TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY ASSESSMENTS

Certification Uptake & State of Play
2021-2025

JULY 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT
For contacting the authors, please use certification@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS
ENISA

ISBN 978-92-9204-795-5 DOI 10.2824/1383820 TP-01-26-011-EN-N

1. Table of Contents

Executive Summary

Considering the main third-party cybersecurity assessment methodologies applicable to ICT products, cloud services, ISMS, and managed security services, as well as the number of assessment bodies involved, this report provides an overview of the evolution of the cybersecurity assessment market over the past five years.

The objective of this study is to analyse and better understand the development of the cybersecurity assessment market and to identify potential future impacts of upcoming EU cybersecurity certification schemes. Particular attention is paid to areas where private schemes have emerged or where methodologies have been adapted, for example to address challenges such as time-to-market for certificates within existing national frameworks that may progressively be replaced by EU-level schemes.

Looking at ICT products, apart from the arrival of EUCC it may be observed that the number of schemes and assessment methodologies has remained stable. The upcoming of the first EUCC certificates means the end of the delivery of national ones under the SOG-IS agreement after more than 20 years.

ICT products represent a significant part of the total market of cybersecurity assessment all schemes combined. As seen in Figure 1 successful assessments of ICT products, including IoT labels, in the last 5 , the growth was significant in 2025. This was due to the increase of the IT Security Label issued by BSI and Singapore. Nonetheless, it is remarkable how the ICT cybersecurity certification market is gaining momentum in the market.

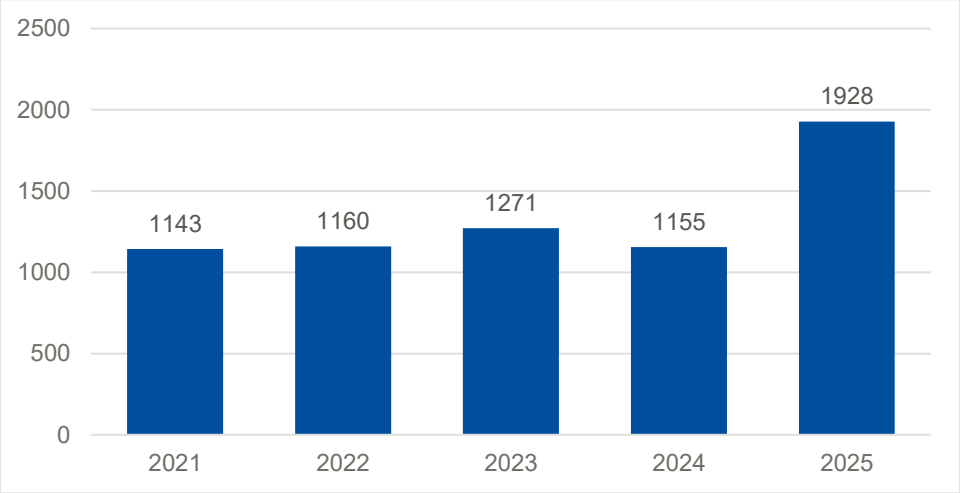


Figure 1 successful assessments of ICT products, including IoT labels, in the last 5 years.

In the following figure, it has been included only the ICT certificates without the IoT category, that is, without IT Security Label issued by BSI, IoXT alliance and IoT label from Singapore. It can be observed how the market keeps growing despite the normal fluctuations in each scheme. It is expected that the entry into force of EUCC and different regulations at EU level (e.g. CRA) and worldwide will impact significantly in the following years.

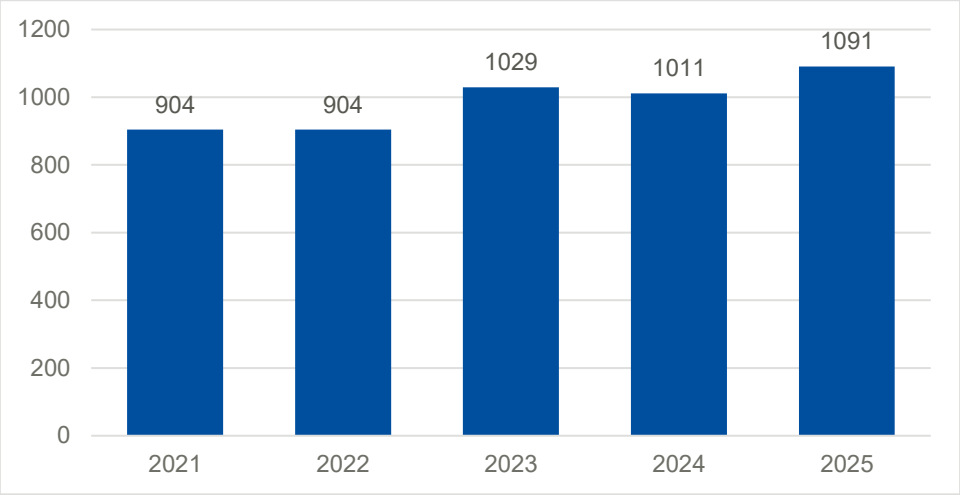


Figure 2 Total ICT products certificates in the last 5 years.

Regarding Information Security Management Systems and Cloud Services, there are fewer assessment frameworks. ISO/IEC 27001 stands out in terms of number of certified Information Security Management Systems with a record number in 2024 (data for 2025 is not available at the date of publication of this report). Moreover, the number of ISMS & Cloud Services certificates have increased significantly in the last year due to the growth of CPSTIC Cloud Evaluations, FedRAMP and IT-Grundschutz.

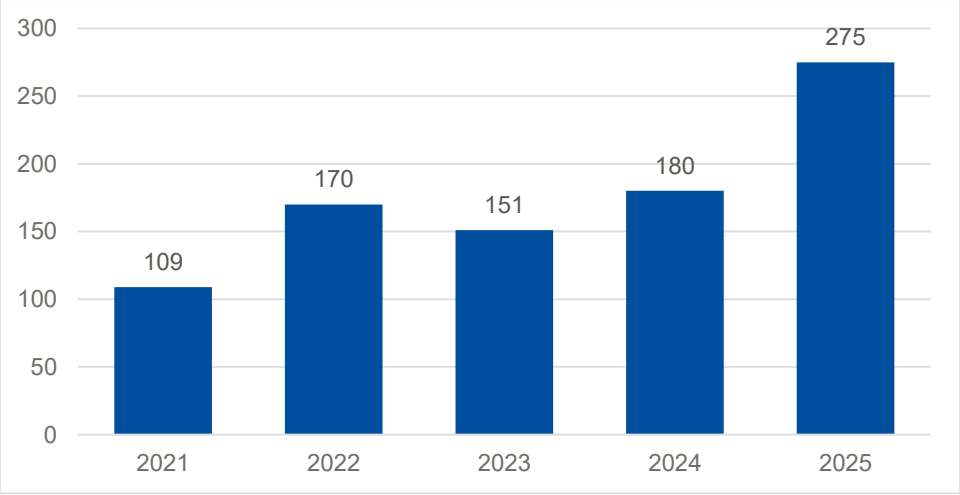


Figure 3 Total ISMS & Cloud Services certificates (Without ISO/IEC27001) in the last 5 years.

Managed Security Services is the new category of services addressed in the report, the scope of activities under this denomination is larger and encompass different type of services. While some European member states approached the topic in a horizontal way, the study highlights a segmented market with no existing common denominator.

Cornerstone of third-party evaluations, the report aims also at highlighting the number of accredited laboratories or conformity assessment bodies for the different assessment frameworks. The numbers show that the cybersecurity Certification market is growing worldwide, and the European Union has significant capabilities. Regarding the Common Criteria scheme for ICT products, 52% of the total

assessment bodies are in Europe. But 2025, marks a turn as first EUCC certificates were issued and new ITSEFs and CBs are expected to be accredited and authorised.

Introduction

The Cybersecurity Assessment report aims to present the current state of play of cybersecurity assessments of ICT products, cloud services, ISMS, and managed security services along with the conformity assessment bodies involved with such schemes.

This present version is an update from the initial report[1] published in January 2024. Some frameworks have been removed from the study[2] due to lack of data or irrelevance.

The two major changes are the introduction of data regarding the first EU cybersecurity certification scheme, EUCC, and the inclusion of a new category of ICT solutions: managed security services. The type of MSSs included in the report is based on the definition and examples of activities provided in the targeted amendment of the Cybersecurity Act[3] giving the mandate to ENISA to develop certification schemes for such activities.

To study the dynamic of the related market, the report focuses on the evolution of the number of assessed ICT solutions and assessment bodies in the past 5 years, between 2021 and 2025. It considers the several ways to assess cybersecurity of ICT solutions such as standards, national, and private, certification schemes and methodologies.

The report also focuses on conformity assessment bodies, the cornerstone of cybersecurity assessments.

Ultimately, with this report ENISA wants to track the uptake of the new EU cybersecurity certification scheme such as EUCC.

[1] ENISA Certification website: Report Market of Cybersecurity Assessments 2018-2022, https://certification.enisa.europa.eu/publications/market-cybersecurity-assessments-2018-2022_en
[2] Removed and added categories can be found in Appendix 3
[3] Consolidated text: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) EUR-Lex - 02019R0881-20250204 - EN - EUR-Lex

Methodology

The report contains a quantitative analysis of the market. For each of the different conformity assessment methodologies and related schemes, the following information has been provided:

- Description and introduction (including: the scope, validity of the certificate and mutual recognition between certificates).
- Statistics of the last 5 years (number of approved/certified/listed products or solutions per year).

The assessment frameworks and methodologies presented in the report were selected after consultation with stakeholders involved in the EU Cybersecurity Certification Ad-Hoc Working Groups. Following the CSA targeted amendment and introduction of a new family of activities entering the scope of EU cybersecurity certification, it has been decided to include the major existing national certification schemes on managed security services to display the dynamic and level of maturity for each different type of Managed security service. To improve the readability of the report, schemes that do not longer have activity or for which the data cannot be obtained, have been removed.

For instance, the report does not consider the following conformity assessment methodologies:

- Cybersecurity labels relying on the made-in criterion, which is based on location where the solution is developed: such as France Cybersecurity Label or Made in Europe Label.
- Outdated methodologies like FIPS 140-1.
- Schemes related to production or evaluation sites such as Site Certification in Common Criteria or SAS for UICC Production (SAS-UP).

When counting successful assessments, only the ones issued during the year have been considered. The calculation does not include the total number of existing certificates. The numbers also do not reflect certification projects that failed and did not end with a certificate,

The 5 years' data comes from several sources such as: websites, surveys, tools, or direct contact with the schemes' owner.

In case the authors of the report have missed or misinterpreted some data, we invite the owners of the mentioned schemes to reach out to ENISA to improve the next edition.

SECTION 1

ICT Products

2. Assessments of ICT Products

ICT products such as components, chips, hardware, and software are at the core of information systems. Ensuring that these products provide an appropriate level of security is essential and is supported by recognised third-party cybersecurity assessment methodologies.

The scope of ICT products has expanded over time and now includes a broad range of digital and connected solutions, such as mobile devices, Internet of Things (IoT) devices, industrial components, secure elements, payment devices, and digital identity solutions. These products are often integrated into complex environments and interconnected ecosystems, increasing the importance of consistent and reliable security assessment practices.

Cybersecurity assessments of ICT products aim to evaluate whether a product complies with defined security requirements and whether it provides an adequate level of assurance for its intended use. Depending on the methodology, these assessments may involve documentation analysis, functional and security testing, vulnerability analysis, and, where relevant, penetration testing. The level of assurance varies according to the evaluation approach and the criticality of the product.

The landscape of ICT product assessments includes a variety of approaches, ranging from international standards and certification schemes to national frameworks and sector-specific methodologies. In addition, more recent approaches, such as fixed-time evaluations and IoT labelling schemes, have been introduced to address specific market needs, including reduced time-to-market and cost considerations.

The ICT product assessment methodologies presented in this report are organised according to their scope and evaluation approach, providing an overview of the main existing schemes and their characteristics.

2.1 Common Criteria

2.1.1 Description

Common Criteria[4] (CC) is an international family of standard (ISO/IEC 15408 and ISO/IEC 18045) and the most recognised certification used for assessing security in ICT products. The standard was developed by the governments of the U.S., Canada, Germany, France, the UK, and the Netherlands.

Common Criteria is the result of combining the CTCPEC (Canada), the TCSEC (U.S.), and the ITSEC (European) standards. Common Criteria standards support verifying that a product meets a specification of security requirements with a guarantee aligned with the level of assessment established. Depending on the Evaluation Assurance Level (EAL) the requirements of the standard increase (up to EAL 7), in accordance with the possible potential of attackers trying to tamper with the target of evaluation (TOE).

Common Criteria is a horizontal scheme, therefore several types of products are certified using Common Criteria such as telecommunication, ePassports, digital signature, etc…

Date of Creation	1994
Scope	International (more than 30 countries)
Validity of Certificate	5 years
Mutual recognition	The Common Criteria Recognition Arrangement (CCRA). gathers countries and organisations that have agreed to recognise and accept the results of security evaluations conducted under Common Criteria.

2.1.2 Statistics covering the last 5 years – Certified products according to Common Criteria

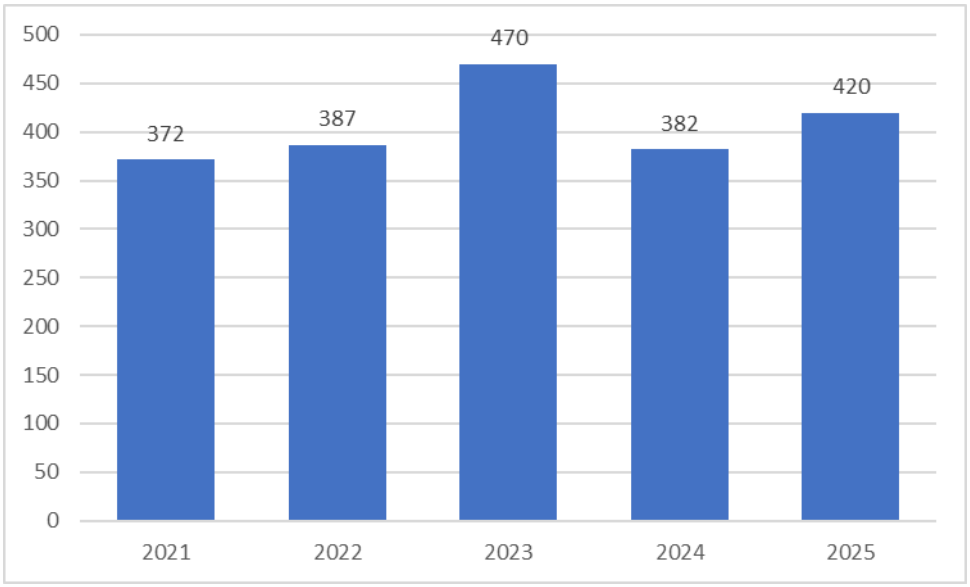


Figure 4 Common Criteria certified products worldwide in the last 5 years.

The progression in terms of the number of certified products has remained stable with some fluctuations over the past five years. Starting with 365 certificates in 2020, the number increased

[4] Common Criteria website: https://commoncriteriaportal.org/

slightly to 372 in 2021 and then to 387 in 2022. A more noticeable rise occurred in 2023, reaching 470 certificates, before declining to 382 in 2024, suggesting a return to earlier levels after a temporary peak.

2.1.3 Focus on the European Union

2.1.3.1 SOG-IS

The year 2025 is the year of twilight for SOG-IS; after more than 20 years the scheme is retiring with the entry into force of EUCC.

There are 7 countries in the European Union that can certify under the SOG-IS agreement against the Common Criteria: France, Germany, Italy, The Netherlands, Poland, Spain, and Sweden. It is important to note that the SOG-IS[5] agreement allowing mutual recognition of CC evaluation made by third parties includes both European Union (EU) member countries and countries from the European Free Trade Association (EFTA), totalling 28 countries on the list. These countries work together to improve the security of information and communication systems, facilitate cooperation, and ensure mutual recognition of information technology security evaluations and certifications within the European region.

As of February 2026, certification bodies cannot deliver SOG-IS certificates anymore. All new common criteria certificates issued by the seven historical certification bodies and the twenty new other EU Member States authorised to issue certificates under the European Union Cybersecurity Certification Scheme (EUCC) must comply with the EUCC framework. It should be expected that the number of EUCC certificates in the coming years should follow to the pattern of number of certificates shown below.

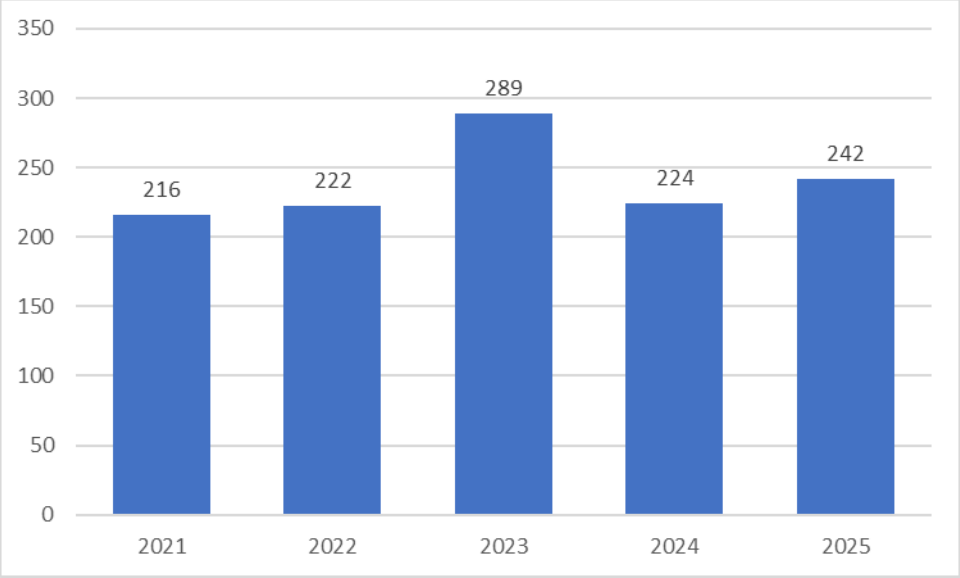


Figure 5 Common Criteria certified products – under SOG-IS- in the European Union in the last 5 years.

[5] SOG-IS Website: https://www.sogis.eu/index_fr.html

The progression in terms of the number of certified products under SOG-IS has remained stable with some fluctuations over the past five years. **The number of European Common Criteria certificates is around 60% of the worldwide Common Criteria certificates.**

Data collection

Modality	Data collected from CCScraper which is a tool developed by JTSEC.

2.1.3.2 EUCC

Adopted in January 2024, the EUCC scheme widely reuses the SOG-IS Mutual Recognition Agreement. Based on the European Cybersecurity Act, all EU Member States can now certify ICT products against two level of assurance, substantial and high.

The scheme EUCC allows private CABs to operate both for evaluation and certification activities, whereas historically, within the Common Criteria SOG-IS scheme only public Certification Bodies (CBs) were delivering certificates (except for one national scheme relying on the prior approval model).

The EUCC implementing regulation entered in adoption one year after its publication, meaning that certificates could not be issued before February 2025[6].

Date of Creation	2024
Scope	European
Validity of Certificate	5 years or more depending on scope
Mutual recognition	Not yet

2.1.4 Statistics covering the last 5 years – Certified products according to EUCC.

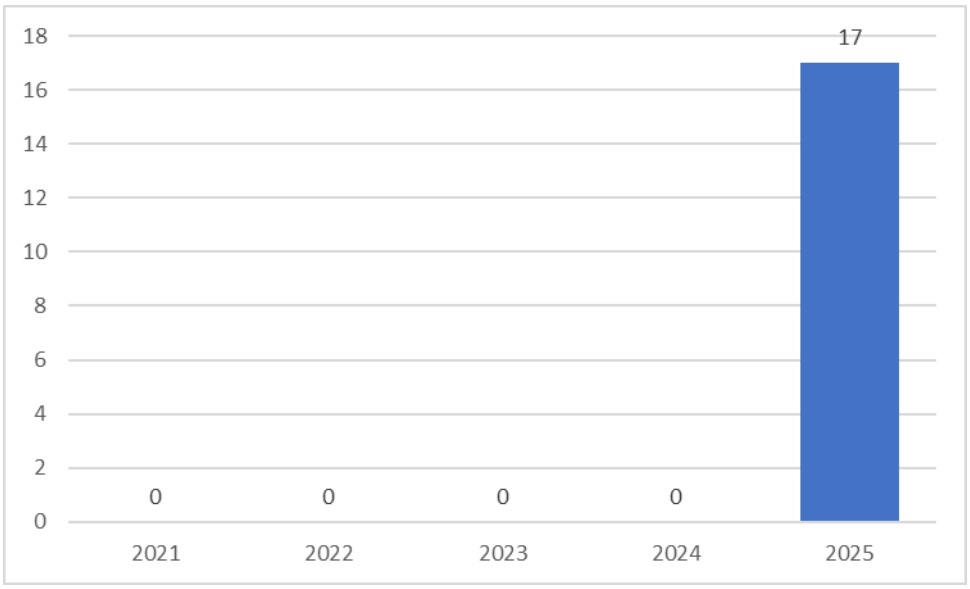


Figure 6 EUCC certified products in the last 5 years.

[6] For information, as of the date of publication of the report, 20 EUCC certificates were published for 2026.

2.1.4.1 Data collection

Modality	ENISA certification website[7].

2.2 Fixed-time methodologies

This type of methodology was created in Europe; in fact, four EU Member States (France, Germany, the Netherlands, and Spain) have developed their fixed-time methodology at national level. These methodologies have points in common such as:

- Effort and duration are known beforehand;
- Focus on vulnerability analysis and penetration testing, more emphasis on product testing than on documentation;
- In terms of assurance: not targeting assurance level like the highest assurance levels of the Common Criteria (AVA_VAN.4 and 5);
- Certification processes that SMEs can afford;
- National scope with so far only limited mutual recognition arrangement (ANSSI/CSPN – BSI/BSZ).

2.2.1 FiTCEM

The importance of these national schemes led to the development by CEN/CENELEC of EN 17640 “Fixed-time Cybersecurity Evaluation Methodology for ICT Products” (FiTCEM) inspired from the existing national methodologies from France, Spain, The Netherlands, and Germany. As mentioned on the standardisation organisation website[8], it “is the first standard that implements by design the requirements of the European Cybersecurity Act (CSA), which establishes the rules for future cybersecurity certification schemes in Europe. For this reason, it provides future CSA schemes with the necessary building blocks to conduct evaluations at the three assurance levels "basic", "substantial" and "high", together with further legal requirements. At the same time, the standard can be adapted to the requirements of specific markets requiring cybersecurity certification or in general security evaluation.”

BSZ has implemented EN 17640 (FiTCEM) since version 2.0 of November 2023 as the framework methodology for the scheme. CSPN has also declared conformity to FiTCEM. Both member States have delivered their first FiTCEM labels displaying the recognition between their evaluation methodologies.

LINCE is compliant with FiTCEM and Spain is currently developing a mapping to demonstrate it.

2.2.2 CSPN – France

2.2.2.1 Description

According to the ANSSI (Agence Nationale de la Sécurité des Systèmes d’information – National Agency for the safety of information systems) website: “The First Level Security Certification (CSPN Certification de Sécurité de Premier Niveau or The First Level Security Certification), aims to certify the robustness of a technological product, based on a conformity analysis and intrusion tests carried

[7] https://certification.enisa.europa.eu/certificates_en
[8] CEN/CENELEC website: https://www.cencenelec.eu/news-and-events/news/2022/eninthespotlight/2022-10-27-new-en-17640-helps-evaluate-the-cybersecurity-of-ict-products/

out by a CESTI (Centre d'Evaluation de Sécurité des Technologies de l'Information), an ITSEF licensed by ANSSI".

This certification addresses for a specific product version. All subsequent versions of the product must therefore be re-certified. CSPN certification applies to several types of cybersecurity products such as "secure storage," "identification, authentication, and access control," or "secure communication." Holding a CSPN allows to receive a Security Visa from ANSSI and to be part of the Security Visa Catalogue of certified solutions published by the French cybersecurity agency.

Date of Creation	2008
Scope	France
Validity of Certificate	3 years
Mutual recognition	With Germany through BSZ

2.2.2.2 Statistics covering the last 5 years - Certified products according to CSPN.

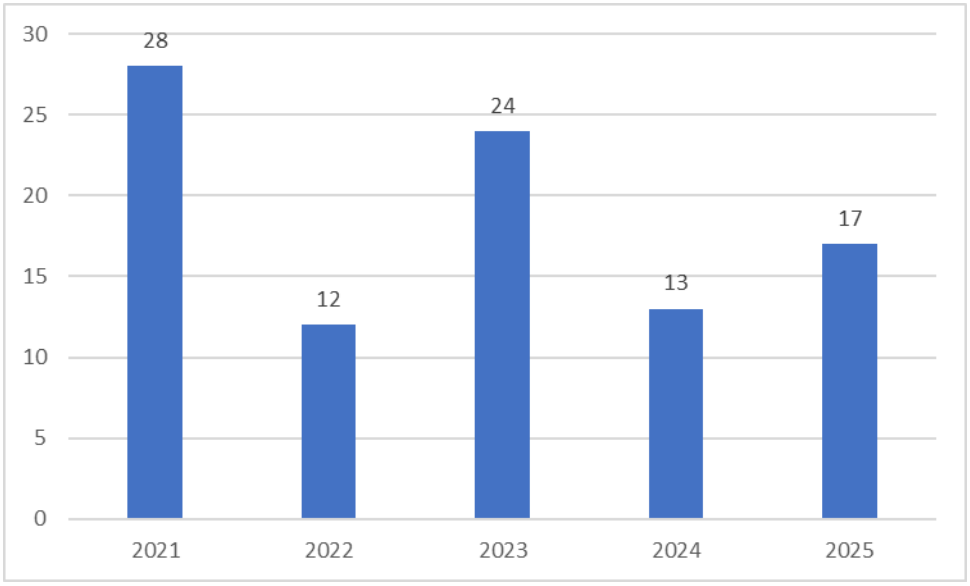


Figure 7: CSPN Certified products according in the last 5 years.

The progression in terms of the number of certified products has shown a fluctuating trend over the past five years. Starting with 28 certificates in 2021, the numbers drop sharply to 12 in 2022. A partial recovery occurred in 2023, with 24 certificates, but the figure declined again to 13 in 2024 with a light increase in 2025. Nonetheless, the need of CSPN evaluations has remained high with more than 40 evaluation processes finished per year in the last 3 years and a high rate of failed evaluations.

2.2.2.3 Data collection

Modality	ANSSI, the certification body for CSPN, provided the information.
Date of data Collection	17/04/2026

2.2.3 BSPA – The Netherlands

2.2.3.1 Description

The Baseline Security Product Assessment, BSPA, is an ICT product assessment scheme developed and maintained by NLNCSA (Nationaal Bureau voor Verbindingsbeveiliging, NBV – Netherlands National Communications Security Agency).

This scheme provides a framework in which products (both hardware and software components) can be assessed in a limited time (and cost) against a baseline of security requirements (Government security baseline). Manufacturers willing to work with Dutch government agencies are required to be Compliant to the BSPA.

Date of Creation	2015
Scope	The Netherlands
Validity of Certificate	3 years
Mutual recognition	None

2.2.3.2 Statistics covering the last 5 years – Certified products according to BSPA.

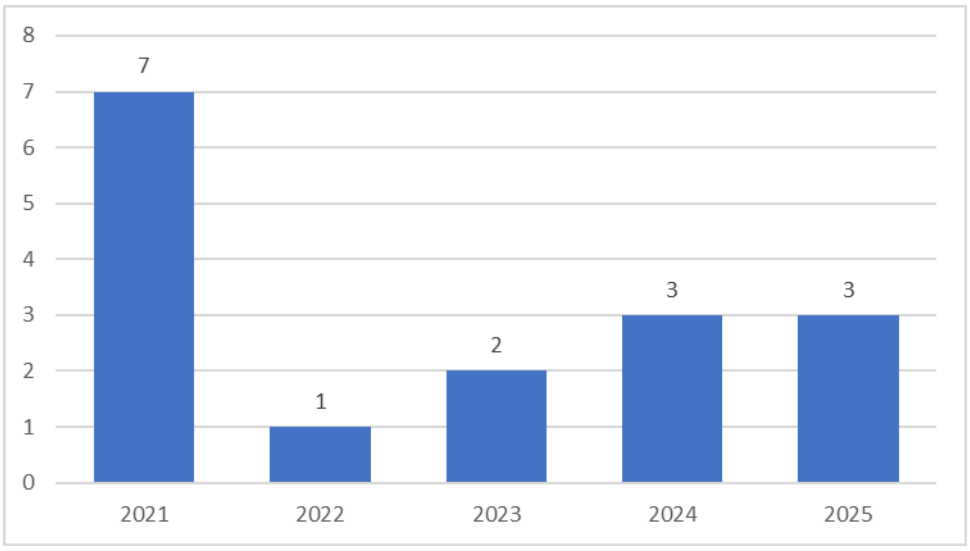


Figure 8: Certified products according to BSPA in the last 5 years.

Starting with 7 certificates in 2021, the number dropped significantly to 1 in 2022. A slight recovery followed with 2 certificates in 2023, and a further increase to 3 and 5 in 2024 and 2025, suggesting a slow but gradual rebound after the sharp decline.

2.2.3.3 Data collection

Modality	The Nationaal Bureau voor Verbindingsbeveiliging (NBV) provided the information. Therefore, the data is extracted from information provided by the Certification Body.
Date of data Collection	30/03/2026

2.2.4 LINCE – Spain

2.2.4.1 Description

LINCE (Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad)[9] is an evaluation and certification methodology for ICT security products developed by the Spanish CCN[10] (Centro Criptológico Nacional – National Cryptologic Centre). This scope-limited and time limited methodology addresses ICT products requiring certification with medium or low security criticality.

The objective of a LINCE assessment is to enable an evaluation laboratory to verify whether a product conforms to its specification by determining the effectiveness of the security functionality implemented. ICT products with a LINCE certification appear in the CPSTIC Catalogue, which is the CCN-STIC-105 reference catalogue for cybersecure ICT products in the Spanish Public Administration.

Date of Creation	2018
Scope	Spain
Validity of Certificate	5 years
Mutual recognition	None

2.2.4.2 Statistics covering the last 5 years – LINCE product according to CCN.

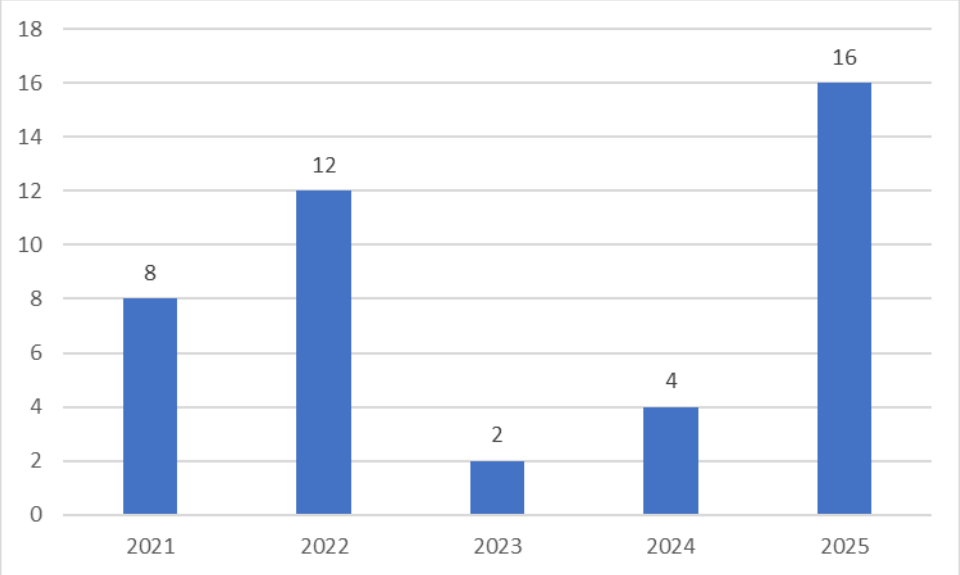


Figure 9 LINCE certified products in the last 5 years.

The number of certified products under this methodology has shown significant fluctuations over the last years. After a moderate figure of 8 certifications in 2021, the number increased notably to 12 in 2022, followed by a sharp decrease to 2 certifications in 2023. Since then, a gradual recovery can be observed, with 4 certifications in 2024, culminating in a sturdy growth reaching 16 certifications in

[9] LINCE methodology : Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad https://www.en.une.org/la-asociacion/sala-de-informacion-une/noticias/primer-estandar-une-de-evaluacion-de-ciberseguridad-de-productos-tic-lince

[10] CCN Website https://www.ccn.cni.es/index.php/en/

2025. This evolution suggests renewed momentum and a growing interest in the methodology, pointing towards a positive trend for certifications in the coming years.

2.2.4.3 Data collection

Modality	The data is extracted from information published in the CCN Lince Catalogue[11]
Date of data Collection	29/03/2025

2.2.5 BSZ - Germany

2.2.5.1 Description

According to BSI (Bundesamt für die Sicherheit in der Informationstechnik – Federal Office for Security in Information Technology) website[12], "the Beschleunigte Sicherheitszertifizierung (BSZ – Accelerated security certification) enables manufacturers to have their security statements regarding a product confirmed by an independent certificate. The associated certification scheme is based on predictable evaluation times and ensures a reasonable level of expenditure for product manufacturers, particularly when it comes to documentation. The evaluation follows a risk-driven approach that establishes a high level of trust in the security statements."

Date of Creation	2021
Scope	Germany
Validity of Certificate	2 years
Mutual recognition	with France through CSPN

2.2.5.2 Statistics covering the last 5 years – Certified products according to BSZ in the last 5 years.

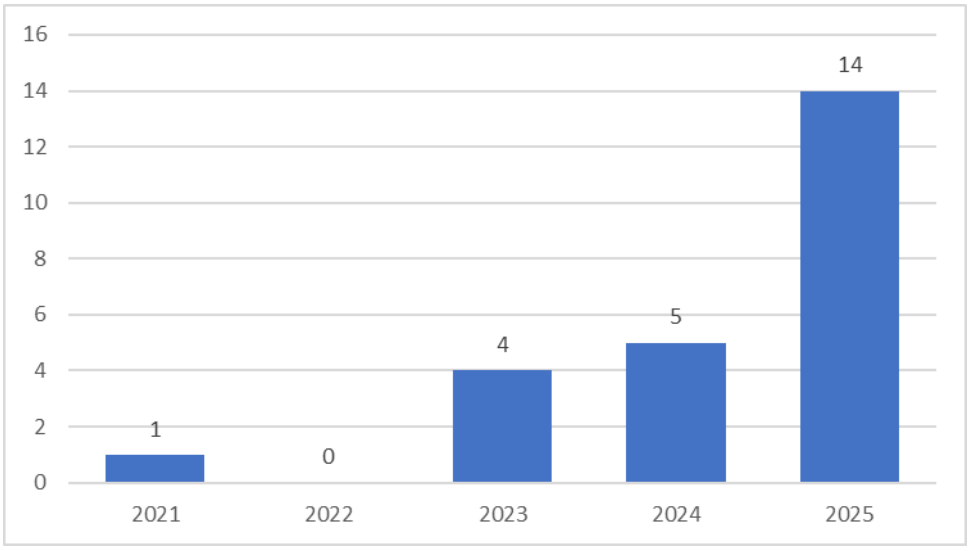


Figure 10: Certified products according to BSZ in the last 5 years.

[11] CCN Lince catalogue : https://oc.ccn.cni.es/en/certified-products/certified-products
[12] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Zertifizierung/beschleunigte-zertifizierung.html

The progression in terms of the number of certified products has shown a slow but steady upward trend except in 2022. Starting with 1 in 2021, dropped again to 0 in 2022, and then increased to 4 in 2023. This growth continued modestly in 2024 and 2025, reaching 7 certificates, suggesting a gradual reactivation of certification activity over the last two years.

2.2.5.3 Data collection

Modality	The data is extracted from the information provided by BSI.
Date of data Collection	07/05/2026

2.3 Cryptographic products

2.3.1 FIPS 140-2 & FIPS 140-3

2.3.1.1 Description

FIPS 140-2 and FIPS 140-3 are standards developed by the National Institute of Standards and Technology (NIST)[13] and Communications Security Establishment Canada (CSEC) to define the requirements to be satisfied by a cryptographic module in order to protect sensitive information. The issuance of FIPS 140-2 certificates progressively declined following the transition to FIPS 140-3. While the CMVP stopped accepting new FIPS 140-2 submissions in 2021, with a final extended deadline in April 2022, certifications continued to be issued for modules already in process within the validation queue. For a better understanding of the scheme operation, certificates issued with both standards are included.

Date of Creation	2001
Scope	International
Validity of Certificate	5 years
Mutual recognition	None

[13] NIST website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Advanced&CertificateStatus=Historical&ValidationYear=0

2.3.1.2 Statistics covering the last 5 years – Certified products according to FIPS.

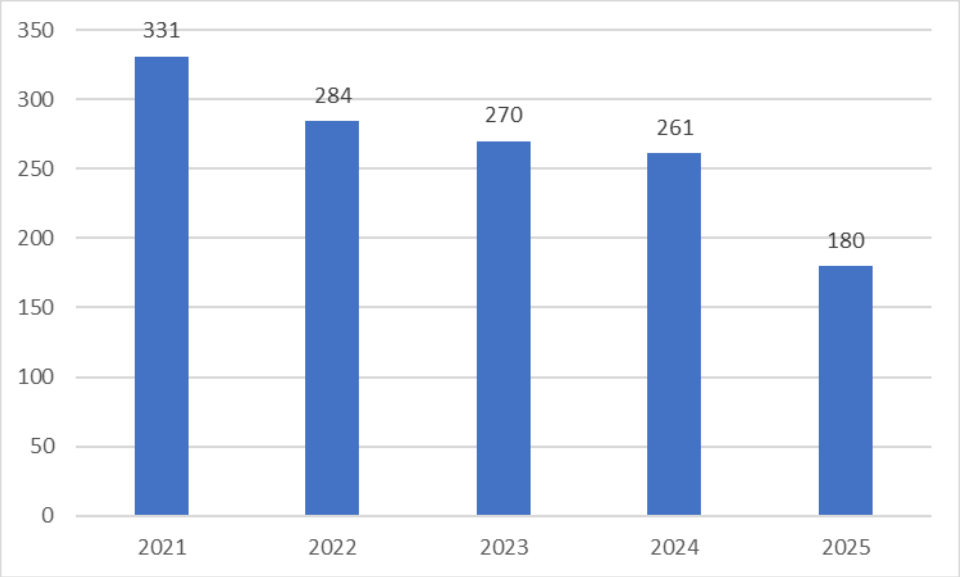


Figure 11: Certified products according to FIPS in the last 5 years.

Many certificates are issued every year against FIPS. However, in the last 5 years, the number of certifications has never fallen below 200 but it could be considered as a stable and consolidated scheme.

2.3.1.3 Data collection

Modality	Data collected manually from the official website of FIPS[14]. In calculating the data, the three types of validation status that FIPS gives to certificates have been taken into account (active, historical and revoked).
Date of data Collection	29/03/2026

2.4 Identity & Digital signature

2.4.1 eIDAS

2.4.1.1 Description

The eIDAS[15] acronym stands for “electronic Identification, Authentication and trust Services” and designates Regulation (EU) No. 910/2014 of the European Parliament and Council of July 23, 2014.

The eIDAS certification sets the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates, and online trust services. Furthermore, it rules electronic transactions and their management.

The eIDAS framework manages the certificate issuance of a qualified electronic signature, being possible to keep confidence in the identity of a person from another recognised certificate.

[14] FIPS’ website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Advanced&CertificateStatus=Historical&ValidationYear=0
[15] Website dedicated to eIDAS https://digital-strategy.ec.europa.eu/en/policies/discover-eidas

Date of Creation	2014
Scope	European Union
Validity of Certificate	5 years
Mutual recognition	Mutual recognition of eIDAS certificates is implicit across the European Union. In addition, there are development with MRA to 3rd countries outside the European Union.

2.4.1.2 Statistics covering the last 5 years – Number of qualified signature/seal creation devices and secure signature creation devices included in the eIDAS list.

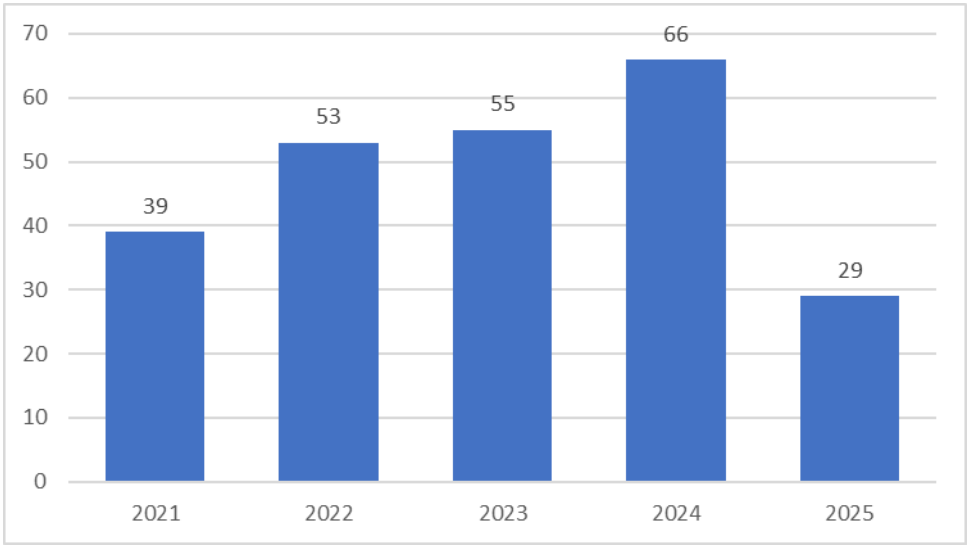


Figure 12: Number of eIDAS qualified signature/seal creation devices and secure signature creation devices in the last 5 years.

The progression in terms of the number of products has shown a positive trend over the past five years. While drastically dropping in 2025, the early high number of certificates in the first years shows a positive uptake of the framework.

2.4.1.3 Data collection

Modality	Data collected manually from the official website of eIDAS[16]. Collection is based on the effective starting date description. The products with no effective starting date are not counted in this report because it is complicated to find the date on which they were listed.
Date of Data Collection	29/04/2026

2.5 Industrial

2.5.1 IECEE - IEC 62443

2.5.1.1 Description

IEC 62443 is a framework developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TR), and technical

[16] https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

specifications (TS). The standard family addresses not only the technology that comprises a control system, but also the work processes, countermeasures, and employees.

Component certification is made against the requirements of IEC 62443-4-2. Certificates are emitted by IECEE.

Date of Creation	2019
Scope	International
Validity of Certificate	The duration of validity varies depending on the issuing National Certification Body.
Mutual Recognition	Within the IECEE scheme

2.5.1.2 Statistics covering the last 5 years – Number of certified products according to IEC 62443-4-2

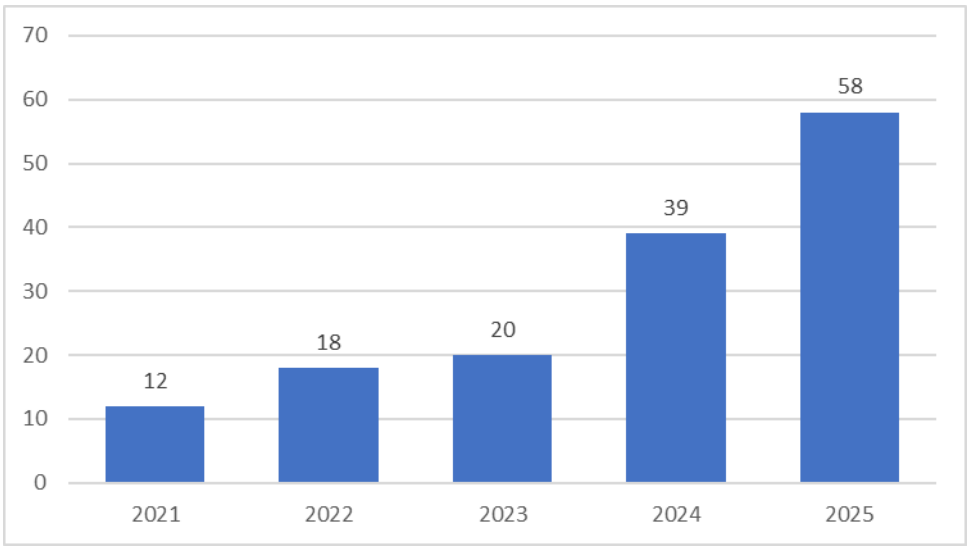


Figure 13: Certified products according to IEC 62443-4-2 in the last 5 years.

The progression in terms of the number of certified products has shown a steady and encouraging upward trend over the past five years. The growth accelerated in last 2 years, reaching 58 certificates in 2025, marking the highest point in the period, and reflecting a strong momentum in certification activity.

2.5.1.3 Data collection

Modality	Data collected manually from the official website of IECEE Certificates[17].
Date of Data Collection	22/05/2025

2.5.2 ISA Secure CSA

2.5.2.1 Description

ISA Secure CSA is a certification scheme developed to assess the cybersecurity of components used in industrial automation and control systems (IACS), in alignment with the IEC 62443-4-2 standard. It

[17] https://certificates.iecee.org/#/search

is part of the broader ISASecure® program, which is managed by the International Society of Automation (ISA) and supports the IEC 62443 series of standards throughout the product lifecycle.

The CSA (Component Security Assurance) certification focuses on embedded devices, host devices, network devices, and software applications. To be certified, components must meet the technical security requirements of IEC 62443-4-2 and demonstrate that they were developed using a secure development lifecycle in accordance with IEC 62443-4-1.

Date of Creation	2019
Scope	International
Validity of Certificate	The duration of these certificates varies depending on the certification body.
Mutual Recognition	None

2.5.2.2 Statistics covering the last 5 years – Number of certified products according to ISA Secure CSA

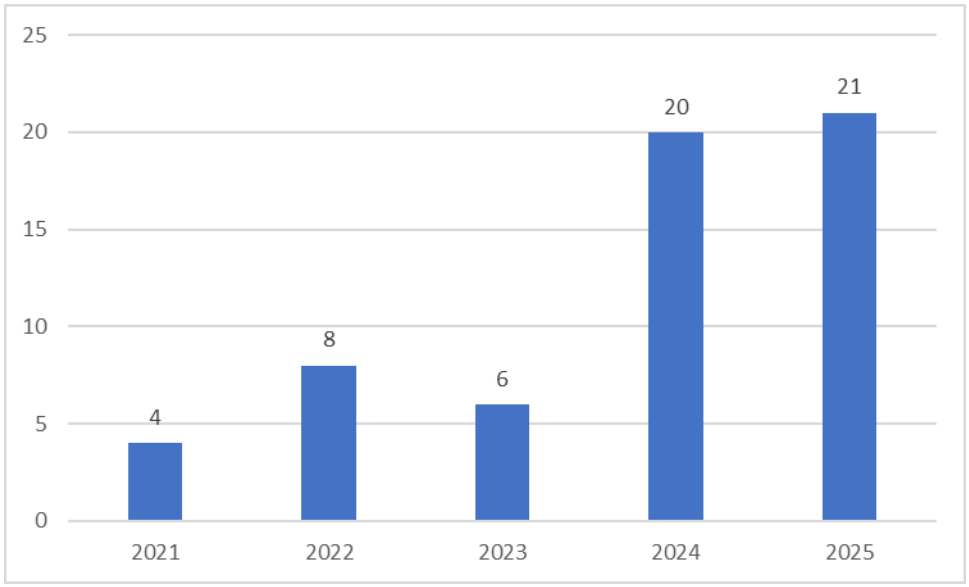


Figure 14: Certified products according to ISA Secure CSA in the last 5 years.

The progression in terms of the number of certified products has shown a fluctuating trend over the past five years. Starting with 4 certificates in 2021, the number rose to 8 in 2022. A slight decline followed in 2023, with 6 certificates, before a significant increase to 20 and 21 in the last two years, showing an acceleration of the adoption of the framework.

2.5.2.3 Data collection

Modality	Data collected manually from the official website of ISA Secure CSA website.
Date of Data Collection	29/03/2026

2.6 Mobile Communications

2.6.1 APP Defense Alliance

2.6.1.1 Description

The App Defense Alliance is focused on improving applications security with common standards and certification programmes recognised by different application platforms. It relies on recognized industry standards, such as OWASP MASVS. Through App Defense Alliance, developers can have their apps validated against a common standard.

As of November 2023 Google, Microsoft, and Meta announced they are formally partnering as the founding steering committee to improve app security through a newly restructured App Defense Alliance, under the Joint Development Foundation, part of the Linux Foundation family[18].

Date of Creation	2022
Scope	International
Validity of Certificate	1 year
Mutual Recognition	None

2.6.1.2 Statistics covering the last 5 years – Certified products according to APP Defense Alliance

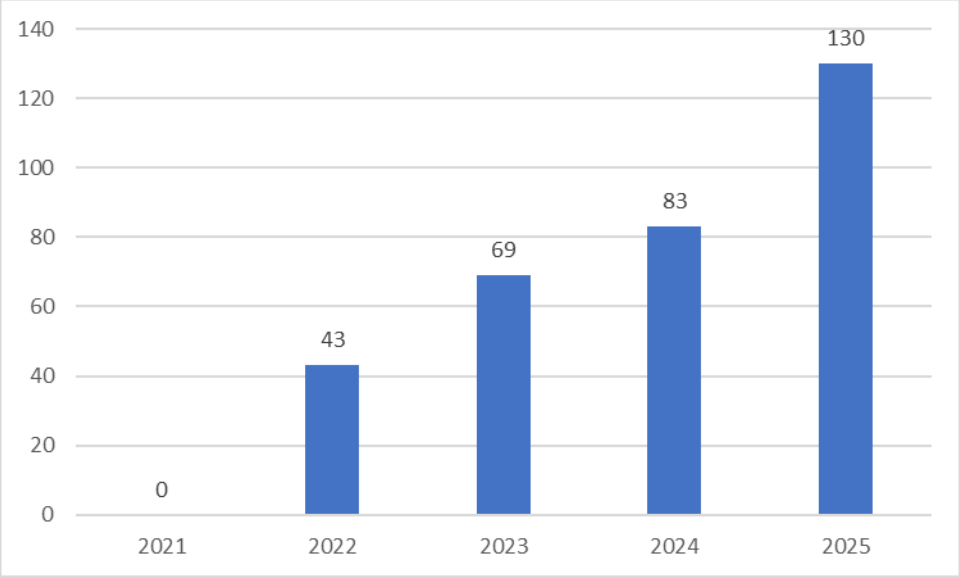


Figure 15: Certified products according to APP Defense Alliance in the last 5 years.

Being 2022 the first year in which this certification was in operation with a total of 43 certificates. The progression in terms of the number of certified products has shown a strong and sustained upward since 2022 followed by further increases to reach 130 certificates in 2025, marking a consistent and accelerating growth in certification activity.

[18] https://www.linuxfoundation.org/press/app-defense-alliance-migrates-under-jdf-with-google-meta-microsoft-as-steering-committee

2.6.1.3 Data collection

Modality	Data collected manually from the official website of APP Defense Alliance[19].
Date of Data Collection	29/03/2026

2.6.2 GSMA eUICC eSA

2.6.2.1 Description

GSMA eSA (eUICC Security Assurance)[20] is based on the Common Criteria approach and the GSMA Protection Profiles (i.e., SGP.05 (for M2M devices) and SGP.25 (for Consumer devices)) but defines a more dynamic set of procedures for the security evaluation of Embedded Universal Integrated Circuit Cards (eUICC).

Date of Creation	2021
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.6.2.2 Statistics covering the last 5 years – Certified products according to eUICC Security Assurance (eSA)

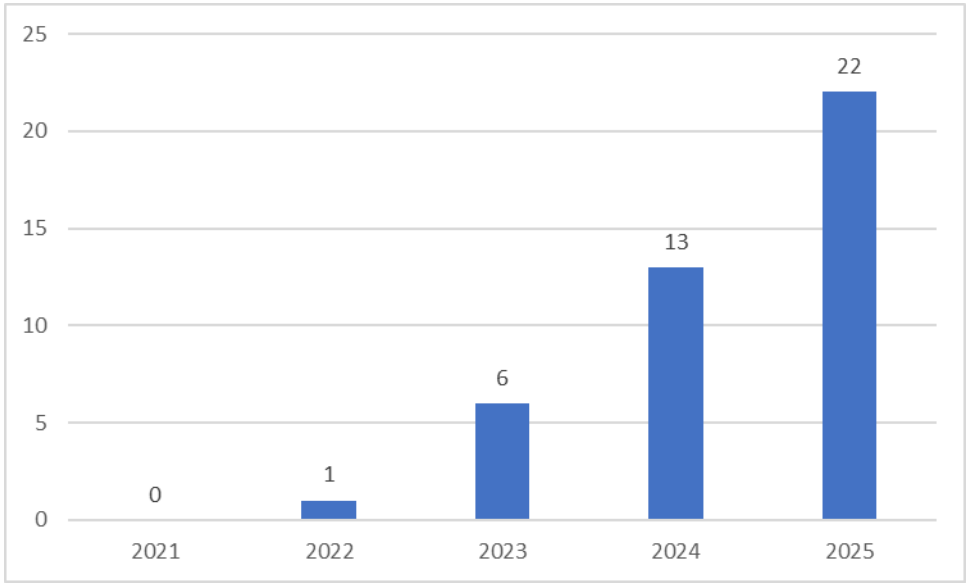


Figure 16: Certified products according to GSMA eUICC (eSA) in the last 5 years.

The progression in the number of records has shown a steadily rising trend over the past five years. Starting with 0 records in 2021, the count increased slightly to 1 in 2022. A notable jump followed in 2023, reaching 6 records, and culminated in a significant peak of 13 records in 2024 — marking the highest point in the period and indicating strong momentum in activity.

[19] https://appdefensealliance.dev/
[20] https://www.gsma.com/esim/wp-content/uploads/2021/02/eSA-Scheme-Step-by-Step-Guide_.pdf

2.6.2.3 Data collection

Modality	Data collected manually from GSMA Network[21] website
Date of Data Collection	23/03/2026

2.6.3 NESAS

2.6.3.1 Description

The GSMA Network Equipment Security Assurance Scheme[22] (NESAS) facilitates improvements in network equipment security levels, across the mobile industry. Providing one universal and global security assurance framework. Ultimately, raising confidence and trust in mobile network equipment.

The purpose of the program is to audit and evaluate network equipment vendors, and their products, against a security baseline. So, they can demonstrate to network operators that they are conforming to the desired standard. The program has been defined by industry experts through GSMA and 3GPP. Therefore, it reflects the security needs of the entire ecosystem, including governments, mobile network operators, and regulators. Currently, audits and evaluations do not lead to GSMA certification but to reports.

Date of Creation	2019
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.6.3.2 Statistics covering the last 5 years – Assessed products according to NESAS.

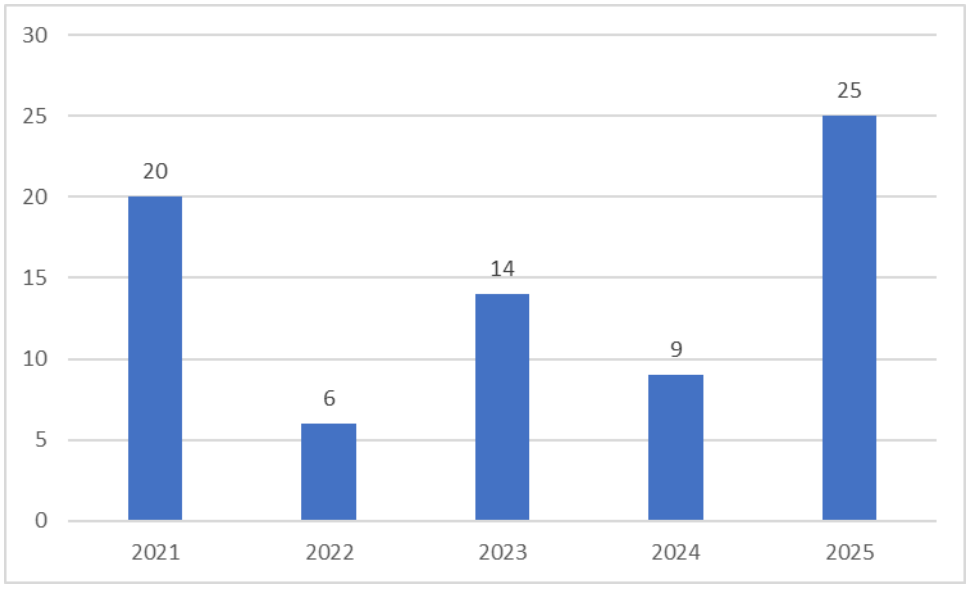


Figure 17: Assessed products according to NESAS in the last 5 years.

The progression in the number of records has shown a fluctuating trend over the past five years. Starting with 15 records in 2020, the number rose to 20 in 2021, marking the highest point in the

[21] https://www.gsmaservices.com/assurance-services/euicc-security-assurance-esa/esa-certified-products/
[22] https://www.gsma.com/services/esim/esa-certified-products/

period. However, a sharp decline followed in 2022, with only 6 records. Activity rebounded in 2023 with 14 records, and 2025 marks a strong increase in terms of assessed products, suggesting a pattern of alternating peaks and troughs in engagement.

2.6.3.3 Data collection

Modality	Data collected manually from the official website of GSMA Network[23]. This program includes two modalities: products evaluated and process audits. The analysis only carries on evaluated products.
Date of Data Collection	23/032026

2.7 Payment

There are several cybersecurity certifications that focus on payment security and are relevant for professionals working in the payment industry. Cybersecurity certifications play a crucial role in the payment industry due to the sensitive nature of payment transactions and the potential risks associated with handling financial data.

In the case of the traditional smart cards market, evaluations of integrated circuits and operation systems for the payment sector have reused the evaluation efforts of the Common Criteria standard being a widespread practice to do both certifications within the same evaluation effort.

Specific Assessment methodologies have been developed to address different specificities of the industry, either from the stakeholders individually but also through the PCI SSC standing for Payment Card Industry Security Standards Council and gathering the major actors from the industry: EMVco, American Express, Discover, JCB international, MasterCard and Visa Inc.

2.7.1 Common.SECC

2.7.1.1 Description

Common.SECC[24] is an international security certification scheme for card payment. Common.SECC covers the Point of Interactions (POIs) deployed at merchants in Germany and the UK, but that scope may be extended. Common.SECC requires that terminals be evaluated for security using Common Criteria.

As mentioned on their website: “Common.SECC ensures recognition by the regulators (EU, ECB, and ECSG) as providing an adequate degree of security, operational reliability, and business continuity according to the ECB’s Oversight Framework for Card Payment Schemes Standards, covering all related SEPA standards of the ECSG’s Volume Book of Requirements. Regulation is aimed at banks.”

Date of Creation	2005
Scope	International
Validity of Certificate	6 years
Mutual Recognition	None

[23] https://www.gsmaservices.com/nesas-conformance-results/
[24] Common SEC Scheme website http://www.common-secc.org/

2.7.1.2 Statistics covering the last 5 years – Certified products according to Common. SECC

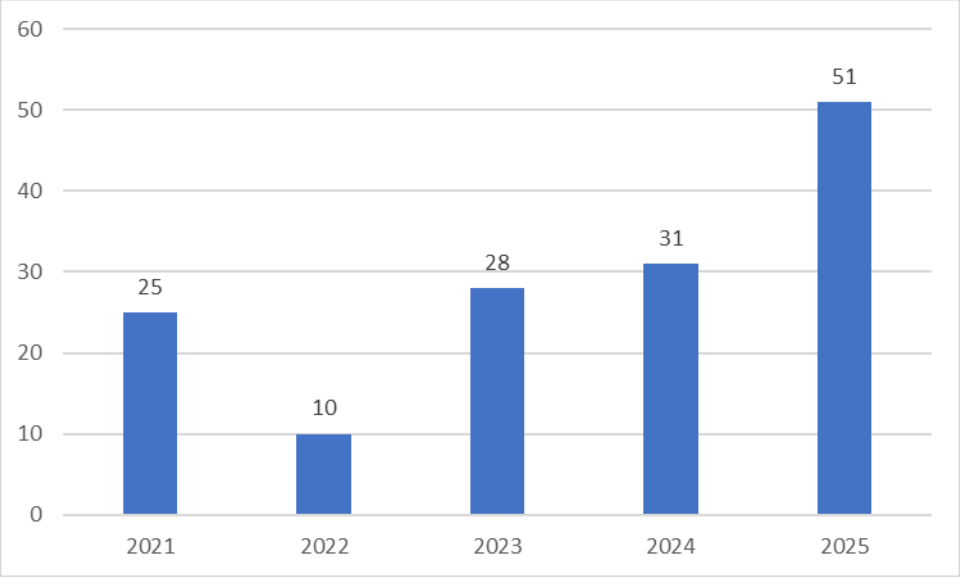


Figure 18: Certified products according to Common.SECC in the last 5 years.

The progression in the number of records starts slowly with ups and down but the higher raise experienced during the past two years shows renewed and growing engagement.

2.7.1.3 Data collection

Modality	Data collected manually from the official website of Common.SECC[25]
Date of Data Collection	23/03/2026

2.7.2 PCI CPoC

2.7.2.1 Description

The PCI CPoC Standard is the second standard released by the PCI Council to address mobile contactless acceptance. The purpose of Contactless Payments on COTS (CPoC™) Security and Test Requirements, is to provide a set of principles and requirements for a mobile payment-contactless acceptance solution on Merchant Mobile Devices Using NFC (Near-Field Communication).

Date of Creation	2019
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

[25] https://www.common-secc.org/devices/

2.7.2.2 Statistics covering the last 5 years – Certified products according to PCI CPoC

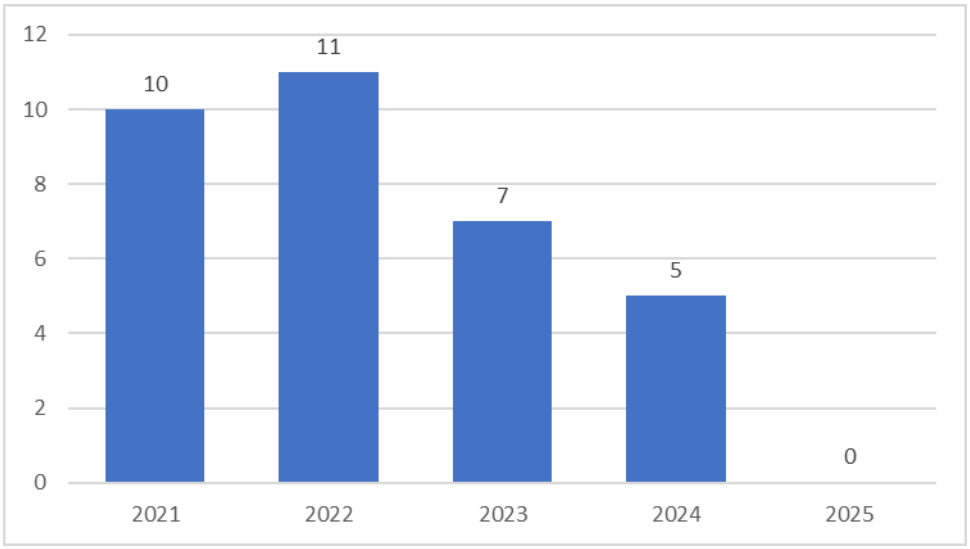


Figure 19: Certified products according to PCI CPoC in the last 5 years.

The number of records has shown a declining trend with some fluctuations over the observed period. Starting from 10 records in 2021, the activity slightly increased to a peak of 11 in 2022. However, this was followed by a marked decrease to 7 records in 2023 and a further decline to 5 in 2024. By 2025, the number of records dropped to zero, indicating a complete cessation of new certifications under the scheme.

This evolution can be strongly associated with the progressive transition within the PCI ecosystem towards the MPoC standard, which consolidates and extends the functionalities previously covered by CPoC and SPoC.

2.7.2.3 Data collection

Modality	Data collected manually from the website of PCI Security Standards[26].
Date of Data Collection	27/03/2026

2.7.3 PCI MPoC

2.7.3.1 Description

PCI Security Standards Council (PCI SSC) published a standard designed to support the evolution of mobile payment acceptance solutions. As described on their blog[27], the " PCI Mobile Payments on COTS (MPoC) builds on the existing PCI Software-based PIN Entry on COTS (SPoC) and PCI Contactless Payments on COTS (CPoC) Standards which individually address security requirements for solutions that enable merchants to accept cardholder PINs or contactless payments, using a smartphone or other commercial off-the-shelf (COTS) mobile device. The PCI MPoC Standard aims to provide increased flexibility not only in how payments are accepted, but in how COTS-based payment acceptance solutions can be developed, deployed, and maintained.

Date of Creation	2022

[26] https://listings.pcisecuritystandards.org/assessors_and_solutions/spoc_solutions
[27] https://blog.pcisecuritystandards.org/just-published-pci-mobile-payments-on-cots?

Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

2.7.3.2 Statistics covering the last 5 years – Certified products according to PCI MPoC

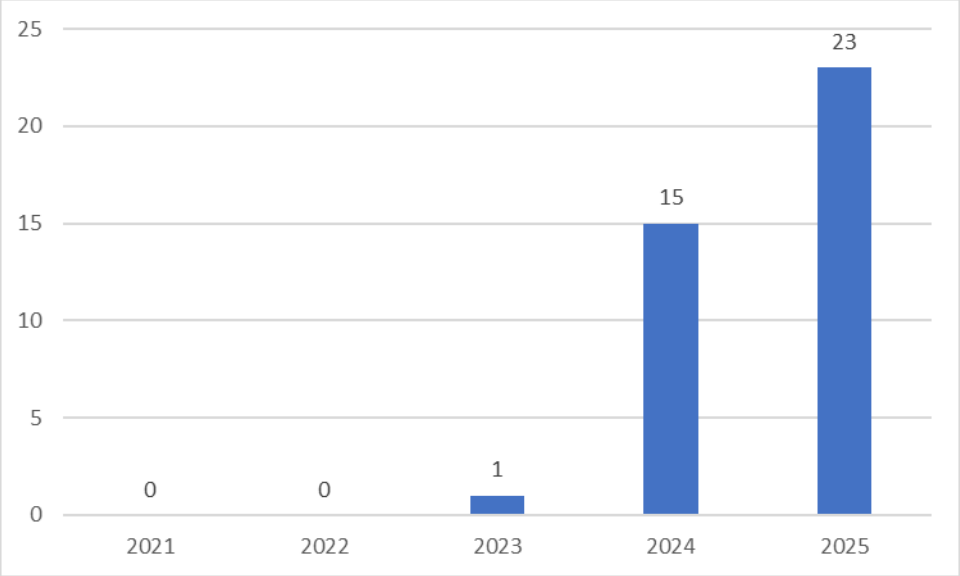


Figure 20: Certified products according to PCI MPoC in the last 5 years.

Due to its recent creation, there are no certified products before 2023. In 2023, the first sign of movement appeared with 1 record. This was followed by a strong surge in the next two years, reaching 23 records in 2025 — the highest point in the five-year period and a strong signal of renewed and accelerating engagement.

2.7.3.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards[28].
Date of Data Collection	29/03/2026

2.7.4 PCI SPoC

2.7.4.1 Description

PCI SPoC is a security standard announced by the Payment Card Industry Security Standards Council (PCI SSC) to regulate the security of electronic mobile transactions on commercial off-the-shelf devices (COTS).

Date of Creation	2018
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

[28] https://listings.pcisecuritystandards.org/assessors_and_solutions/mpoc_solutions

2.7.4.2 Statistics covering the last 5 years - Certified products according to PCI SPoC

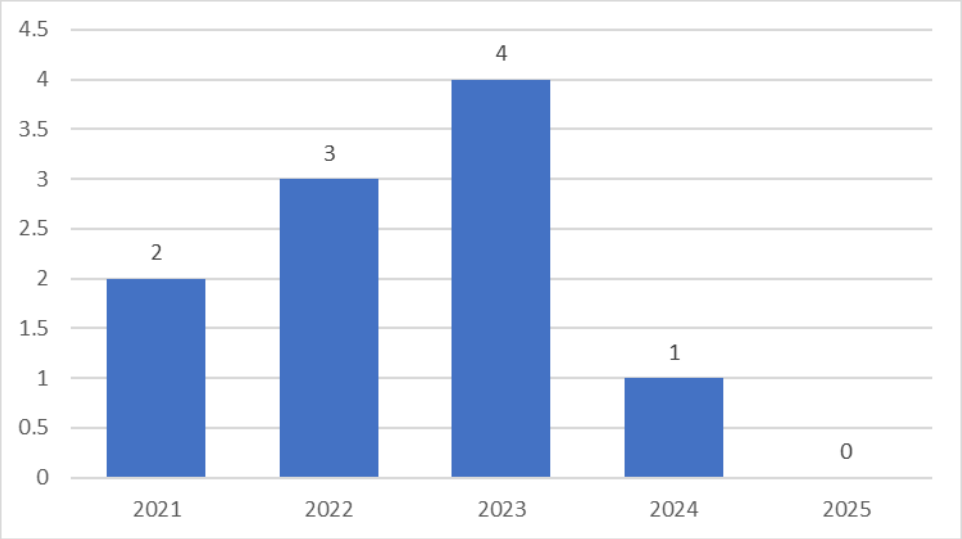


Figure 21: Certified products according to PCI SPoC in the last 5 years.

The number of records has shown an initial growth phase followed by a sharp decline over the observed period. Starting from a low level of 2 records in 2021, the activity increased to 3 in 2022 and reached a peak of 4 in 2023, reflecting a period of gradual adoption. However, this upward trend was reversed in 2024, with a significant drop to 1 record, and no records were observed in 2025.

This evolution suggests that, after a short phase of increasing uptake, the certification activity under the scheme rapidly diminished, influenced by the transition towards more comprehensive frameworks such as MPoC, which consolidate and supersede the functionalities previously addressed by earlier schemes.

2.7.4.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards[29].
Date of Data Collection	22/05/2025

2.8 Internet of Things, IoT

IoT Assessment methodologies are the newest categories schemes addressing ICT products. While remaining voluntary these schemes aim at bringing clarity in the diverse ecosystem of IoT devices. Moreover, they have been a key support for European Regulations such as the RED Directive and the upcoming Cybersecurity Resilience Act.

IoT products time-to-market and cost sensitivities are key drivers for these labels.

[29] https://listings.pcisecuritystandards.org/assessors_and_solutions/spoc_solutions

2.8.1 Labelling – Germany

2.8.1.1 Description

According to the IT-Security Act 2.0 published in 2021, the BSI was tasked with introducing a voluntary IT Security Label. The IT Security Label creates transparency for consumers, revealing basic security features of IT products. This label is based on a self-assessment of compliance to the BSI requirements conducted by the manufacturer followed by a BSI review and a subsequent market surveillance for the validity period.

Date of Creation	2021
Scope	Germany
Validity of Label	Validity of Label: 2-5 years depending on product category
Mutual Recognition	Mutual Agreement with Singapore cybersecurity IoT label thanks to a Memorandum of Understanding (MoU) signed in 2022 and extended in 2024. Mutual Recognition Arrangement with South Korea's "Certification of IoT Cybersecurity" (CIC) signed in 2025.

2.8.1.2 Statistics covering the last 5 years – Products labelled according to the IT security Label – Germany

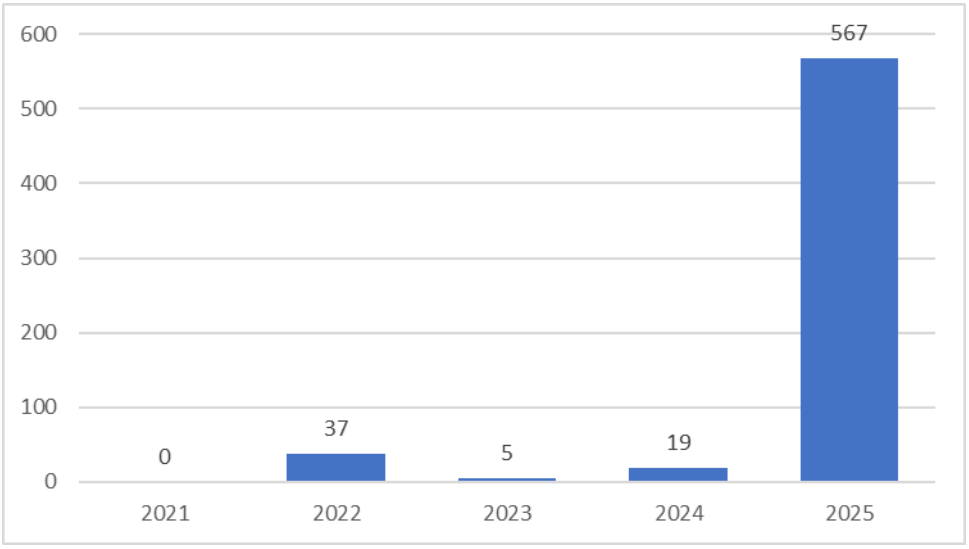


Figure 22: Products labelled according to IT security Label – Germany in the last 5 years.

The progression in terms of the number of labelled products has shown a highly dynamic evolution over the observed period. 2022 was the first full operational year of the label, with 37 labels granted, marking a clear take-off. However, this momentum was not sustained in 2023, where the number dropped sharply to just 5 labels. The activity partially recovered in 2024, reaching 19 labels, indicating a renewed but still moderate level of issuance. Finally, 2025 stands out with a significant surge to 567 labels, suggesting an exceptional expansion phase and a potential structural shift in the trend.

2.8.1.3 Data collection

Modality	Data collected manually from the official BSI website[30].
Date of Data Collection	22/05/2025

2.8.2 IoT Label – Singapore

2.8.2.1 Description

According the official web of The Cyber Security Agency of Singapore (CSA)[31]: "CSA has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace." . Under the scheme, smart devices are rated according to their levels of cybersecurity provisions. This enables consumers to identify products with better cybersecurity provisions and make informed decisions.

The CLS was first introduced to cover Wi-Fi routers and smart home hubs. These products were prioritised because of their wider usage, as well as the impact that a compromise of the products could have on users. It has since been extended to include all categories of consumer IoT devices, such as IP cameras, smart door locks, smart lights, and smart printers.

Date of Creation	2020
Scope	Singapore
Validity of Certificate	3 years
Mutual Recognition	Finland: Consumer IoT products that have met the requirements of the label are recognised as having met the requirements of Level 3 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 3 and above are recognised by Finland to have met their requirements. **Nonetheless, Finland has stopped issuing labels**. Germany: Smart consumer products issued with Germany's IT Security Label will be recognised by CSA to have fulfilled Level 2 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 2 and above are recognised by Germany to have met their requirements

[30] https://www.bsi.bund.de/SiteGlobals/Forms/IT-Sicherheitskennzeichen/EN/IT-Sicherheitskennzeichen_Formular.html
[31] The Cyber Security Agency of Singapore (CSA): https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

2.8.2.2 Statistics covering the last 5 years – Products labelled according to IoT Label – Singapore

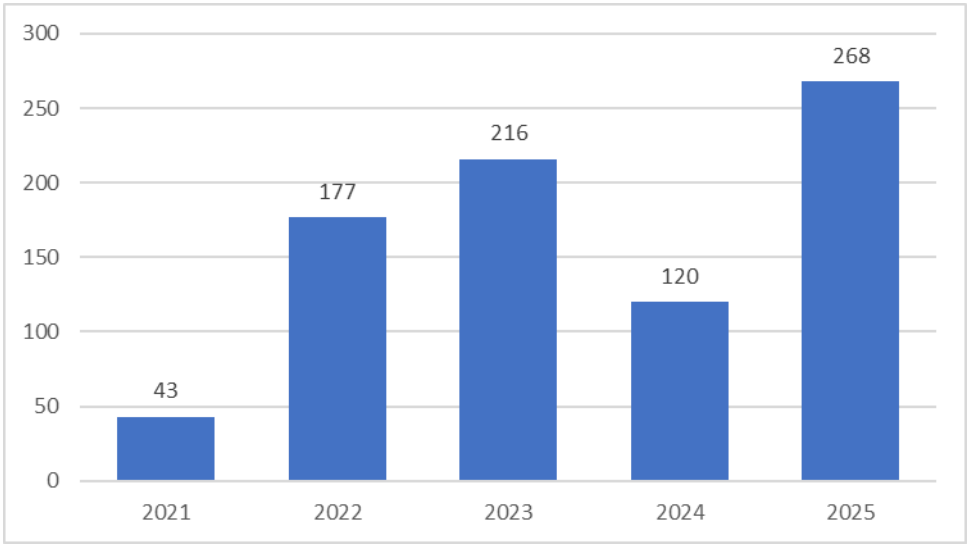


Figure 23: Products labelled according to IoT Label – Singapore in the last 5 years.

The progression in terms of the number of certified products has been consistently upward, especially in the early part of the period. Starting with just 5 certificates in 2020, the number jumped significantly to 43 in 2021 and then surged to a peak of 177 in 2022. This growth continued into 2023, reaching the highest point with 216 certificates. However, in 2024, the trend reversed slightly, with the number dropping to 120, suggesting a potential stabilization or adjustment after two years of rapid expansion.

2.8.2.3 Data collection

Modality	The Certification Body Singapore (CSA Singapore) provided the information. Therefore, the data is extracted from information provided by the Certification Body.
Date of Data Collection	22/05/2025

2.8.3 PSA Certified

2.8.3.1 Description

PSA Certified (PSA for Platform Security Architecture) is a security certification dedicated to IoT hardware such as chips, software, and devices. The scheme provides standardised resources to limit the growing fragmentation of IoT requirements and ensure security of the solution from development phase. The different levels of certification address different stakeholders.

Date of Creation	2019
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.8.3.2 Statistics covering the last 5 years.

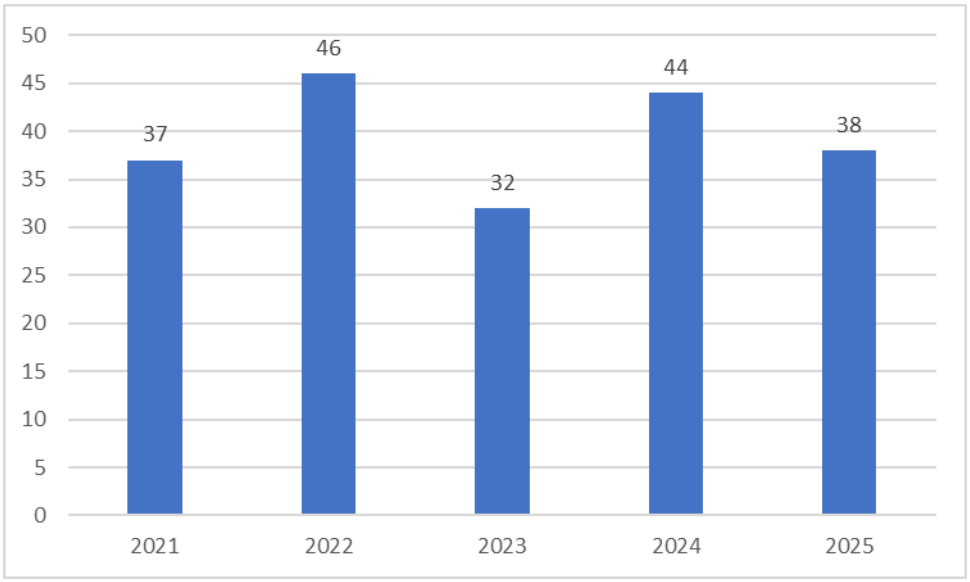


Figure 24: Certified products according to PSA in the last 5 years.

The progression in terms of the number of certified products has shown a positive trend with some fluctuations over the years. The numbers of certified products show a continued interest in certification efforts.

2.8.3.3 Data collection

Modality	Data collected manually from the official website of PSA Certified[32].
Date of Data Collection	29/03/2026

2.8.4 ioXt

2.8.4.1 Description

The ioXt security certification has been developed by the ioXt Alliance founded by leading technology companies willing to build confidence in IoT products. According to the ioXt website[33]: “The program measures a product against each of the eight ioXt principles with clear guidelines to quantify the appropriate level of security required for a specific product.” The scheme is addressing products involved with smart home, lighting controls, smart building, IoT Bluetooth, smart retail, portable medical, smart home, mobile apps, pet trackers, routers, and automotive technology.

Date of Creation	2020
Scope	International
Validity of Certificate	None
Mutual Recognition	None

[32] https://www.psacertified.org/certified-products/
[33] ioXt website: http://www.ioxtalliance.org/

2.8.4.2 Statistics covering the last 5 years – Certified products according to ioXt.

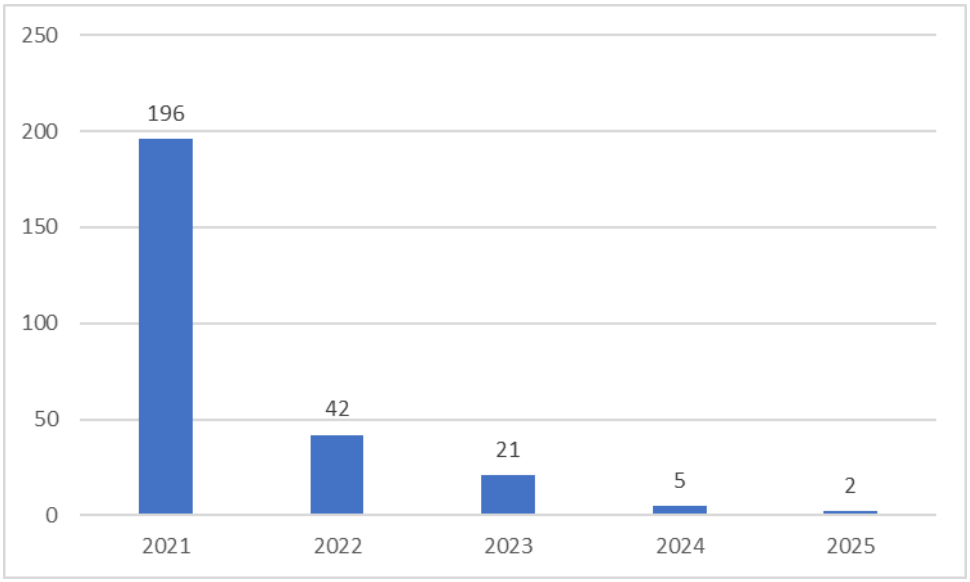


Figure 25: Certified products according to ioXt in the last 5 years.

The progression in terms of the number of certified products has been decreasing significantly over the past years. While the number skyrocketed to 196 in 2021, this momentum did not sustain, as 2022 saw a sharp drop to 42 certificates, followed by a further decline to 21 in 2023. The downward trend continued into 2024 and 2025, to reach 2 certificates issued, suggesting a significant slowdown after the initial peak. The decline in ioXt certifications can be attributed to the increasing shift towards regulatory-driven initiatives, such as the U.S. Cyber Trust Mark where ioXt has been selected as the Lead Administrator for the United States Cyber Trust Mark program.

2.8.4.3 Data collection

Modality	Data collected manually from the official website of ioXt[34].
Date of Data Collection	29/03/2026

2.8.5 Global Platform SESIP

2.8.5.1 Description

Inspired by the experience of the Common Criteria, the SESIP methodology[35] (Security Evaluation Standard for IoT Platforms) provides a common and optimised approach for evaluating the security of IoT components and platforms.

As per November 2023, the SESIP methodology has been adopted as a European Standard by CEN/CENELEC, as EN 17927.

Date of Creation	2018
Scope	International
Validity of Certificate	2 Years.
Mutual Recognition	None

[34] https://compliance.ioxtalliance.org/products
[35] SESIP Methodology: https://globalplatform.org/sesip/

2.8.5.2 Statistics covering the last 5 years – Certified products according to SESIP.

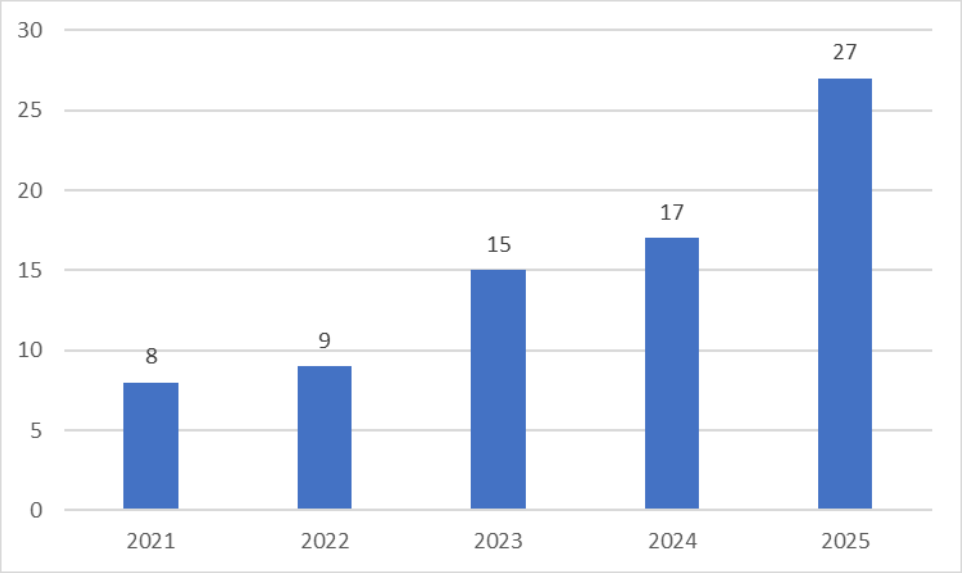


Figure 26: Certified products according to SESIP in the last 5 years.

The progression in terms of the number of certified products has been steadily increasing over the past five years. The number rose gradually from 8 in 2021 to reach 15 certificates in 2023, and further climbed to 27 in 2025, reflecting a consistent and growth in certification activity.

2.8.5.3 Data collection

Modality	Data collected manually from the official website of SESIP Certificates[36].
Date of Data Collection	29/03/2026

[36] https://www.trustcb.com/iot/sesip/sesip-certificates/

SECTION 2

Cloud Services & ISMS

3. Information Security Management Systems and Cloud Services

Cloud services and information security management systems (ISMS) require cybersecurity assessment approaches that differ from traditional product-based evaluations. Due to their service-oriented and continuously evolving nature, assessments focus on the effectiveness of organizational, technical, and operational controls rather than on static product properties.

The assessment landscape is characterised by a limited number of widely adopted frameworks, with ISO/IEC 27001 providing a common baseline for information security management. At the same time, national and sector-specific schemes have emerged to address additional requirements, including data protection and sovereignty considerations.

While mature frameworks show important levels of adoption, more recent or specialised schemes demonstrate slower uptake, reflecting market and regulatory dynamics. Overall, cloud and ISMS assessments illustrate a shift towards risk-based and continuous assurance models, combining governance, processes, and technical controls.

3.1 ISMS assessment methodology: ISO/IEC 27001

3.1.1 Description

While ISO/IEC 27001, the world's best-known standard for ISMS**, is not specifically designed for cloud computing services, it provides relevant best practices that are used as references for many Cloud certification schemes.**

ISO Standard website[37] indicates that:" the ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining, and continually improving an information security management system. (…) Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard."

Date of Creation	2005
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

3.1.2 Statistics covering the last 5 years – Certified ISMS, including cloud computing services according to ISO/IEC 27001

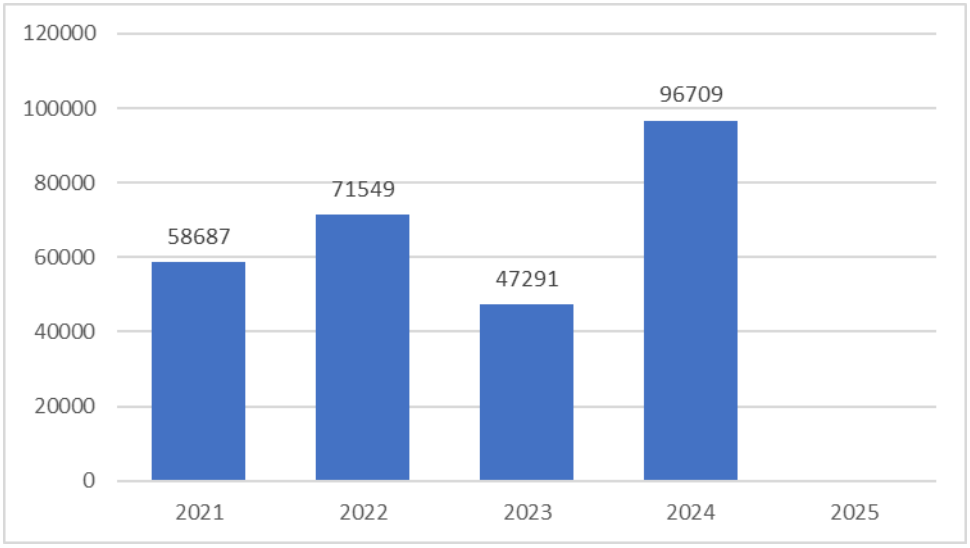


Figure 27: Certified ISMS, including cloud computing services, according to ISO/IEC 27001 in the last 5 years.

The progression in terms of the number of certified products over the past five years shows a dynamic trend. In **2019**, there were **36,362 certificates** issued. The number **increased** to **44,486 in 2020**, then **rose further** to **58,687 in 2021**, and peaked at **71,549 in 2022**. There is a strong decrease in the number of assessments in 2023, however, to be made up for during the year 2024. The data for 2025 has not been published on the date of publication of this report.

[37] ISO Standard website: https://www.iso.org/standard/27001

3.1.3 Data Collection

Modality	Data comes from the survey[38] that ISO leads every year. The latest survey gathers data from 2024
Date of Data Collection	28/04/2026

3.2 ISMS assessment methodology: IT-Grundschutz – Germany

3.2.1 Description

IT-Grundschutz framework aims to provide a standardised methodology for implementing and maintaining an ISMS. The framework helps organisations identify and manage risks to their information assets, thereby improving their overall information security posture. The objective is to guide organisations in establishing, maintaining, and continuously improving their information security mechanisms, while focusing on practical implementation. According to BSI website, “IT-Grundschutz offers various offers to prove the status quo of information security to third parties. In this way, the implementation of the basic protection can be proven by an auditor by means of an attestation. With such an attestation, a basic safeguarding of the business processes can first be conducted. With the implementation of the standard protection, an ISO 27001 certificate based on IT Grundschutz can be achieved.”

Date of Creation	2017
Scope	Germany
Validity of Certificate	3 years with annual surveillance audits
Mutual Recognition	None

3.2.2 Statistics covering the last 5 years – Assessed ISMS against IT-Grundschutz scheme.

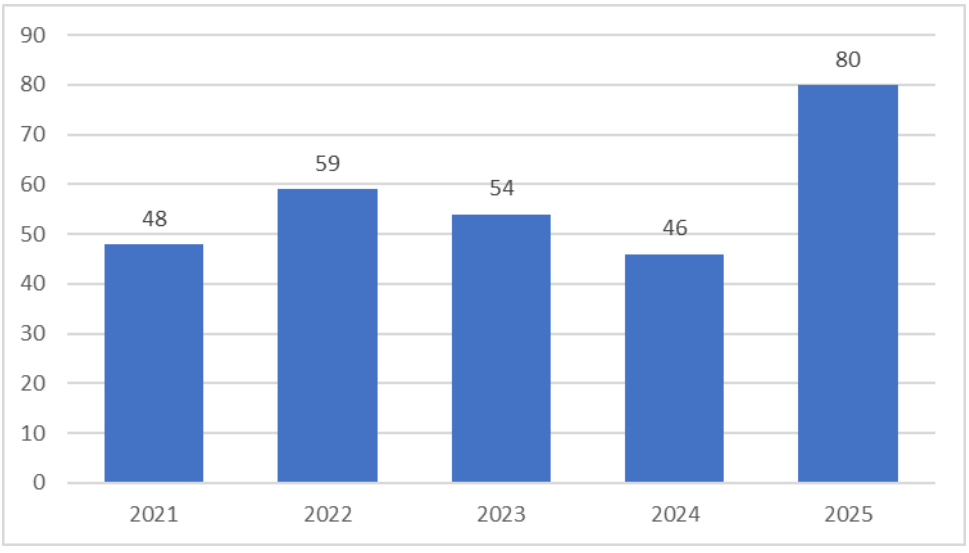


Figure 28: Services adhered according to IT Grundschutz in the last 5 years.

3.2.1 Data Collection

Modality	Data shared by BSI

[38] https://www.iafcertsearch.org/services/iso-survey

Date of Data Collection	18/05/2026

3.3 EU Cloud code of Conduct

3.3.1 Description

The EU Cloud Code of Conduct (EU Cloud CoC) was drafted together with the industry and authorities of the European Union. The first version of the Code was published in April 2017 and the first service certified was in 2018.

As mentioned on the website[39]: "The EU Cloud Code of Conduct consists of requirements for CSPs that wish to adhere to the Code, plus a governance section that is designed to support the effective and transparent implementation, management, and evolution of the Code. (…) The primary objective of the EU Cloud CoC is to harmonize the implementation of GDPR requirements."

Date of Creation	2017
Scope	European Union
Validity of Certificate	1 year
Mutual Recognition	None

3.3.2 Statistics covering the last 5 years – Adhered cloud computing services according to EU Cloud Code of Conduct

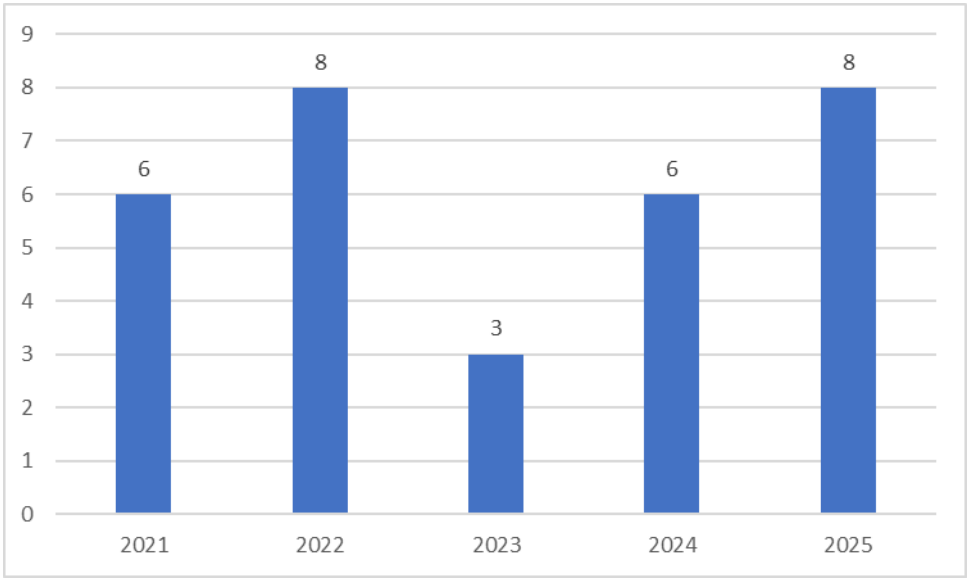


Figure 29: Services adhered according to EU Cloud Code of Conduct in the last 5 years.

The progression in terms of the number of adhered services has shown a modest but fluctuating trend over the past five years. Starting with 6 services in 2021, the number increased to 8 in 2022 However, 2023 saw a notable drop to 3 services, before recovering slightly to 6 in 2024 and 8 in 2025, suggesting a return to earlier levels after a temporary decline.

[39] EU Cloud of Conduct website: https://eucoc.cloud/en/home

3.3.3 Data Collection

Modality	Data collected manually from the official website of EU Cloud CoC.
Date of Data Collection	24/03/2026

3.4 C5 – Germany

3.4.1 Description

The C5 (Cloud Computing Compliance Criteria Catalogue[40]) published by the German Federal Office for Information (BSI) Security specifies minimum requirements for secure cloud computing. It is primarily intended for professional cloud providers, their auditors, and customers.

European and global cloud providers, as well as a wide range of cloud services. Medium-sized and small providers now use the catalogue too. C5 gives cloud customers an important guide to selecting a provider. It is the foundation for putting a customer-specific system of risk management in place. C5 was completely revised in 2019 to consider the latest developments in detail and increase quality still further.

Date of Creation	2016
Scope	Germany
Validity of Certificate	1 year
Mutual Recognition	None in force. “ESCloud” was signed with the French SecNumCloud but never applied

3.4.2 Statistics covering the last 5 years – Cloud Services Providers with a C5 attestation.

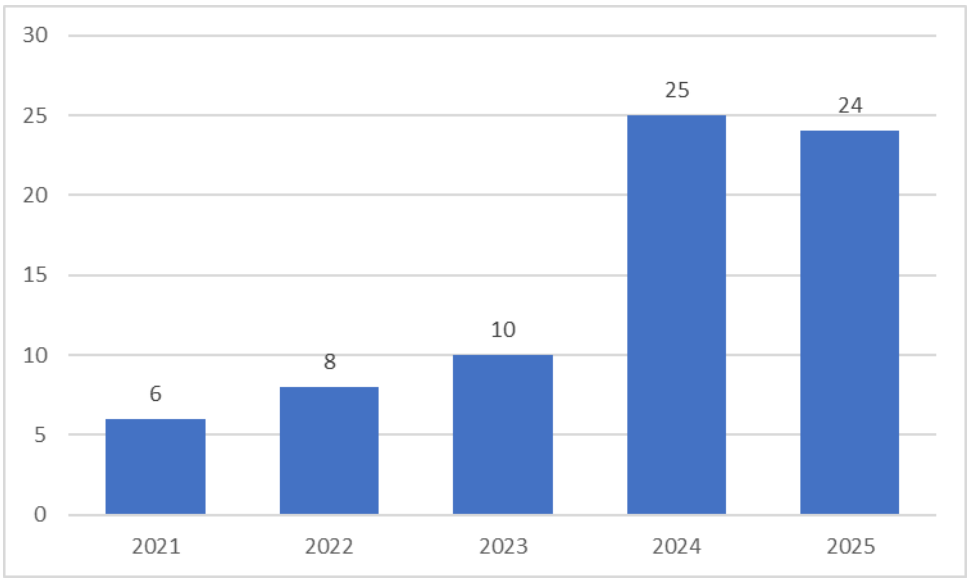


Figure 30: New CSP with a C5 attestation in the last 5 years.

[40] C5 (Cloud Computing Compliance Criteria Catalogue https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

The progression in terms of the number of new CSP attestations has shown a steady upward trend with a notable acceleration and stabilisation in the final years. Starting with 6 new attestations in 2021, 8 in 2022, and 10 in 2023. However, 2024 saw a significant jump to 25 new attestations, indicating a sharp increase in certification activity confirmed in 2025 with 24 delivered attestations.

3.4.3 Data Collection

Modality	Data collected directly from C5 Attestations.
Date of Data Collection	12/04/2026

3.5 SecNumCloud – France

3.5.1 Description

SecNumCloud is the qualification proposed by ANSSI[41] to distinguish cloud operators who respect good security practices. The objectives of SecNumcloud are to promote, enrich and improve the offer of cloud providers for public and private entities wishing to outsource the hosting of their data, applications, or information systems to trusted providers. SecNumCloud certification is built upon international standards such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 which outline security requirements.

Date of Creation	2016
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None in force. “ESCloud” was signed with the German C5 but never applied.

3.5.2 Statistics covering the last 5 years – Qualified cloud services according to SecNumCloud.

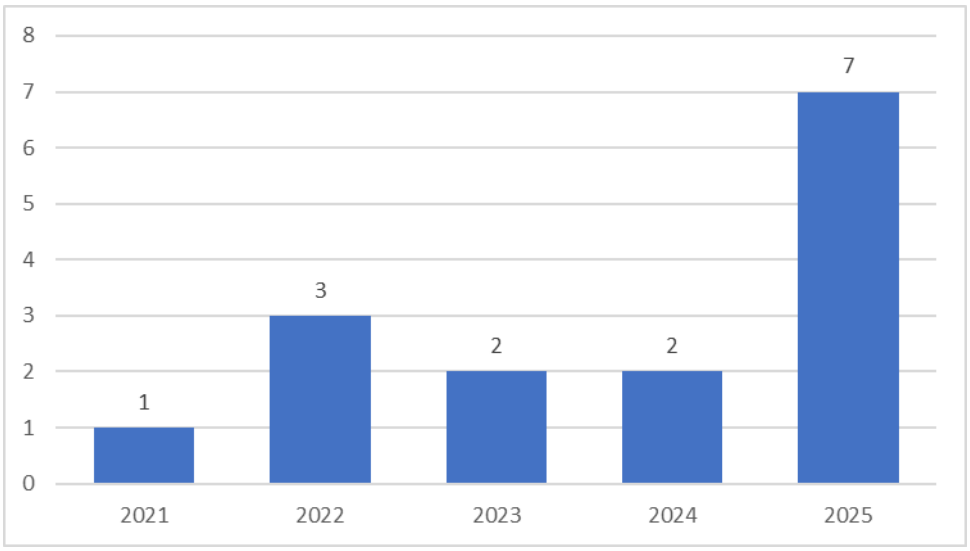


Figure 31: Cloud Computing services qualified according to SecNumCloud in the last 5 years.

[41] ANSSI website: https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/

The progression in terms of the number of certified products has been steady for four years before increasing significantly to seven providers in 2025. Additionally, it is important to note that the 7 qualified providers represent 15 solutions in total.

3.5.3 Data Collection

Modality	Data collected directly from ANSSI
Date of Data Collection	28/04/2026

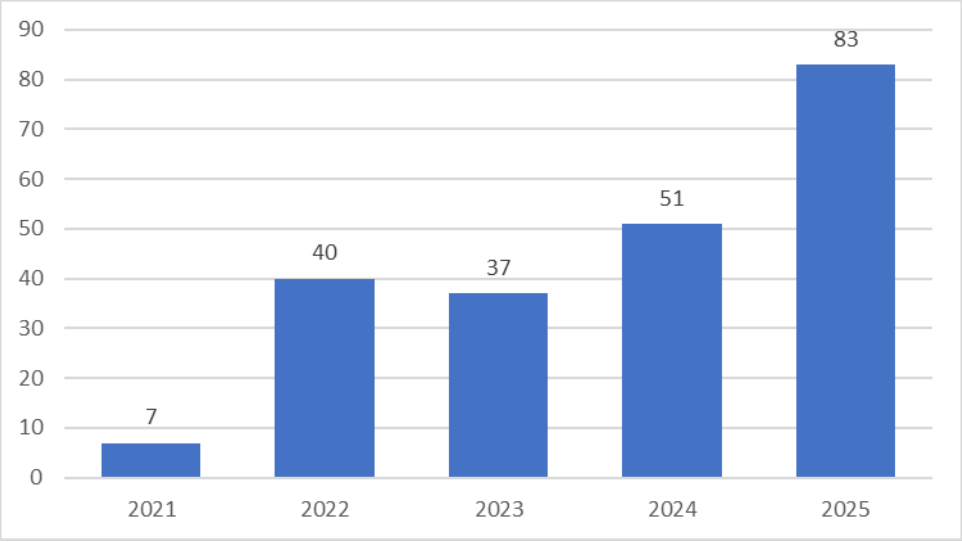
3.6 CPSTIC Cloud Evaluations - Spain

3.6.1 Description

CPSTIC[42], short for Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones, is the official Spanish catalogue for cybersecurity-assured ICT products, managed by the Centro Criptológico Nacional (CCN). It includes cloud services that must pass a Cloud STIC (Security Technologies and Information Certification) evaluation. These evaluations are designed to ensure that cloud-based solutions meet stringent national security requirements and are suitable for use in public administration and critical infrastructure. CPSTIC evaluations are structured around a taxonomy of product families and follow a fixed-time approach. The fixed-time approach is optimized for accessibility and cost-efficiency, especially for SMEs, while the comprehensive method aligns with international standards and is suitable for high-assurance use cases. Evaluations cover both technical vulnerability analysis and compliance with the Spanish National Security Framework (ENS).

Date of Creation	2021
Scope	National (Spanish)
Validity of Certificate	2 years – ENS is a prerequisite to maintain the certification valid
Mutual Recognition	None

3.6.2 Statistics covering the last 5 years – Cloud Services listed in the CPSTIC Catalogue



[42] CPSTIC Catalogue : https://cpstic.ccn.cni.es/en/catalogue?search=&f_cualificado=5&order=i.created&dir=desc&f_familia=&f_nivel_ens=&f_nivel_clasificacion=&f_tipo=&cm=0#tlb

Figure 32: Solutions listed in the CPSTIC catalogue in the last 5 years.

The progression in terms of the number of CPSTIC cloud evaluations has shown a strong upward trend over the past five years. Starting with 7 in 2021, followed by a sharp increase to 40 in 2022. Although 2023 saw a slight decline to 37, the growth resumed in 2024, reaching 51 evaluations. This upward trajectory continued significantly in 2025, with 83 evaluations, marking a new peak and highlighting a sustained and accelerating interest in cloud evaluations under the CPSTIC framework.

3.6.3 Data Collection

Modality	Data directly obtained from CCN
Date of Data Collection	13/05/2026

3.7 FedRAMP – United States

3.7.1 Description

As mentioned on their website[43]: "The Federal Risk and Authorisation Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the United States' federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information. (…) It promotes the adoption of secure cloud services by providing a standardised approach to security and risk assessment for cloud technologies and federal agencies."

Date of Creation	2011
Scope	United States
Validity of Certificate	1 year
Mutual Recognition	None

3.7.2 Statistics covering the last 5 years – Authorised services according to FedRAMP.

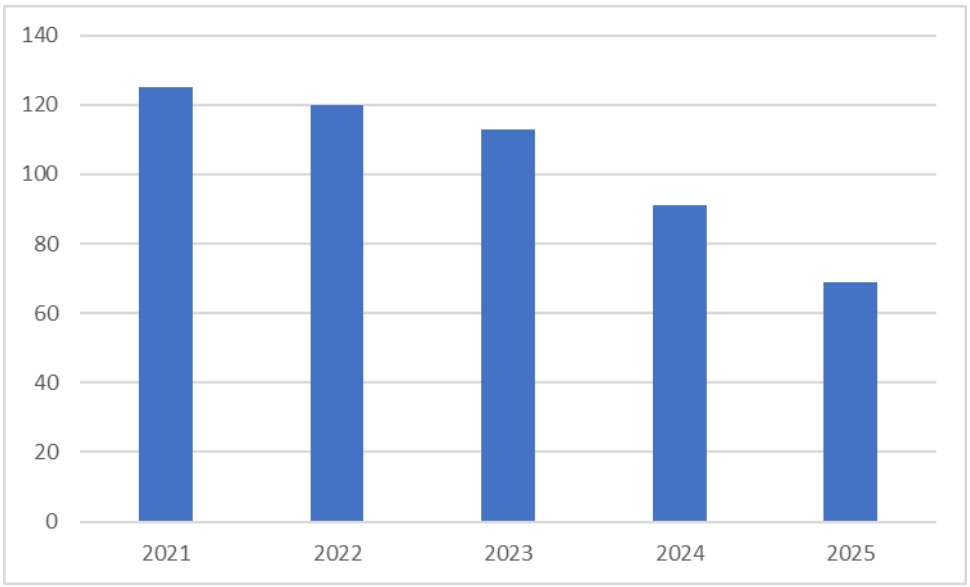


Figure 33: Services authorised according to FedRAMP in the last 5 years.

[43] FedRamp: https://www.fedramp.gov/

The progression in terms of the number of certified solutions has shown a steady downward trend over the past five years. Starting from an important level of approximately 125 certified solutions in 2021, the number gradually declined to around 120 in 2022 and continued decreasing to about 112 in 2023. This downward trajectory persisted in 2024, with a more pronounced drop to 90, followed by a further reduction to 70 in 2025. This evolution is reasonable given that only new certified solutions are counted and the scheme is mature.

3.7.3 Data Collection

Modality	Data collected manually from the official website of FedRAMP[44]
Date of Data Collection	04/05/2026

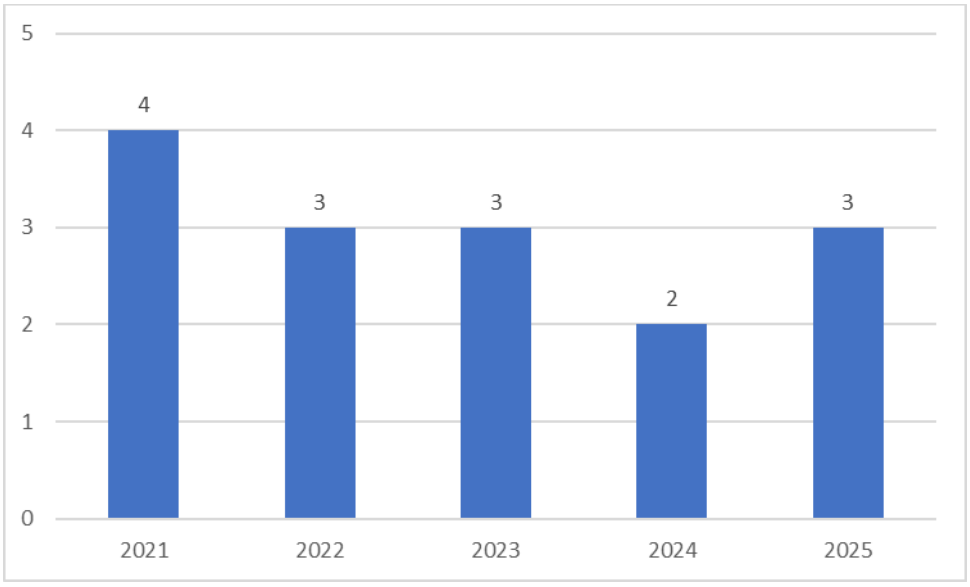
3.8 CSA STAR

3.8.1 Description

CSA STAR stands for Cloud Security Alliance, Security Trust and Assurance Registry. It is a certification led by the Cloud Security Alliance[45] Association gathering members from enterprises and Cloud Services Providers (CSPs) worldwide. It includes two levels of assurance, the first one being a self-assessment. CSA STAR covers both operational security and privacy legal compliance. The certification is designed to work as a complement to the ISO/IEC 27001 framework and aims at demonstrating a higher level of security.

Date of Creation	2013
Scope	International
Validity of Certificate	3 years – ISO/IEC 27001 is a prerequisite to maintain the certification valid
Mutual Recognition	None

3.8.2 Statistics covering the last 5 years – Solutions listed according to CSA STAR



[4444] https://marketplace.fedramp.gov/#!/products?status=FedRAMP%20Ready&sort=productName
[45] http://www.cloudsecurityalliance.org/

Figure 34: Solutions listed according to CSA STAR in the last 5 years.

The numbers in this figure represent the new certifications issued each year. It should be noted that only newly issued records are considered. The progression in terms of the number of certified solutions shows a moderately fluctuating trend over the past five years. Starting with 4 certifications in 2021, the number declined to 3 in 2022 and remained stable at 3 in 2023. A further decrease to 2 certifications was observed in 2024, followed by a partial recovery to 3 in 2025. Overall, this evolution suggests a low but stable level of certification activity, with minor variations but no clear long-term growth or decline.

3.8.3 Data Collection

Modality	Data collected manually from the official website of CSA.
Date of Data Collection	04/05/2026

SECTION 3

Managed Security Services

4. Managed Security Services

Managed Security Services is the new category of ICT solutions to be addressed within the EU Cybersecurity Certification framework following the revision of the Cybersecurity Act. According to the legislation: "'managed security service' means a service provided to a third party consisting of conducting, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits, and consulting, including expert advice, related to technical support;"[46].

Following the request of the European Commission, ENISA has launched the Ad Hoc Working Group to build a draft candidate scheme to address MSS and more specifically the activity of Incident Response. A preliminary internal work led by the European Agency for Cybersecurity aimed at studying existing schemes addressing the different MSS activities. Conclusions indicated that the market of cybersecurity assessment on MSS currently offers two types of approaches:

- **Horizontal Schemes**: requirements addressing the service in the background. No matter what security services are being provided, the provider must apply the requirements. To be noted that existing national horizontal schemes addressing MSS aims at providing compliance to the national transpositions of NIS2 Directive.
- **Vertical Schemes**: requirements specifically addressing the Managed security services delivered by the provider. They would differ according to the type of activities.

The following section presents the schemes accordingly.

[46] Regulation (Eu) 2025/37 of the European Parliament and of the Council of 19 December 2024. Article 2(14a)

4.1 Horizontal schemes

Spain is the precursor regarding the development and implementation of a horizontal scheme addressing IT Services Providers and Managed Security Services providers. In 2023, Belgium developed Cyber Fundamental, a scheme dedicated to NIS2 Entities and MSSP but there are no certified providers so far[47].

4.1.1 ENS – Spain

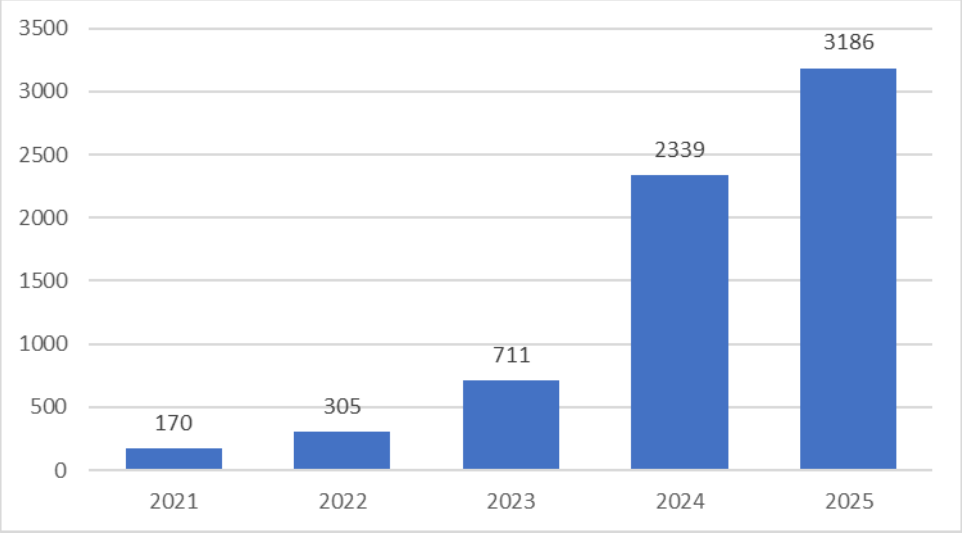
4.1.1.1 Description

The **National Security Framework**[48] (ENS by its acronym in Spanish), is applicable to the entire Public Sector, as well as its suppliers. It offers a common framework of basic principles, requirements, and security measures for the adequate protection of the information processed and the services provided. The framework applies to any company and entity providing ICT services to the public sector. The last update of the scheme is from 2022 with Royal Decree 311/2022[49].

Additionally, specific compliance profiles (PCE), can be created and modified according to the evolving needs and requirements. Therefore, CCN-STIC 896 – Specific Compliance Profile for Managed Security Services" defines, evaluates, and certifies the operational requirements and the minimum technical, organisational and personnel competencies necessary for the provision of managed security services.

Date of Creation	2010
Scope	Spain
Validity of Certificate	2 years
Mutual Recognition	None

4.1.1.2 Statistics covering the last 5 years – Certified Companies, including CSPs, according to ENS.



[47] https://cyfun.eu/en
[48] ENS Website http://www.ens.ccn.cni.es/
[49] https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

Figure 35: Certified Companies, including CSPs, according to ENS in the last 5 years.

The progression in terms of the number of certificates has demonstrated a strong and accelerating upward trend over the past five years. Starting with 170 in 2021 and continued rising to 305 in 2022. This growth surged dramatically in 2024, with 2,339 certificates then 3186 in 2025, marking the highest point in the period and reflecting a significant expansion in certification activity.

4.1.1.3 Data Collection

Modality	Data provided by CCN
Date of Data Collection	29/03/2026

4.2 Vertical Scheme - Audit and Pentesting

4.2.1 "IS penetration tests" – Germany.

4.2.1.1 Description

The certification of IT security service providers by the Federal Office for Information Security (BSI)[50] was originally established to assist the German government in safeguarding the national security landscape, particularly within government sectors.

BSI's certification process is structured to ensure that both organisations and individual professionals adhere to rigorous standards of competence and reliability. For an organisation to obtain certification, it must employ at least two certified professionals in the specific type of services it offers.

As mentioned on the BSI website: "An IS penetration test is a proven and appropriate technique for identifying the susceptibility to attack for an IT network, an individual IT system or a (web) application.

Certified IT security service providers within the scope "IS penetration tests" complete the following tasks and offer the following services: Completion of security analyses and vulnerability detection work, Performance of penetration tests.

Date of Creation	2013
Scope	Germany
Validity of Certificate	3 years
Mutual Recognition	None

[50] BSI - IS audit based on IT-Grundschutz/IS penetration tests

4.2.1.2 Statistics covering the last 5 years – Certified IT security service providers in the scope IS penetration tests.

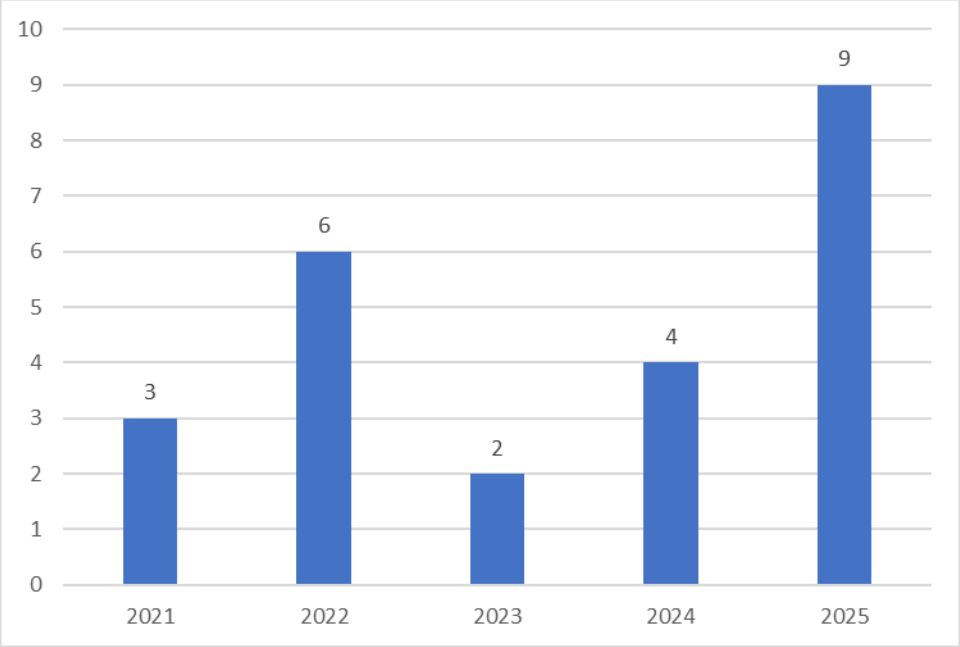


Figure 36: Certified IT security service providers in the scope IS penetration tests in the last 5 years.

This figure shows the Certified IT security service providers in the scope IS penetration tests. The progression in terms of the number of certified solutions has shown a limited but steady trend over the past five years. Starting with 3 certificates in 2021, the number gradually rose to 6 in 2021, but then 2 in 2023, and 4 in 2024. 2025 shows a raise to reach 9 certified IT service providers.

4.2.1.3 Data Collection

Modality	Data provided by BSI
Date of Data Collection	12/01/2026

4.2.2 PASSI – France

4.2.2.1 Description

Under the banner of the Security Visas[51], the qualification scheme PASSI (Information systems security audit providers) ensure that audits led by qualified providers are impartial and objectively led. Information systems security audit providers are qualified for one or more of the following activities: organisational and physical audit, architectural audit, configuration audit, source code audit, penetration testing.

Date of Creation	2015
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None

[51] https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/

4.2.2.2 Statistics covering the last 5 years – Qualified PASSI Services

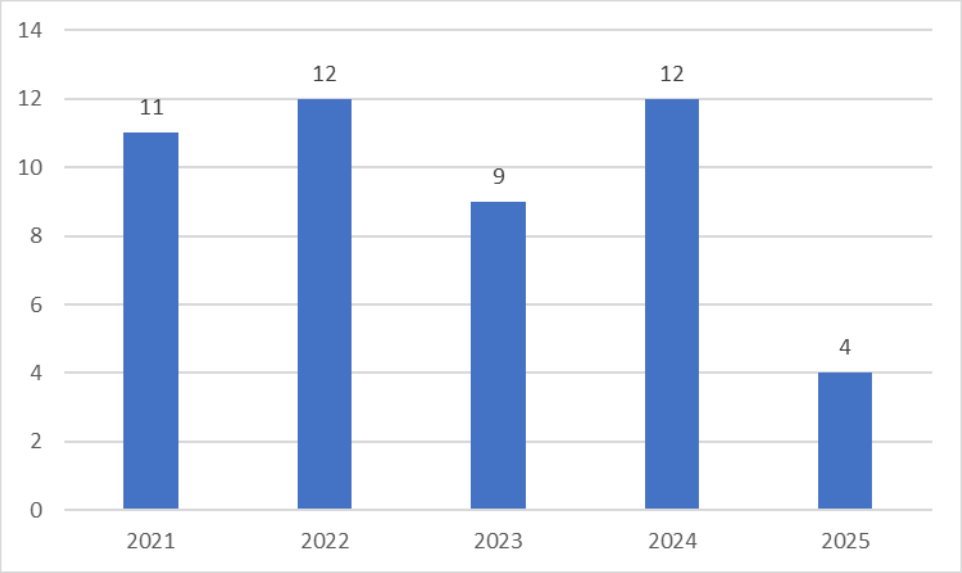


Figure 37: Qualified PASSI Services, according to ANSSI in the last 5 years.

The progression in terms of the number of services has remained stable with minor fluctuations over the past five years. Starting with 11 services in 2020, the number stayed the same in 2021, then increased slightly to 12 in 2022. However, 2023 saw a decline to 9 services, before recovering to 12 in 2024, suggesting a return to previous levels after a temporary dip.

4.2.2.3 Data Collection

Modality	Data provided by ANSSI
Date of Data Collection	03/12/2025

4.2.3 Pentest – The Netherlands

4.2.3.1 Description

As mentioned on CCV website[52]: “To ensure that providers of penetration tests deliver high-quality work, the CCV certification for Pen tests has been developed. As with door locks and car alarm systems, it is important that the digital security of your business is in order. Independent supervision of the quality of pen test services is a major step in the fight against cybercriminals.”

Date of Creation	2015
Scope	The Netherlands
Validity of Certificate	1 year
Mutual Recognition	None

4.2.4 Statistics covering the last 5 years – CCV Pentest qualification.

CCV does not display the yearly new certified providers. However, there are in total 45 certified pen test providers according to CCV.

[52] Pen test (English) - Het CCV

4.2.4.1 Data Collection

Modality	Data collected on CCV website[53]
Date of Data Collection	04/05/2026

4.3 Vertical Scheme - Cybersecurity Consulting services

4.3.1 Scope "IS-Revision and IS-Beratung" – Germany

4.3.1.1 Description

The certification of IT security service providers by the Federal Office for Information Security (BSI)[54] was originally established to assist the German government in safeguarding the national security landscape, particularly within government sectors.

The BSI's certification process is structured to ensure that both organisations and individual professionals adhere to rigorous standards of competence and reliability. For an organisation to obtain certification, it must employ at least two certified professionals in the specific type of services it offers.

Date of Creation	2010
Scope	Germany
Validity of Certificate	3 years
Mutual Recognition	None

4.3.1.2 Statistics covering the last 5 years – List of certified IT security service providers in the scope of IS-Revision and IS-Beratung

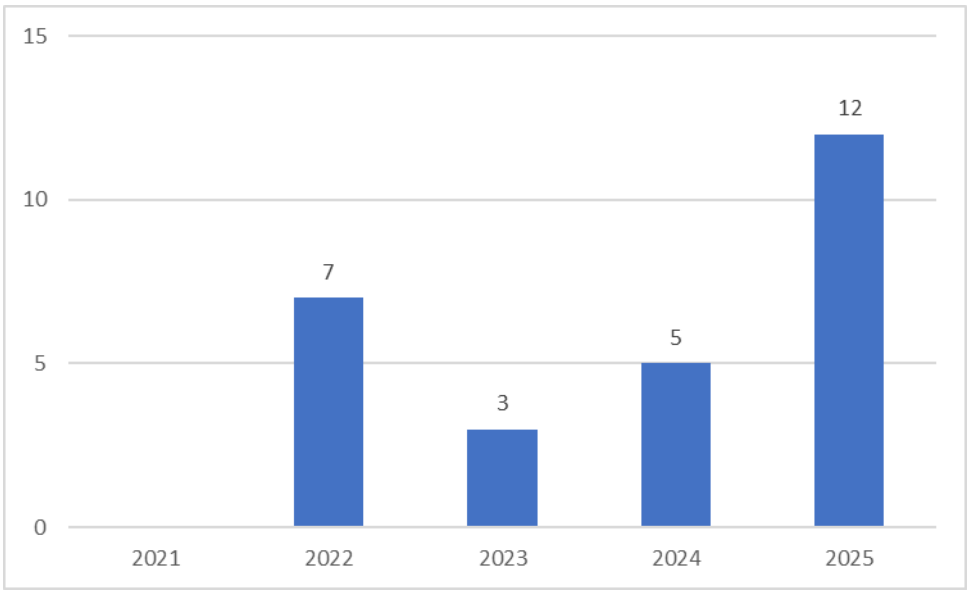


Figure 38 List of certified IT security service providers in the scope of IS-Revision and IS-Beratung

[53] Pentesten – Het CCV: https://hetccv.nl/certificaat-schema/pentesten/
[54] BSI - IS audit based on IT-Grundschutz/IS penetration tests

This figure shows certified IT security service providers in the scope of IS audit based on IT-Grundschutz. The progression in terms of the number of certified has been fluctuating during the past five years with a slight increase in the past year with 12 certified providers in 2025.

4.3.1.3 Data Collection

Modality	Data collected manually on the website.
Date of Data Collection	06/05/2026

4.3.2 PACS- France

4.3.2.1 Description

Under the banner of the Security Visas[55], the qualification scheme, PACS (Information systems security assistance and consulting) providers assist a client in securing its information system and maintaining it in a secure condition. Information systems security assistance and consulting providers are qualified for the following activities: Information systems security certification consulting, information systems security, risk management consulting, information systems architecture security consulting, and cyber crisis management consulting.

Date of Creation	2023
Scope	France
Validity of Certificate	2 years
Mutual Recognition	None

4.3.2.2 Statistics covering the last 5 years – qualified PACS Services

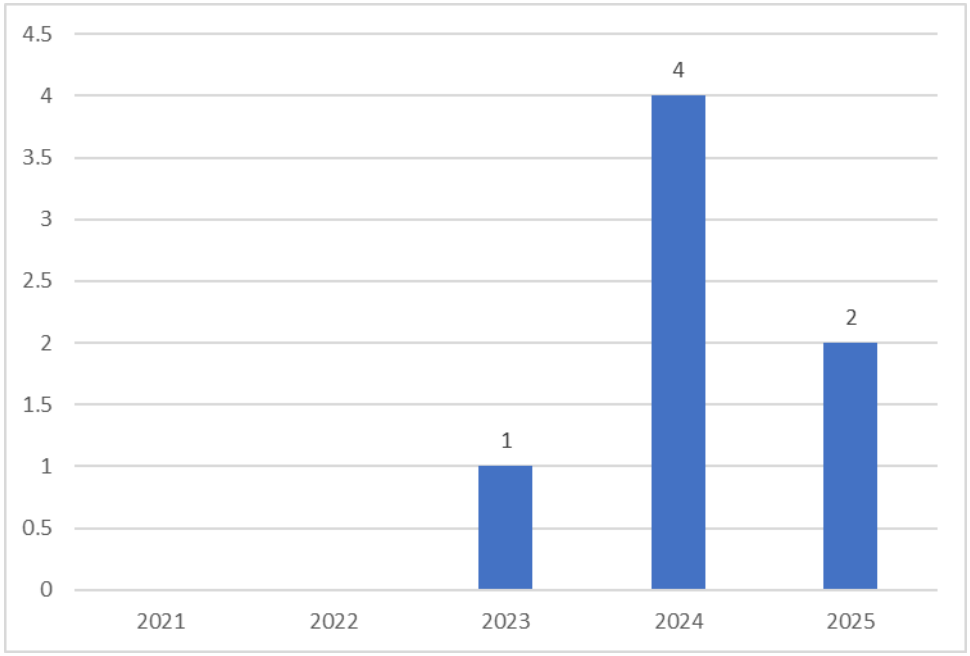


Figure 39: Qualified PACS Services, according to ANSSI in the last 5 years.

[55] Security VISA | ANSSI

Numbers in this figure show the qualified PACS Services, according to ANSSI. Launched in 2023, the scheme shows a direct adoption in the first years. In 2024, 4 providers got qualified but by 2025, the count dropped to 2.

4.3.2.3 Data Collection

Modality	Data provided by ANSSI
Date of Data Collection	03/12/2025

4.4 Vertical Scheme - Detection[56]

4.4.1 PDIS – France

4.4.1.1 Description

Under the banner of the Security Visas[57], the qualification scheme PDIS[58] addresses Security incident detection service providers (SIDS). The goal is for qualified providers to be able to monitor activities within an information system in real time to detect any abnormal or potentially malicious activity.

Date of Creation	2017
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None

4.4.1.2 Statistics covering the last 5 years – Qualified PDIS Services

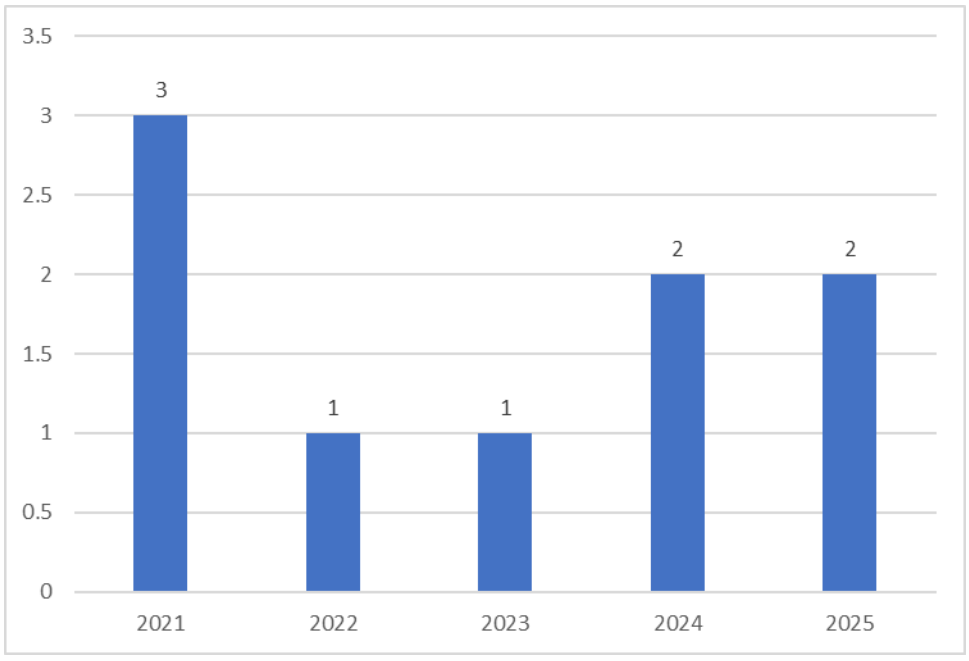


Figure 40: Qualified PDIS Services, according to ANSSI in the last 5 years.

[56] The SOC maturity framework (SOC-MF) developed in the Netherlands has been published in 2024 and does not yet have any certification data. More information can be found: SOC-CMM - Improving security operations globally
[57] Security VISA | ANSSI
[58] Referential PDIS pdis_referentiel_v2.0_en[1].pdf

The numbers in this figure show the qualified PDIS Services, according to ANSSI. The numbers are steady though relatively low. Showing between one and 3 qualified provider per year between 2021 and 2025.

4.4.1.3 Data Collection

Modality	Data provided by ANSSI
Date of Data Collection	03/12/2025

4.5 Vertical Scheme - Incident Response

4.5.1 Vorfallbearbeitung – Germany

4.5.1.1 Description

The certification of IT security service providers by the Federal Office for Information Security (BSI) was originally established to assist the German government in safeguarding the national security landscape, particularly within government sectors.

The BSI's certification process is structured to ensure that both organisations and individual professionals adhere to rigorous standards of competence and reliability. For an organisation to obtain certification, it must employ at least two certified professionals in the specific type of services it offers.

According to BSI website, "certified service provider [according to the German scheme] has demonstrated that he or she has a team of at least two incident experts or one incident expert and two incident practitioners. It offers the following tasks and services:

- Analysis of more complex IT security incidents, especially on-site,
- Rapid containment of the extent of damage from a major IT security incident,
- Identifying the causes of more complex attacks,
- Recovery of various affected systems after an IT security incident.

The aim is to be able to rely on competent and experienced IT security service providers within the framework of the cyber security network who offer support after an IT security incident.

Date of Creation	2023
Scope	Germany
Validity of Certificate	3 years
Mutual Recognition	None

4.5.1.2 Statistics covering the last 5 years – Certified Service Provider on Incident Response - Vorfallbearbeitung

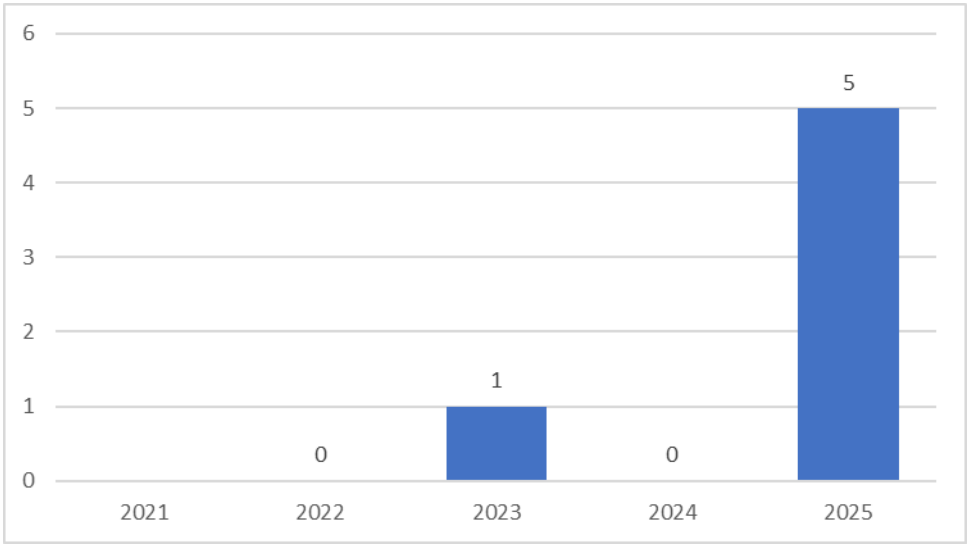


Figure 41: Certified Service Provider on Incident Response, according to BSI in the last 5 years.

The figure shows the certified service provider on incident response according to BSI. Published in 2023, the adoption has shown a timid start. However, the year 2025, with 5 certified service providers indicates a higher adoption.

4.5.1.3 Data Collection

Modality	Data provided by BSI
Date of Data Collection	12/01/2026

4.5.2 PRIS – France

4.5.2.1 Description

Under the banner of the Security Visas[59],The requirements framework for security incident response service providers (PRIS) is a set of rules that apply to service providers wishing to obtain qualification for their services in this area. It covers requirements relating to the incident response provider, its personnel, and the conduct of incident response services.

Qualification can be granted to incident response providers for the following activities: searching for indicators of compromise, digital forensics, malicious code analysis, and managing and coordinating investigations.

Date of Creation	2017
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None

[59] Security VISA | ANSSI

4.5.2.2 Statistics covering the last 5 years – Qualified PRIS Services

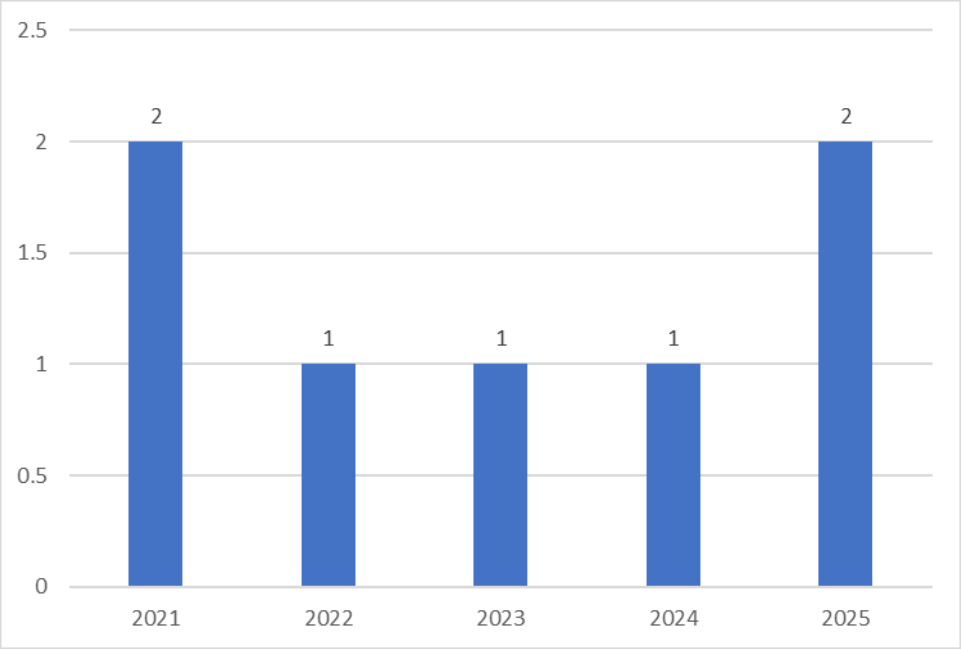


Figure 42: Qualified PRIS Services, according to ANSSI in the last 5 years.

The figure shows the Qualified PRIS Services, according to ANSSI. The progression in terms of the number of qualified providers has been steady in the past five years with between 1 and 2 certifications per year.

4.5.2.3 Data Collection

Modality	Data provided by ANSSI
Date of Data Collection	03/12/2025

4.6 Vertical Scheme - Secure Managed Services

4.6.1 PAMS – France

4.6.1.1 Description

Under the banner of the Security Visas[60], the requirements framework for secure administration and maintenance service providers (PAMS[61]) is a set of rules that apply to service providers who wish to obtain a qualification for their services in this area. It covers requirements relating to secure administration and maintenance service providers, their personnel, and the conduct of services.

Date of Creation	2022
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None

[60] Security VISA | ANSSI
[61]

4.6.1.2 Statistics covering the last 5 years – Qualified PAMS Services

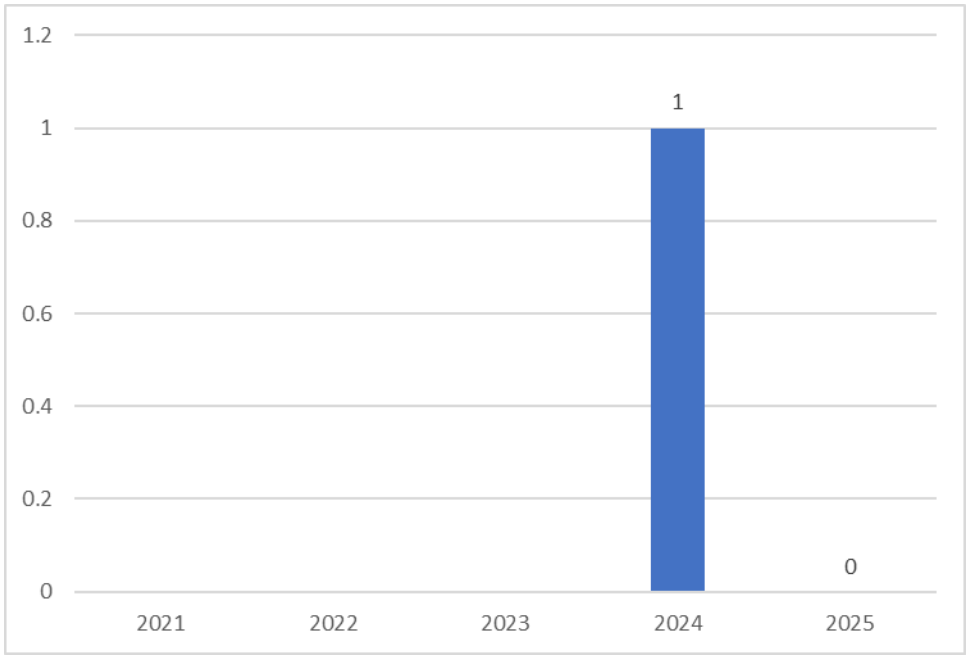


Figure 43: Qualified PAMS Services, according to ANSSI in the last 5 years.

The figure shows the number of services since the launch of the scheme in 2022. Only new listings are considered. The trend indicates no activity during the first two years of the scheme, followed by a minimal start. In 2022 and 2023, the count remained at 0, showing no new services. In 2024, the number reached 1, marking the first listing since the introduction of the scheme.

4.6.1.3 Data Collection

Modality	Data provided by ANSSI
Date of Data Collection	03/12/2025

SECTION 4

Conformity Assessment Bodies

5. Conformity Assessment Bodies

Conformity Assessment Bodies (CABs) constitute a fundamental component of the cybersecurity assessment ecosystem, ensuring the credibility, consistency, and reliability of third-party evaluations. These entities are responsible for performing assessments and, where applicable, issuing certificates that attest to the compliance of ICT products, ICT services, ICT processes and managed security services with defined requirements.

CABs operate within structured accreditation frameworks and are typically subject to international standards, such as ISO/IEC 17025 for laboratories and ISO/IEC 17065 for certification bodies. This ensures a harmonised level of competence, independence, and impartiality across different schemes. Their role is therefore essential in building trust between manufacturers, service providers, regulators, and end users.

From a market perspective, the availability and distribution of CABs directly influence the scalability and accessibility of cybersecurity certification schemes. A higher number of accredited bodies can facilitate market uptake by reducing bottlenecks and supporting competition, while limited capacity may constrain adoption, particularly for emerging or highly specialised schemes.

The CAB landscape is heterogeneous and reflects the diversity of assessment methodologies. It includes evaluation laboratories, certification bodies and, in some cases, entities performing both roles depending on the scheme. This section provides an overview of these actors across the distinct categories of ICT solutions covered in the report, highlighting their role in supporting the overall functioning and growth of the cybersecurity assessment market.

5.1 ICT products Laboratories

In this section we include all accredited laboratories assessing against ICT products schemes. Being formally accredited by accreditation bodies, laboratories represent the cornerstone of third-party cybersecurity assessments. They are the ones in charge of performing the competent tests. Laboratories are usually accredited using ISO/IEC 17025.

The graph below only mentions schemes that count more than one accredited laboratory.

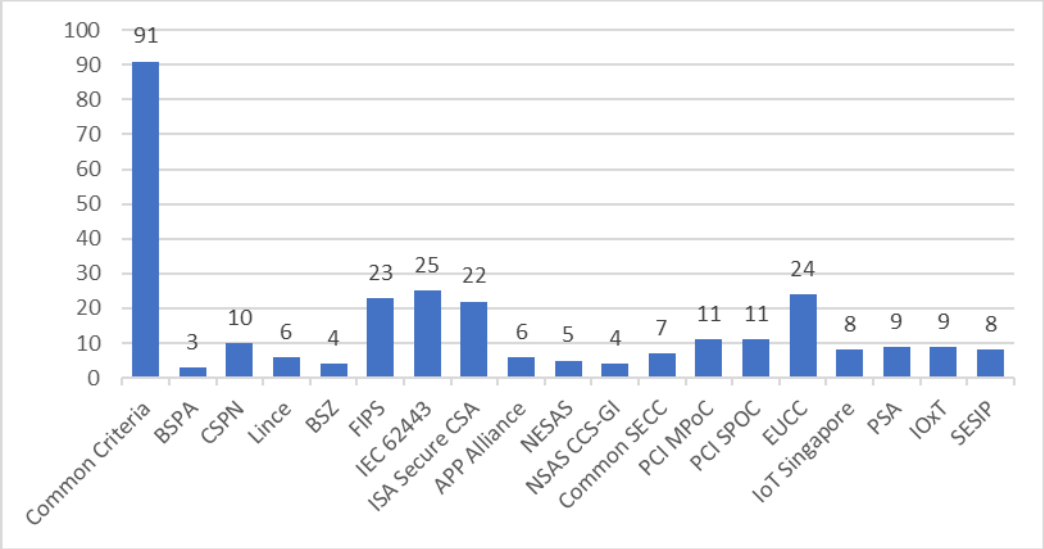


Figure 44: Number of laboratories per ICT products assessment methodology.

The total number of laboratories is 252, most schemes show a stable number compared to the last edition of the report. The new EU scheme EUCC shows a significant adoption with 24 ITSEFs for its first year of operation.

5.1.1 Laboratories based in EU countries

EU countries have many laboratories evaluating different methodologies and schemes. Common Criteria scheme is particularly represented with 48 of the 91 laboratories being in the EU.

However, it is important to note that since February 2026, it is not possible to issue CC Sog-IS certificates. These ITSEFs should therefore be accredited to assess against EUCC.

5.1.2 Data Collection

Modality	Data collected manually from the official website of the different schemes. For standards that do not have a unique scheme website, like ISO/IEC 27001, data have not been collected.
Date of Data Collection	24/04/2026

5.2 Certification Bodies

5.2.1 Description

Certification Bodies establish certificates based on in-house assessments or assessments provided by external CABs accredited under relevant standards. CBs are usually accredited using ISO/IEC 17065.

The graph below only mentions schemes that count more than one accredited CB.

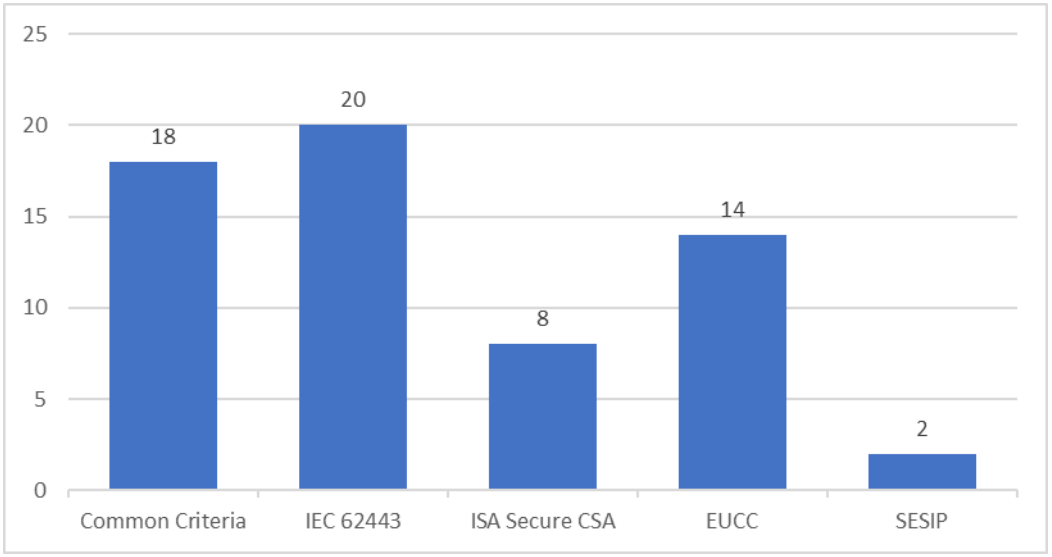


Figure 45: Worldwide Number of CBs per assessment methodology.

The number of CBs remains stable compared to last report study. EUCC dynamically enters the market with 14 Certification Bodies.

5.2.2 Data Collection

Modality	Data collected manually from the official website of the different schemes.
Date of Data Collection	23/06/2025

5.3 Assessment Bodies for Cloud, ICT and MSS Services

The graph below only mentions schemes that count more than one accredited CAB.

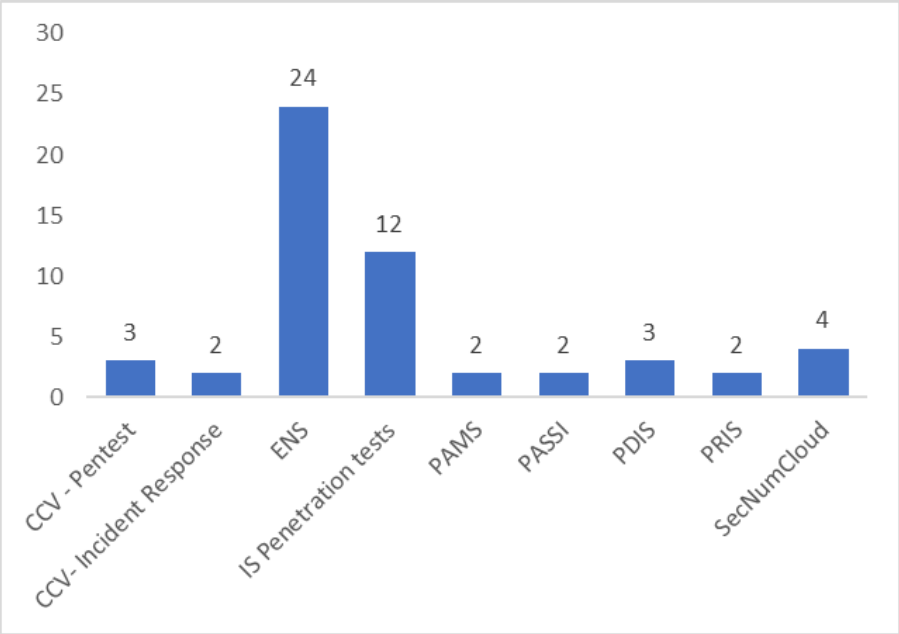


Figure 46: Number of CABs per assessment methodology.

This is the first time the number of CABs for Cloud Services and Managed Security Services have been included in the report.

5.3.1 Data Collection

Modality	Data collected manually from the official website of the different schemes.
Date of Data Collection	04/04/2026

SECTION 4

Appendix

1. Appendix 1: Index of Figures

2. Appendix 2: Acronyms table reference

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AMEX	**American Express**
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
AVA_VAN	**Vulnerability Assessment**
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSPA	**Baseline Security Product Assessment**
BSZ	Beschleunigte Sicherheitszertifizierung
C5	**Cloud Computing Compliance Criteria Catalogue**
CAB	Conformity Assessment Body
CB	**Certification Body**
CC	Common Criteria
CCN	**Centro Criptológico Nacional**
CCRA	Common Criteria Recognition Arrangement
CESTI	**Centres d'Évaluation de la Sécurité des Technologies de l'Information**
CLS	Finnish Transport and Communications Agency
COTS	**commercial off-the-shelf**
CPoC	Contact Payment on COTS
CPSTIC	**Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación**
CRA	Cyber Resilience Act
CSA	**Connectivity Standard Alliance**
CSA	Cybersecurity Agency of Singapore
CSA STAR	**Cloud Security Alliance - Security Trust Assurance and Risk**
CSP	Cloud Services Provider

CSPN	**Certification de Sécurité de Premier Niveau**
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CyFun	**Cybersecurity Fundamentals**
DISC	Discover Information Security & Compliance
EAL	**Evaluation Assurance Level**
ECB	European Central Bank
ECSG	**European Cards Stakeholders Group**
EFTA	European Free Trade Association
eIDAS	**Electronic IDentification, Authentication and trust Services**
EMV	Europlay Mastercard Visa
ENISA	**European Union Agency for Cybersecurity**
eSA	eUICC Security Accreditation
ETSI	**European Telecommunications Standards Institute**
EU	European Union
EU5G	**European Union Cybersecurity Certification Scheme on 5G**
EUCC	Common Criteria based European candidate cybersecurity certification scheme
EUCS	**European Union Cybersecurity Certification Scheme on Cloud Services**
FedRAMP	Cloud Computing Compliance Criteria Catalogue
FIDO	**Fast Identity Online**
FIPS	Federal Information Processing Standards
GCA	**Global Cyber Alliance**
GSM	Global System for Mobile Communication
HSM	**Hardware security module**
IC	Integrated Chip
ICT	**Information and communications technology**
IEC	International Electrotechnical Commission
IECEE	**IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components being a body of the International Electrotechnical Commission**

IOT	Internet of Thing
ioXt	**Internet Of Secure Things**
IP	Internet Protocol
IPS	**Intrusion Prevention System**
ISA	International Society of Automation
ISAE	**International Standard on Assurance Engagements**
ISO	International Organization for Standardization
ITSEC	**Information Technology Security Evaluation Criteria**
ITSEF	Information Technology Security Evaluation Facility
JCB	**Japan Credit Bureau**
LINCE	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad
MPoC	**Mobile Payments on COTS**
MRA	Mutual Recognition Agreement
NBV	**Nationaal Bureau voor Verbindingsbeveiliging**
NCSC-FI	National Cyber Security Centre Finland
NESAS	**Network Equipment Security Assurance Scheme**
OCR	Optical Character Recognition
OS	**Operating System**
OWASP	Open-Source Foundation for Application Security
PACS	**Prestataires d'Accompagnement et de Conseil en Sécurité**
PAMS	Prestataires d'Administration et de Maintenance Sécurisées
PASSI	**Prestataires d'Audit de Sécurité des Systèmes d'Information**
PCI DSS	Payment Card Industry Data Security Standards
PCI PTS	**PCI Payment Terminal System**
PCI SSC	PCI Security Standards Council
PDIS	**Prestataires de Détection d'Incidents de Sécurité**
POI	Point of Interaction
PRIS	**Prestataires de Réponse à Incidents de Sécurité**
PSA	Platform Security Architecture

PSWG	**Product Security Working Group**
SCADA	Supervisory Control and Data Acquisition
SESIP	**Security Evaluation Standard for IoT Platforms**
SME	Small and Medium Enterprises
SOG-IS	**Senior Officials Group Information Systems Security**
SPoC	Software-based PIN entry on Commercial off-the-shelf devices (SPoC)
SSAE	**Statement on Standards for Attestation Engagements**
STIC	Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
TCSEC	**Trusted Computer System Evaluation Criteria**
TEE	Trusted Execution Environments
TOE	**Target of Evaluation**
Traficom	Finnish Transport and Communications Agency
TTP	**Tactics, Techniques and Procedures**
UK	United Kingdom
US	**United States of America**

3. Appendix 3: Modifications from last version of the report

The following modifications have been included in this version of the report compared to previous version:

- The following schemes have been removed because the number of certificates are not available, are not in scope with cybersecurity or because they don't have activity: FIDO, NESAS CCS-GI, EMVco, PCI HSM, PCI PTS, Calypso, Global Platform TEE, IoT Label – Finland, Matter, MiFare, HITRUST CSF, PCI DSS and FeliCa.
- In the chapter dedicated to ISMS and Cloud services, the following schemes have been added: CPSTIC Cloud evaluations and IT-Grundschutz.
- Schemes related to Managed Security Services have been included.
- The report also includes the information related to cloud services and Managed Security Services Assessment Bodies.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union