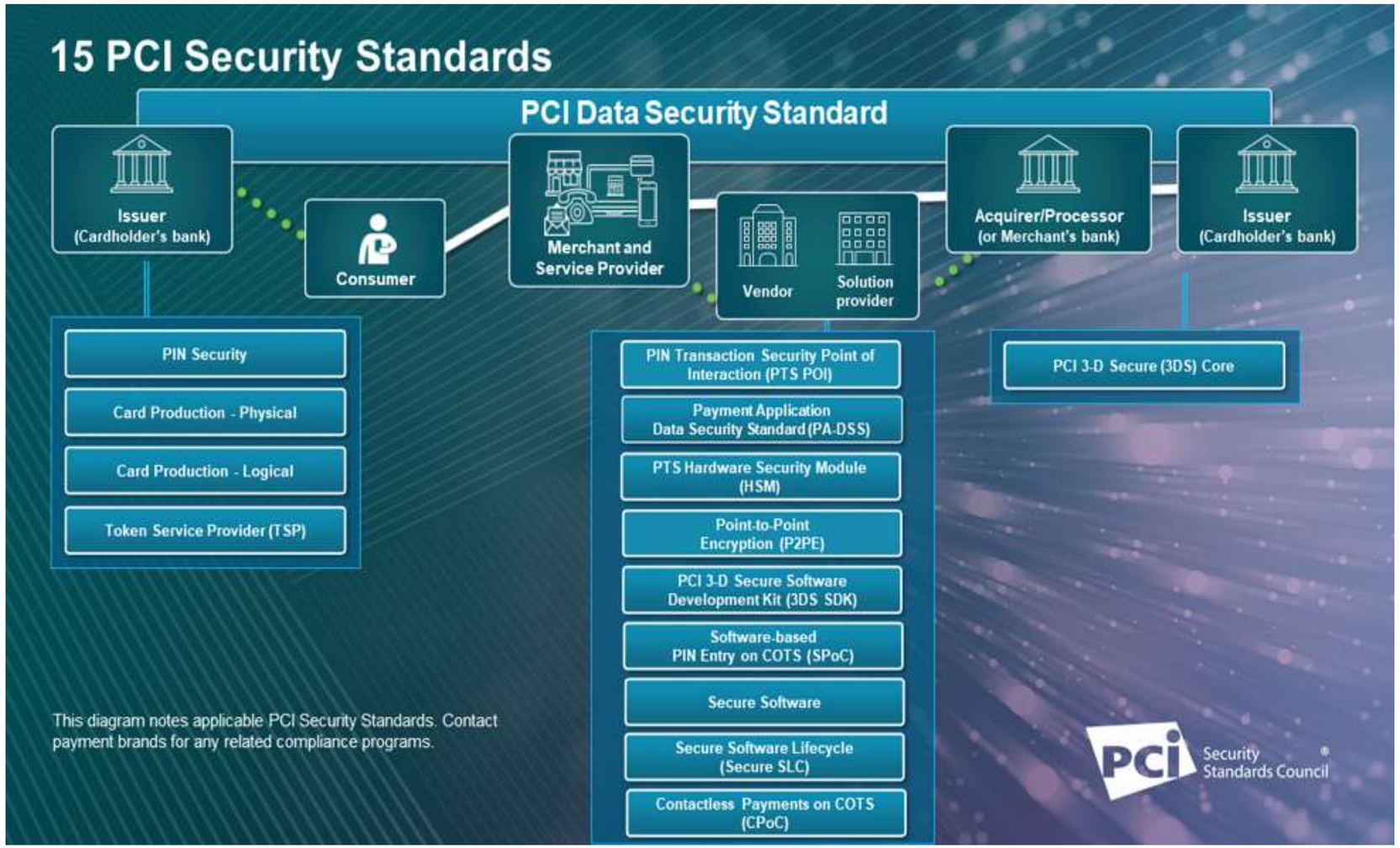
PCI DSS CERTIFICATION: THE REQUIREMENTS

A company must meet certain **requirements** to be **PCI DSS compliant** . These requirements concern the ways in which cardholder data is stored, processed and transmitted, but also how card data *flows*, how it is stored and *which IT systems are used*.

The PCI-DSS certification was created to guarantee the protection of credit card holder data and indicates precise requirements for procedures, network architecture and software that must be met by the companies that manage credit card numbers.

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD



[Source: it.pcisecuritystandards.org]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Hackers want cardholder data. By obtaining the Primary Account Number (PAN=cardholder data) and sensitive authentication data, a thief can **impersonate** the cardholder, **use** the card, and **steal** the cardholder's identity.

[Source: it.pcisecuritystandards.org]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Sensitive cardholder data can be stolen from many places:

- *Compromised card reader*
- *Paper stored in a filing cabinet*
- *Data in a payment system database*
- *Hidden camera recording entry of authentication data*
- *Secret tap into your store's wireless or wired network*

[Source: it.pcisecuritystandards.org]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Cardholder data can be secured where it is captured at the point of sale and as it flows into the payment system. The best step you can take **is to not store any cardholder data**. This includes protecting:

- *Card readers*
- *Point of sale systems*
- *Store networks & wireless access routers*
- *Payment card data storage and transmission*
- *Payment card data stored in paper-based records*
- *Online payment applications and shopping carts*

[Source: it.pcisecuritystandards.org]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

[Source: PCI-DSS v.4]

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

This document, the Payment Card Industry Data Security Standard Requirements and Testing Procedures, consists of the **12** PCI DSS principal requirements, **detailed** security requirements, corresponding **testing** procedures, and **other** information pertinent to *each* requirement.

[Source: PCI-DSS v.4]

Some online resources

Common Criteria – Part 1 , 2 and 3

Nist FIPS 140-3

Agenzia per la cybersicurezza nazionale

PCI DSS (at a glance)

PCI DSS document library

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M7 - Certification of products and technologies