PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le
N° **/ANSSI/SDE/PSS/CCN**
Référence **: ANSSI-CCN-MQ_v6.4**

CERTIFICATION BODY QUALITY MANUAL

Subject: Certification Body Quality Manual

Application: As soon as approved

Circulation: Public

COURTESY TRANSLATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

REVISION HISTORY

Version	Date	Modifications
1.0	01/12/2003	Creation
2.0	08/03/2016	Document revision
3.0	27/05/2019	Compliance with EN ISO/IEC 17065 standard
3.1	28/08/2019	Clarification in Appendix C for easier reading Updated calculation of risk analysis priorities
3.2	29/01/2020	Internal audit results : Le "comté des utilisateurs" devient "groupe des utilisateurs" Impartiality preservation added Alignment of §7.8 with §9.1 of CER-P-01 EN ISO/IEC 17065 conformity matrix added
4.0	26/01/2021	Reports / certificates publication and validity date management added Spelling errors corrected and details added Removal of the paragraph on "utilisation des certificats et usage de la marque" to include its content in the dedicated chapter Addition of a paragraph dealing with derogatory measures New graphic charter taken into account
5.0	23/09/2021	Details on related organizations added ITSEF status corrected. ITSEF aren't an related organization but subcontractors Details on the DG's delegation of signing authority added
6.0	12/01/2023	Impartiality preservation process added Risk analysis redesigned Terms and conditions for revisions and reassessments added References added Organization chart updated Appendix C removed
6.1	13/05/2024	Correspondence following changes to PER-P-01 made Minor updates (change of website address, deletion of monitoring procedure no longer applicable, etc.)
6.2	18/10/2024	EUCC update and dedicated chapter added
6.3	13/02/2025	Scope of accreditation updated EUCC amendment updated
6.4	18/10/2025	Update following the accreditation of CCN

In accordance with the April 18th, 2002 decree No. 2002-535 as amended, the present manual has been submitted to the Executive Certification Committee, which gave a favourable opinion.

It is planned that this application note will be submitted to the Executive Certification Committee for comment when major modifications are made.

This application note is available at the ANSSI's institutional website (www.cyber.gouv.fr).

TABLE OF CONTENTS

Chapitre 1 The Quality Manual

1.1. Purpose

The quality manual presents the methods and procedures used by the national certification body (CCN - Centre de Certification National) to ensure and maintain the quality and continuity of its services to certify the security of IT products and systems.

The quality manual is the reference for:

- any third-party entity calling upon the agency's certification services;
- any person or entity of ANSSI exercising a function related to certification activity, in order to define their role and responsibilities;
- any newly hired personnel at the certification body, to inform them of ANSSI policies and to foster their integration;
- peer review between ANSSI and other organizations – foreign ones in particular – with a view to creating mutual recognition.

1.2. Creating, updating and distribution

The manual is drawn up and updated by the quality manager. It is then checked by the head of certification body, validated by the "Security Products and Services" division manager and the head of the Expertise Department , and then approved by the Directeur Général of ANSSI. It is also submitted for comment to the Executive Certification Committee when major modifications are made.

Updates to the quality manual follows the same validation process as the initial release.

The quality manager ensures the quality manual's distribution, following the same rules as for other documents of the quality system.

All versions are stored by electronic means. However, the French version, on paper, is the reference version.

Chapitre 2 The certification scheme

2.1. Regulatory framework

French amended decree No. 2002-535 of April 18th, 2002, related to the evaluation and certification of the security provided by information technology products and systems, defines the regulatory context and organization required for an evaluation to be carried out by a third party and for its verification, leading to the issuing of certificates.

These rules are implemented in a third-party certification scheme.

2.2. The executive certification committee

Article 15 of amended decree No. 2002-535 defines the Executive Certification Committee's missions regarding IT security as follows:

- formulating opinions or proposals on the certification policy, on the rules and standards used for evaluation and certification procedures and on technical guides provided to the public;
- providing an opinion on issuing and revoking approval for ITSEF (Information Technology Security Evaluation Facilities);
- examining, with an objective of conciliation, any dispute, submitted to it by the parties, regarding the evaluation procedures organized by amended decree 2002-535;
- providing an opinion on mutual recognition agreements with foreign organizations.

The executive certification committee meets at least once a year. It is chaired by the Secrétaire général de la défense et de la sécurité nationale or his representative. It reports to the Premier Ministre.

2.3. The user committee

The French certification scheme user committee is formed of a varied range of participants, mainly sponsors and developers of certified products, but also contracting parties that rely on certification to specify security requirements for products they use or recommend. The committee is set up, at the initiative of the certification body, to bring together the participants, thereby creating a forum for exchanging information and consulting with the certification body.

The user committee's objectives are to enable ANSSI:

- to communicate changes in rules and standards;
- to identify the needs and expectations of the scheme's users;
- to exchange opinions on future prospects.

Certain users can be consulted for their expertise in order to support the agency's ongoing works. Even so the proposals remain consultative.

2.4. The certification body

2.4.1. Status

French Cybersecurity Agency (ANSSI) was created by decree No. 2009-834 of 7 July 2009 (official journal of 8 July 2009), as a national authority. ANSSI reports to the General Secretary for Defense and National Security (SGDSN) whom assists the Prime Minister. ANSSI's Executive Office is composed of a Director General appointed by Decree from the Prime Minister, and a Deputy Director General, both of whom are assisted by a Chief of Staff and a Head of Cabinet.

The certification body is attached to the Expertise Department and to the Security Products and Services Division.

As a national authority, the certification body benefits from government financial stability. The certification body's activities are carried out in the framework of the French amended decree 2002-535 of 18 April 2002, rather than the framework of contracts, in the commercial sense of the term. Its status prevents it from providing advisory or training services intended to help obtain or retain certification.

2.4.2. Impartiality

The certification body must guarantee that certification decisions are taken objectively and reliably, and that they are not influenced by commercial or other considerations.

To do this, the certification body sets up a system for preserving impartiality [QUA-P-02] in order, in particular, to formalise opinions on the risk analysis concerning the impartiality of its activities. This system includes a committee made up of members with a significant interest in the certification activities implemented by the certification body, the risk analysis dedicated to the impartiality of the certification body's activities and all other documents essential to the implementation of impartiality.

In addition, the certification body implements the certification policies and principles applied to the certification body, its staff, the ITSEF and external persons in order to guarantee total independence of the certification decision.

Certification body policies and principles :

- the work of the certification body is carried out within the framework of decree 2002-535 of 18 April 2002, as amended, and not through commercial contracts;

- the certification body is a subdivision of a government department;

- the financial resources are provided by the State. The services offered by the certification body are free of charge;

- the certification body and ANSSI are not designers, manufacturers, installers or maintainers of certified products;

- the certification body does not issue any confidential information during meetings attended by all members of the Users Group;

- the certification body does not use external personnel to carry out certification activities;

- the certification body does not agree to pool its staff with an entity likely to undermine its impartiality;

- the certification body does not provide consultancy or training aimed at obtaining or maintaining certification;

- the certification body does not provide consultancy services for the design, manufacture, installation or distribution of a product which is in the process of being certified or which has already been certified;

- the certification body meets criteria which enable it to guarantee its customers total impartiality both in carrying out the work and in the final certification decision, whether positive or negative, in accordance with standard EN ISO/IEC 17065 [17065].

Policies and principles applied to ANSSI personnel involved in a certification project:

- all ANSSI personnel involved in projects are civil servants with at least Secret level clearance. They undertake, among other things, to respect the strictest secrecy regarding sensitive information entrusted to them in the performance of their duties and to declare any fact which could call into question their impartiality;

- each person from ANSSI working on certification projects must declare to their superiors any past, present or future fact which could call into question their independence when a project is proposed to them;

- each person at the certification body must refuse any solicitation, promise, gift, present or advantage whatsoever, either directly or through an intermediary, which could compromise his or her independence of judgement;

- the technical recommendations published by ANSSI's technical experts do not call into question the foundations of impartiality, since they are addressed to the entire community and not to a particular developer;

- a member of the Certification body who has provided recommendations or who has been employed by the complainant may not participate in the review or approve the resolution of the complaint for a period of two years following the issuance of the recommendations or employment by the complainant;

- The decision to resolve a complaint must be taken, reviewed and approved by a member of the Certification body who is not involved in the activities related to the complaint. However, a member involved in the complaint may intervene in the preparation of the response.

Policies and principles applied to ITSEF:

- each ITSEF undertakes not to involve personnel who have previously issued recommendations to the developer for the product under evaluation (e.g. drafting the security target, design assistance or cryptographic specification);

- each ITSEF must ensure that its staff are independent and impartial vis-à-vis the sponsors or developers;

- ITSEF may give recommendations to their customers. However, there is a separation between those involved in giving recommendations and those carrying out the assessment work.

Policies and principles applied to external parties :

- If an audit of the certification body is carried out by external parties (a third-party company that has signed a contract with ANSSI, or members of COFRAC), the auditors accessing the data from the certification projects sign a confidentiality undertaking at the time of each new audit;

- auditors from foreign certification body only have access to information authorised in advance by the sponsors of the products being assessed.

These external parties may only consult the information in the presence of a person from the certification body, on the certification body's premises.

In accordance with article 16 of decree 2002-535 as amended, the members of the steering committee are appointed to ensure broad representation of parties with a significant interest, particularly in the handling of disputes. The policy applied is as follows

- the members of the Certification Steering Committee are bound by confidentiality and impartiality through the 'Certification Steering Committee Rules of Procedure' signed by the parties;

- the members of the Steering Committee have access to all the information they need to carry out their duties.

Policies relating to related organisations :

- the webmaster is employed by ANSSI, and is therefore subject to the same rules as the members of the certification body, and is cleared to at least Secret level. Among other things, he or she undertakes to maintain the strictest secrecy regarding sensitive information entrusted to him or her in the course of his or her duties;

- the cleaning staff work in the offices during working hours and in the presence of at least one person from ANSSI. The SGDSN takes great care in selecting the cleaning company and its staff, insofar as the premises in which these people work are located in a protected area within the meaning of [IGI 1300] ;

- the lessor of the premises in which the certification body carries out its activities only very rarely has relations with the members of the certification body;

- the general services also only very rarely have relations with the members of the certification body;

- the gendarmes who carry out reception and security duties, because of their status, present little risk;

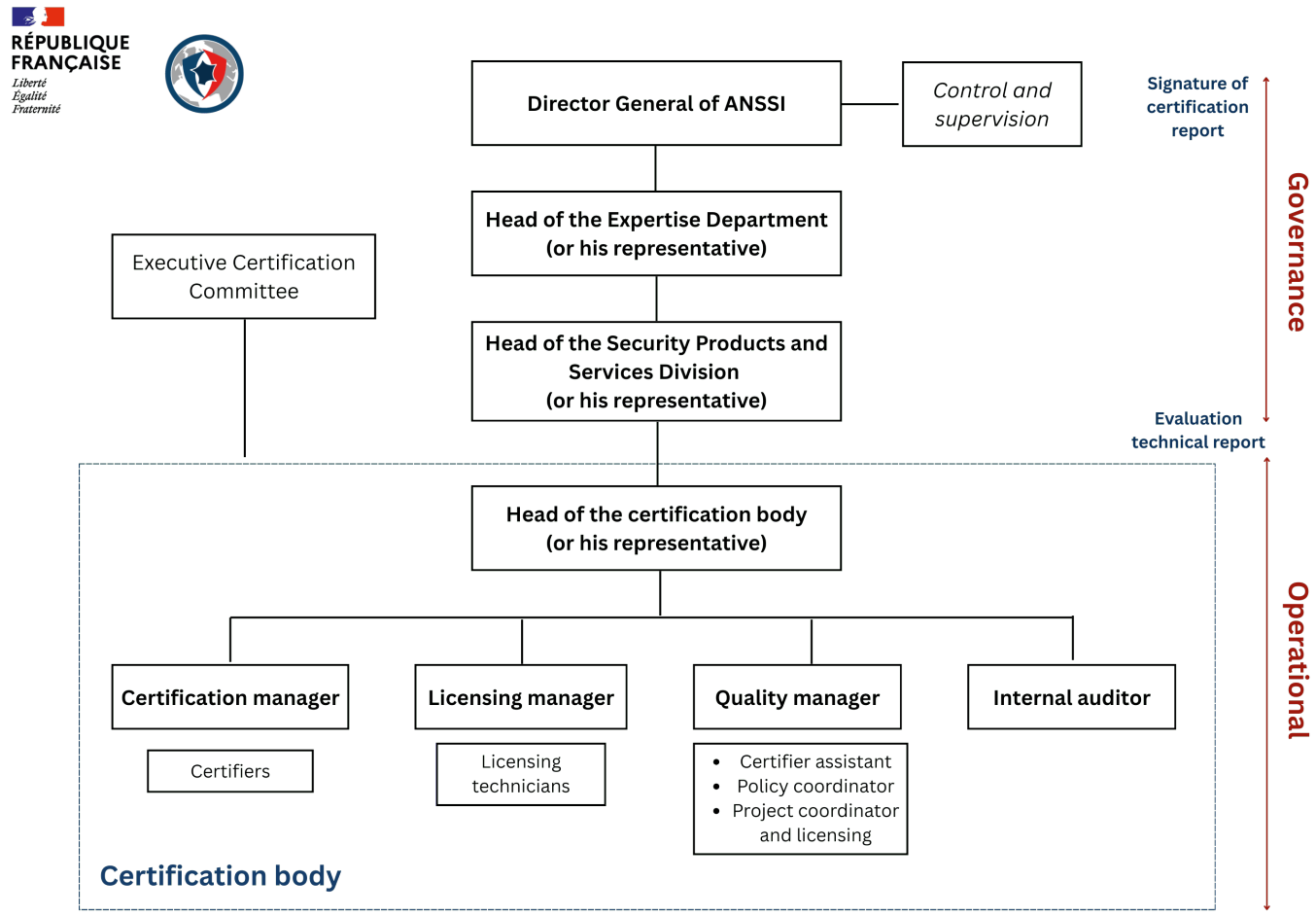
- the members of the Classified Interministerial Information Systems Operator (OSIIC) are subject to the same rules as the members of the certification body and are cleared to at least Secret level. As such, this operator is responsible for ensuring the security of the SGDSN's information and therefore that linked to the work carried out by the certification body. This operator is also responsible for safeguarding, storing and destroying the digital documents produced by the certification body;

2.4.3. Activities

The certification body's mission is to:

- Implement the agency's certification policy;
- Ensure the examination of all applications and the maintenance of certificates issued;
- Ensure the examination of all candidate applications for ITSEF;
- Conduct audits of ITSEF to confirm or revoke their qualification level and technical skills;
- Embody the agency at national and international certification meetings and talks;
- Define the rules and standards used for evaluation and certification procedures and technical guides;
- Promote the French certification scheme publicly and share the latest changes;

2.4.4. *Organization*



The responsibilities for certification activities are defined as follows:

- **Director General** appointed by Decree from the Prime Minister, is responsible of signing certificates and ITSEF's licensing;
- **Head of the Expertise Department (or his representative)** has authority over the certification body but does not intervene in the certification decision. The head of the Expertise Department (or his representative) chairs the Executive Certification Committee as the General Secretary for Defence and National Security's representative;
- **Head of the Security Products and Services Division** has authority over the certification body but does not intervene in the certification decision. In the certification process, he ensures the adequacy of all the certification and maintenance reports;
- **Head of certification body** is responsible for the certification body's operational management. He takes part in recruiting his staff, verifying that they are competent to fulfil their duties. He keeps an up-to-date record of staff experience and training. He is responsible for defining the approval process for the ITSEF. He is responsible for recognition of foreign certificates and maintains contact with his foreign counterparts. He participates in the management of evaluation and certification criteria alongside the

certification manager. He also decides with the certification manager (or a certifier) wether the certificate can be transmitted for signature;

- **Certification Manager** is responsible for implementing the certification scheme. He manages the certifiers team by monitoring the projects and schedules. He also analyses the changes in the technical framework and contributes to the national and internal certification studies and exchanges.
- **Licensing Manager** is responsible for implementing the licensing process and standards. He manages the licensing technicians by monitoring the application for licensing and the licensing audit. He also analyses the changes in the technical framework related to licensing criteria and standards and contributes to the national and international studies and exchanges;
- **Quality manager** is responsible for implementing, maintaining and improving the quality system. He is also responsible for the quality training of certification body staff;
- **Certifiers** are responsible for monitoring evaluations and to ensure that the certification rules and procedures are followed. They are not involved in the evaluation work, nor in the final certification decision. Certain certifiers are qualified to conduct internal audits planned by the quality manager. However it should be noted that most internal audits are carried out by external organizations;
- **Licensing technicians** are responsible for monitoring the licensing procedure from registration to audit. They ensure the ITSEF act in compliance with the current rules and standards, by also verifying the employee's skills and the ITSEF technical equipment;
- **Project coordinator and licensing** is responsible for establishing partnership with the certification and licensing stakeholders (ITSEF and developers). He assists both the Certification Manager and the Licensing Manager in updating and analyzing their project's results;
- **Certifier assistant** is responsible for administrative follow-up on certification body documents and for assisting the head of certification body and certifiers with application, registration, editing and logistics related to their activities;

2.4.5. Stakeholders roles

The certification body's contacts internally include:

- The governance body, composed of all ANSSI's members hierarchy outside the certification body. Their roles are:
    - The Director General
        - signs certification and maintenance reports as well as the associated CC and CSPN certificates;
        - signs ITSEF's licensing following consultation with the executive certification committee;
        - sign the application notes used for assessment and certification procedures following consultation with the executive certification committee;
        - signs mutual recognition agreements with foreign entities following consultation with the executive certification committee;
        - signs part of the quality process documents;

  - Head of the Expertise Department:
    - chairs quality management review meetings;
    - signs part of the quality process documents;
    - represents General Secretary for Defence and National Security during executive certification committee;
  - Head of the Security Products and Services Division
    - ensures consistency of all certification reports;
    - confirms certain documents related to the "quality" process;
- ANSSI's experts who may assist certifiers on specific technical issues. In all cases, certifiers are free to call on them and to account or not their advises;
- Human Resources deals with all aspects of personnel management at the certification body (recruitment, private interviews, training follow-up, etc.);
- Legal Affairs, which is called upon by the certification body for all matters requiring legal advice (Memorandum Of Understanding, Non-Disclosure Agreement, etc.);
- The control and supervision mission (MCS) is responsible for authorizing and supervising the certification body within according to the article No. 58 of the [CSA];
- Ordering institution such as the Qualification and Agreement body of ANSSI, approves trust products and service providers. Those ordering institutions are only involved in the certification process to validate the security issues described in the security target, to ensure that the French government's needs are respected.

The certification body's contacts externally include:

- ITSEF licensed by the certification body are responsible for conducting the evaluation in accordance with the Common Criteria or First Level Security Certification schemes. These facilities are responsible for submitting evaluation reports to the certification body, which then validates them. ITSEF are considered as subcontractors, and must comply with the document's rules to which they are committed;
- sponsors and/or developers who request a certification evaluation for his/their product;
- Ordering institution are responsible for validating that the safety targets submitted with the evaluation files meet their own requirements;
- counterpart schemes from other organizations or countries that participate in the harmonization of international standards and CCRA, SOG-IS and EUCC audits (peer review);
- related organizations/staff: webmaster, cleaners, lessor, general services for the General Secretariat for Defence and National Security, Operator of Classified Interdepartmental Information Systems (OSIIC), COFRAC, management bodies for the following agreements : CCRA, SOG-IS, EUCC and *Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed-time certification process, BSI/ANSSI*.

2.4.6. Certification body staff

The certification body sets recruitment and skills monitoring requirements. Cf. [PER-P-01], latest version.

The certification body does not employ temporary staff for certification activities.

Chapitre 3 Quality management system

3.1. Quality policy

3.1.1. Scope

The certification body operates in a field where confidence, rigour and continuity take on their full meaning. Given the wide geographical and cultural range of its customers, the certification body must, through its quality system, provide the highest levels of confidence in its work, in order to ensure the recognition of its certificates, particularly because of the international framework in which it operates.

Its objectives focus on the recognition of the certificates it issues:

- on a national scale, to establish confidence in the certification work that it carries out with all involved parties;
- on a global scale, to enter in the framework of mutual recognition agreements that it undertakes.

3.1.2. Requirements

To obtain and maintain this recognition, the certification body acts in compliance with the EN ISO/IEC 17065 standard and CCRA and SOG-IS agreements:

- traceability: all evaluations must be reproducible and all evidence elements related to the issuing of the certificate must be identified and stored;
- consistency: all certificates must reflect a comparable level of assurance, regardless of the staff responsible for the monitoring and the evaluation facility that conducted the evaluation;
- confidentiality: the certification body must ensure the confidentiality of sensitive information entrusted to it, or that it develops in the framework of certification;
- impartiality: the certification body must be able to carry out its missions irrespective of any internal changes (organization, staff);

The certification body agrees to:

- publish and update the certification scheme's rules and standards;
- release and update the published certificates and the list of currently approved ITSEF;
- ensure the ITSEF are skilled to conduct the requested evaluation;
- work with skillful and qualified staff.

3.2. Quality planning

3.2.1. Internal audits

Periodic system audits are organized by the quality manager and conducted by qualified auditors who are independent of the functions audited, in accordance with the annual audit program.

The quality manager plans and manages audits so that every requirement of the NF EN ISO/IEC 17065 standard is audited at least once a year.

3.2.2. Quality risk management

Whenever necessary, the certification body takes into account any risks that could compromise its impartiality.

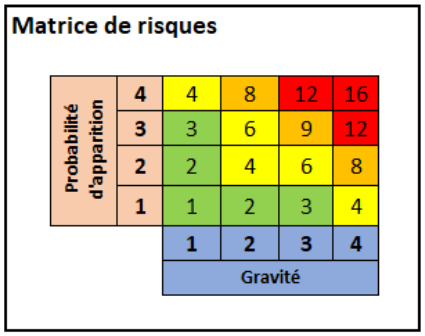
Through its risk analysis, the certification body is able to detect and neutralize the identified uncertainties. An annual review is scheduled and approved as part of the impartiality management procedure [QUA-P-02].

In order to conduct its risk analysis, the certification body choose an appropriate methodology meant to list potential hazards as perceived by the main parties involved (certification body's staff, governance, sponsors and developers, etc). Each of the potential hazard is then measured on a scale of 1 to 4, to identify its impact and likehood.

Impact		
Scale	**Category**	**Description**
1	Minor	Minor event not affecting impartiality
2	Moderate	An event that does not have a major impact on impartiality
3	Major	Major event affecting impartiality system
4	High	Detrimental event that harms deeply the impartiality system

Likehood		
Scale	**Category**	**Description**
1	Very Unlikely	Once a year at most
2	Unlikely	Once a quarter at most
3	Likely	Once a month at most
4	Very likely	Several times a month

The result of these ratings identifies the Risk Level, based on the following formula of multiplying the value of the Impact to the value of Likehood. I (impact) X L (Likehood) = Risk Level



Risk Levels are then labeled as follow:

Risk assessment matrix	
Scale	**Description**
Low 1-3	Known residual risks requiring no specific action
Medium 4-6	Known and controlled risks requiring no specific action
High 8-9	Risks requiring preventive action
Critical 12-16	Risks for which corrective action is imperative and endorse for immediate action

The means taken to control the risk determine the risk level after the corrective action. Some of the risks are considered as known and residual and not require specific action.

Detection rating matrix		
Scale	**Detection**	**Description**
1	Easily detected	Measures allow easy detection of risk
2	Detectable	Measures allow detection of risk
3	Partially detectable	Measures allow partial detection of risk
4	Undetectable	Measures fail to detect risk

A new rating is then issued, making it possible to categorize risks on the basis of actions to be taken or not. Critical risks will be prioritized.

Scale	**Description**
Low 1-3	Risks requiring no specific action
Medium 8-12	Risks requiring no specific action
High 24-27	Risks requiring preventive action
Critical 48-64	Risks requiring imperative and immediate actions

The certification body carries out an internal review once a year to identify any new risks and the measures that have been or can be established to remedy the risks.

Preventive and corrective actions are monitored and handled as part of the quality management system.

3.2.3. Management reviews

During an annual meeting organized by the quality manager[1], the certification body's governance ensures that the quality management system remains relevant, efficient, effective, updated and available for all involved parties.

The following main points are dealt with during the management review meeting:

- the results of the audits (internal, external, mock);
- analysis of the "feedback", in particular the anomalies observed;
- the status of the corrective and preventive actions;
- the changes that may affect the quality management system;
- the assessment of the quality system's effectiveness;

Additional meetings and reviews may be organized throughout the year upon request.

3.3. Documentation System

The certification body's documents used for certification activities are stored as detailed in the documentation hierarchy. Each document is available for inspection by regulatory authorities and subject to the requirements set forth by EN ISO/IEC 17065 standard.

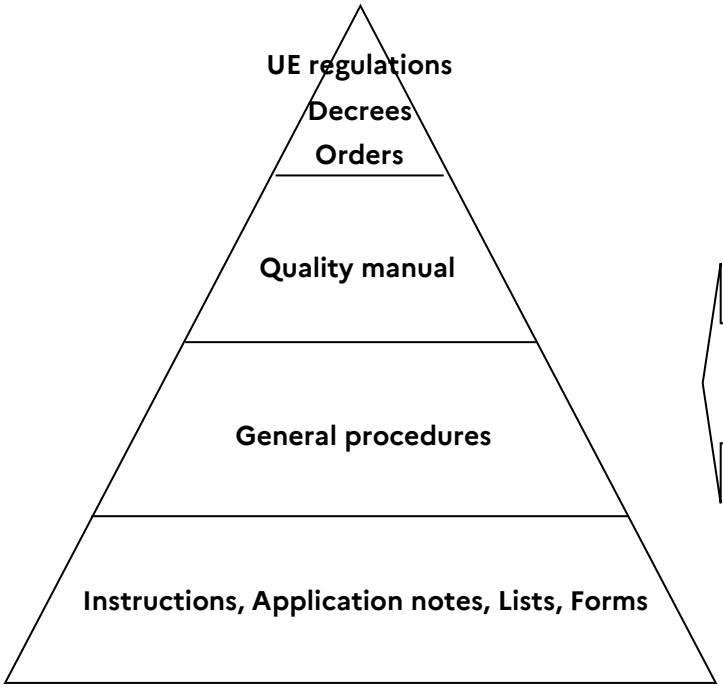
A document review is made by the quality manager at least once a year. The aim is to ensure that the latest documents versions are being used by the certification body's staff, the user committee and other involved parties.

[1] Procedure ANSSI-CC-QUA-P-01 "Management Reviews"

3.3.1. Documentation Hierarchy

The certification body quality documentation is displayed as follow:

Organization



Accreditation standards: EUCC CCRA and SOG-IS EN ISO/IEC 17065, EN ISO/IEC 17025
Evaluation criteria: Common Criteria, ITSEC, EN ISO/IEC 15408 EN ISO/IEC 18045 First Level Security Certification (CSPN) EN 17640 (FiT CEM)

Application

Input	Exit	
Certification request / application form Evaluation report Customer Satisfaction Survey	Registration letter Certification report review Certification report and Certificate Closing letter Audit report Approval audit report Customer Satisfaction Survey	Records concerning certification and approval Customer Satisfaction Survey
Minutes of management reviews Program of internal and external audit	Anomaly report Internal and external audit	Records concerning the quality system

3.3.2. Document control

Documentation is prepared and controlled in accordance with the [DOC-P-01] procedure established by the certification body.

The quality manager maintains a list of all quality documents used by the certification body.

3.3.3. About certification requests recording

There are three types of records to show that all procedures and instructions regarding the certification activity have been properly applied:

- records kept on paper, retained at the certification body or in an archive;
- records stored by electronic means;
- samples provided by sponsors, retained at the certification body.

Recordings are kept for a minimum of 10 years.

Chapitre 4 Certification terms and conditions

4.1. Non-discriminatory access and processing

All developers and suppliers of products and IT systems have access to ANSSI's certification services. ANSSI ensures that all objects submitted for certification receive equal treatment.

Assigning certification is solely contingent on complying with the operating rules of the scheme and satisfying the evaluation criteria.

4.2. Reference documents

All public documents concerning certification are available or referenced at ANSSI's institutional website (www.ssi.gouv.fr)

In particular, the following documents:

- regulatory texts related to the IT product and system's certification;
- certification body's public operating documents (such as procedures, instructions and application notes);
- forms including ANSSI's official certification request;
- evaluation criteria.

4.3. Accreditation scope [EUCC]

The activities of the national certification body's accreditation [EUCC] to ISO/IEC 17065 are listed below in accordance with [CERT CPS REF 48]:

Certification item category	Assurance levels
Product and system "Generic software and network products"	Evaluation Assurance Level higher as defined by the Commission Implementing Regulation (EU) 2024/482 EAL 7+ of ASE TSS.2 and ALC FLR.3 in compliance with ISO/IEC 15408-3 and ISO/IEC 15408-5 standard
Product and system "smart card and similar devices"	
Product and system "hardware devices with security boxes"	
Protection profile	All APE and ACE class safety assurance components as defined in ISO/IEC 15408-3

4.4. Evaluation criteria

The criteria and evaluation methodologies used are approved by the executive certification committee.

These evaluation criteria are subject to change or to be supplemented by technical guides, depending on the technology concerned or specific contexts.

4.5. Certification requirements modifications[2]

The certification requirements may need to change over time such as:

- changes to evaluation criteria coming from international or national standards bodies: directly available from the relevant authorities;
- adaptations of the requirements for a particular field: if they are mandatory or dependent on the national scheme, they are announced by way of a scheme application note that specifies the application schedule;
- changes to the certification scheme's practices: major changes require the executive certification committee's opinion.

[2] Procedure MOD/P/01 "Changes To Certification Requirements"

Chapitre 5 Certification request

5.1. Application form content

After selecting an accredited ITSEF, the sponsor of the evaluation sends ANSSI's certification body an official certification request via the Common Criteria Application form or the First Level Security Certification one.

As indicated in Art. 2 of decree 2002-535, both application forms contain in particular :

- the terms and conditions of certification;
- the commitment of the sponsor and the ITSEF to respect the certification rules;
- the description of the object to be evaluated, including the security target or the protection profile where applicable;
- Supply delivery schedule delivered by the sponsor to the ITSEF and ANSSI;
- the provisional work plan drafted by the ITSEF during the preparation of the Common Criteria evaluation or the estimated delivery time of the First Leval Security Certification's results.

5.2. Request register

Based on the application form, the certification body:

- verifies that the signature's sponsor is binding:
- conducts a thorough document review, particularly regarding the security target and the provisional work plan; if the considers that the security objectives are not defined in a relevant manner with regard to standards, technical specifications or best practice rules applicable when the evaluation begins, they notify the sponsor that, in view of the current state of the file, it cannot proceed with the certification process;
- verifies the prospective workload for the evaluation;
- verifies that the ITSEF has the appropriate licensing autorisation;
- indicates the certifier's name appointed to monitor the evaluation.

The certification body considers the very existence of the evaluation to be confidential by default. Therefore, the certification body does not make any public disclosure of the evaluation unless requested by the customer.

Chapitre 6 Evaluation

6.1. Information Technology Security Evaluation Facilities

6.1.1. Roles and responsibilities

ITSEF are licensed by ANSSI's certification body and are therefore obliged to follow the rules and standard's scheme. The evaluation facility carry out the evaluations: they act as third-parties, independent from the product developers and sponsors.

The certification body is in charge of monitoring the licensing procedure from registration to audit. The licensing team ensure that the ITSEF act in compliance with the current rules and standards, by also verifying the employee's skills and the evaluation facility technical equipment defined in the following licensing procedures [CC-AGR-P-01] and [CSPN-AGR-P-01].

Evaluation facilities are made up of teams of experts and managers, often within an organization with a broader scope. However, the approval criteria require partitioning from the other activities of the organization to which the evaluation facility is attached.

6.1.2. Licensing process

For CC, ITSEF must be accredited by COFRAC (COmité FRançais d'ACcréditation – French accreditation body) according to ISO/IEC standard 17025 "General requirements for the competence of testing and calibration laboratories." COFRAC's technical guides specify each field of information technology security assessment.

ITSEF shall master particular techniques and capable to handle sensitive information.

ANSSI performs a continuous monitoring of the evaluation facilities and makes sure that the obligations related to licensing are respected. Regular audit are performed by the certification body and ANSSI technical experts.

For EUCC, this licenses includes the authorization by the national cybersecurity certification authority.

6.1.3. Evaluation work carried out by the evaluation facility

ITSEF conduct the evaluation work in accordance with the selected evaluation criteria and the work schedule. The appointed certifier monitors the evaluation facility's work.

The evaluation's sponsor is responsible for delivering the supplies required for the evaluation. The list of supplies to be delivered is specified in the provisional work programme in the application form for evaluation.

Certain work must be carried out by the evaluation facility on the development, production or operation site of the product or system being evaluated. Agreements must be established between the sponsor, the developer and the evaluation facility for this work to be carried out. This work must be identified in the application form for evaluation for the evaluators to be authorised to access the sites when the time comes.

6.1.4. Evaluation Technical Report

The evaluation facility produces an Evaluation Technical Report (ETR) describing the work carried out and its results. It is sent to :

- to the certification body and the sponsor, in the framework of CC evaluations;
- only to the certification body, which gives its consent before transmission to the sponsor, in the framework of CSPN evaluations.

The ETR is transmitted for validation to the certifier in charge. When all tasks are completed and confirmed by the certification body, the evaluation is considered closed.

The ETR contains sensitive data covered by industrial and commercial secrecy. Its circulation is controlled: the confidentiality clauses dictated by ANSSI may eventually be definied in the contract between the ITSEF and the sponsor during the evaluation's preparation work.

Chapitre 7 Certification

7.1. Foreword

Certification is an overarching process that allows, through a suite of actions, to ensure that the evaluation was conducted with the required levels of competence and impartiality, in accordance with the corresponding procedures [CC-CER-P-01] et [CSPN-CER-P-01].

7.2. Certification report

After validation of the ETR, the certifier drafts a certification report that recommends whether certification should be granted. The certification report and associated security target are the only documents produced as part of the evaluation that a potential buyer would normally consult.

The certification report describes accurately the evaluated object and may recommend the implementation of measures judged necessary for a secure use.

The certification report constitutes, with the security target, the minimum documentation to be provided for international recognition of the certificate.

7.3. Certification decision

If the certification body decides to certify the assessed object, it forwards the draft certification report and certificate to the Director General of ANSSI or his deputy. The Director General of ANSSI or his deputy, who has been delegated to do so by the Prime Minister, signs the certificate and the certification report.

7.4. Storage rules

All electronic supplies and documents delivered by the sponsor and the ITSEF are systematically recorded and stored on the General Secretariat for Defence and National Security approved networks.

Original signed copied are stored by the certification in a secure location for a minimum of 10 years.

7.5. Publication of the certificate

The certificate, the certification report and its associated security target are published under certain conditions on ANSSI's website and other related ones.

Past their validity date, published documents on ANSSI's website are moved to an archive list. Unless the sponsor has undertaken a reassessment and therefore an extension of its certificate.

7.6. Satisfaction survey

At the end of the certification process, the sponsor or developer may fill in a satisfaction form sent by the certification body. This survey is designed to improve the certification body's activities.

7.7. Certificate withdrawal

The ANSSI certification body may suspend or even withdraw a certificate for various technical reasons (discovery of a vulnerability, etc.) or incomplete or even fraudulent communication cf. [CC-CER-P-01] and [CSPN-CER-P-01].

Chapitre 8 Use of the certificate and marks

The certification body established the regulations for using the certificate and the associated marks.

8.1. Communication rules

The sponsor and, where applicable, the developers, have a duty to provide accurate information to users of the certified product and ANSSI. Specifically:

- to provide the certification report and security target whenever a user request it. Copies must conform to the originals. Users can check with the body certification for verifying the accuracy of information;
- not to make misleading statements concerning the product, for example, by announcing or suggesting that the product is certified when it is only under evaluation;
- signal potential users of security issues of which the developer or sponsor is aware;
- immediately inform all registered users of new vulnerabilities.

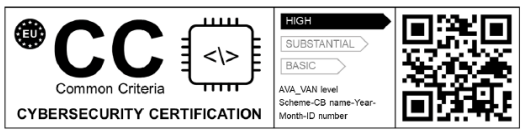
8.2. Rules for using the mark

The "Ti SÉCURITÉ CERTIFICATION" is the French collective, semi-figurative mark, composed of the logo integrating "Ti SÉCURITÉ CERTIFICATION".

It is reproduced below:

The "EUCC" mark is the European mark linked to the European implementing regulation (UE) 2024/482.

It is reproduced below:



The "CCRA" mark is used for testifying CCRA recognition agreement.

It is reproduced below:

The use of these 3 marks are defined in the [MAR-P-01] procedure.

CCRA and SOG-IS trademarks uses for international recognition are described in a specific procedure [MAR-P-02].

8.3. Mark surveillance

Marks surveillance rules are described in the [MAR-P-03] procedure.

8.4. Rules for the accreditation mark

As part of its accreditation (see chapter 4.3 *Accreditation scope*), and in accordance with [GEN-REF-11], the certification body affixes the certification mark to certificates and its certification report related to [EUCC] certifications.

This use complies with the rules set out in chapter 10 of [GEN-REF-11].

This use does not authorize developers or sponsors to use the accreditation mark.

Chapitre 9 Assurance continuity

The certificate attests, as of its signature date, to the conformity of a product or system with the requirements listed in its security target. To sustain confidence in this conformity and facilitate the further development of a previously certified product (reasssement), the certification body offers programs for maintenance or scope reduction measure.

9.1. Maintenance

A certificate applies only to the evaluated version and configuration. However it is possible that the product or its environment evolve in the future.

The sponsor may request feedback on the newest version of its product, in accordance with the [CC-MAI-P-01] and [CSPN-MAI-P-01] procedures. The maintenance report does not replace a reassessment which remains the only way to maintain product reliability over time.

9.2. Scope reduction of a CC certificate

During a certified product's life cycle, new attacks can appear that may impact the security of some of the product's features without affecting others.

To deal with this kind of situation, the classic approach recommended by ANSSI, consists of correcting the product in order to counter the exploited vulnerabilities for these new attacks. A reevaluation of the product is then necessary in order to verify that the modifications made are effective and are not impacting other product's security features.

However such an approach isn't always compatible with the CC evaluation sponsor's cost and time constraints. This application note proposes an approach to reduce the scope of a CC certificate allowing the edition of an update of the certificate at low cost and within a reduced timeline (see [CC-NOTE-25]).

Chapitre 10 Handling confidential information

10.1. Access to premises

The certification body's premises have the same security level that applies to the General Secretariat for Defence and National Security; it thus benefits from the heightened protection and security measures that apply to the latter.

10.2. Information confidentiality

All persons involved in the evaluation files are authorized or in the process of being authorized. They undertake to respect the information's confidentiality according to the evaluation scheme.

The certification body's staff handles with equal care of confidentiality all information related to a client.

In the case of judicial proceedings, the body certification is allowed to deliver confidential information without the client's consent. Whenever possible, the client will be informed.

10.3. Access to information

The information exchanged during the evaluation most often has a sensitive nature. For that reason, the certification body established protection rules when it comes to access and information using[3].

In the framework of the licensing, the certification body ensures that evaluation facilities apply similar information management rules.

The certification body's staff have access to all client's files. Other stakeholders may also have access to certain documents related to a published certificate or an ongoing evaluation. The said stakeholders are:

- ANSSI's technical experts who signed a confidentiality agreement;
- The "Qualification and Agreement" body's staff, if a product qualification request was made by the sponsor or developer;
- Line management involved in the reading and reviewing of ETR and certificates;
- General director of ANSSI (or his representative);

[3] Procedure ANSSI-CC-SECU-P-01 "Gestion de la confidentialité au centre de certification"

- Operator of Classified Interdepartmental Information Systems (OSIIC) to ensures the recording and saving documents.

10.4. Registration and storage time

All documents and supplies used during the assessment are recorded and stored with strict confidentiality requirements [SECU-P-01].

Chapitre 11 Irregularities, complaints

11.1. To the certification body

11.1.1. Recording and processing

The certification body keeps a record of certification anomalies in order to take necessary measures and to act on the cause and the precursory or predisposing factors[4] according to the [ANO-P-01] procedure .

11.1.2. Disputes

The executive certification committee investigates, with the objective of conciliation, any dispute submitted to it by the involved parties, regarding the evaluation scheme organized by decree 2002-535.

The control and supervision mission investigates, with the objective of conciliation, any dispute submitted to it by the involved parties, regarding the EUCC evaluation scheme.

11.2. To sponsors

For certified objects, the certification body requires that the sponsor advise it of any complaint brought to its attention regarding the conformity of the object with the requirements listed in its security target.

[4] Procedure ANSSI-CC-ANO-P-01 "Anomaly Processing"

Chapitre 12 Derogation clause

Should the certification body decide to deviate from the rules set out in its own quality system management, the latter may not take any derogatory measures without first assessing the risks incurred by such a decision, specially those related to impartiality. In this case, any risks will be recorded in the risk analysis.

Appendix A
Reference documents

Regulations

French amended decree No. 2002-535 of April 18th, 2002, related to the evaluation and certification of the security provided by information technology products and systems. Consolidated version 9 November 2019.	
French decree of April 1st, 2014 related to the signature delegation (General Secretary for Defence and National Security)	
EUCC	Common Criteria based European candidate cybersecurity certification scheme European certification scheme based on Common Criteria (Commission Implementing Regulation (EU) 2024/482) and its revisions, current version
CSA	European regulation on ENISA (European Union Agency for cybersecurity) and cybersecurity certification of information and communication technologies (implementing regulation (EU) 2019/881), current version

Decree No. 2009-834 of 7 July 2009 (official journal of 8 July 2009) related to the creation of French Cybersecurity Agency (ANSSI) as a national authority, consolidated version on the 1st july 2020
General Interdepartmental Instruction No. 1300/SGDSN/PSE/PSD of November 13, 2020 on the protection of national defense secrets

Texts on accreditation

EN ISO/IEC 17065	NF EN ISO/CEI 17065 standard: Conformity assessment — Requirements for bodies certifying products, processes and services.
CPS-Ref-02	Accreditation criteria for certification bodies operating products and services, revision 01, November 2002.
EN ISO/IEC 17025	NF EN ISO/CEI 17025 standard: General requirements for the competence of testing and calibration laboratories.
CERT-REF-04	Compendium of doctrinal notes.
CERT-CPS-REF-48	Specific requirements for the accreditation of organizations providing information and communications technology cybersecurity certification

Recognition agreements

CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, CCRA Management Committee.
SOG-IS	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOG-IS Management Committee.
BSZ_CSPN	Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed-time certification process, BSI/ANSSI.

Evaluation criteria

ITSEC	IT system security evaluation criteria (ITSEC)
ITSEM	Information technology security evaluation manual (ITSEM)
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CSPN	First Level Security Certification (CSPN)

References

[SECU-P-01]	Management of the confidentiality at certification body, ANSSI-CC-SECU-P-01, current version
[QUA-P-02]	Dispositif de préservation de l'impartialité, ANSSI-CCN-QUA-P-02, current version (only available in the French version)
[CC-CER-P-01]	Cybersecurity Certification based on the common criteria for products and protection profiles, ANSSI-CC-CER-P-01, current version
[CSPN-CER-P-01]	Certification de Sécurité de Premier Niveau, ANSSI-CSPN-CER-P-01, current version
[CSPN-CER-P-02]	Criteria for evaluation in view of a first level security certification, ANSSI-CCN- CSPN-CER-P-02, current version
[CC-AGR-P-01]	Licensing Of Evaluation facilities, ANSSI-CC-AGR-P-01,current version
[CSPN-AGR-P-01]	Licensing of evaluation facilities for the first level security certification, ANSSI-CSPN-AGR-P-01, current version
[DOC-P-01]	Elaboration et mise à jour de la documentation du système qualité du centre de certification, ANSSI-CSPN-AGR-P-01, current version (only available in the French version)
[MOD-P-01]	Modifying certification requirements, ANSSI-CC-MOD-P-01, current version
[QUA-P-01]	Management reviews, ANSSI-CC-QUA-P-01,current version
[ANO-P-01]	Anomaly processing, ANSSI-CC-ANO-P-01, current version
[MAR-P-01]	Use of the "ti sécurité certification" mark, ANSSI-CC-MAR-P-01, current version
[MAR-P-02]	Use of ccra and sogis logos, ANSSI- MAR-P-02, current version
[MAR-P-03]	Surveillances de marques des produits certifiés, current version (only available in the French version)
[PER-P-01]	Recrutement et qualification du personnel, ANSSI-CC-PER-P-01, current version (only available in the French version)
[CC-MAI-P-01]	Assurance continuity, ANSSI-CC-MAI-P-01, current version
[CSPN-MAI-P-01]	Maintenance of confidence: assurance continuity, ANSSI-CSPN-MAI-P-01, current version
[CC-NOTE-25]	Scope reduction of a cc certificate, ANSSI-CC-NOTE-25, current version
[CERT CPS REF 48]	Exigences spécifiques pour l'accréditation des organismes procédant à la certification de cybersécurité des technologies de l'information et des communications, curent version (only available in the French version)
[GEN-REF-11]	Règles générales pour la référence à l'accréditation et aux accords de reconnaissance internationaux

Appendix B
Definitions and Acronyms

Definitions

Certification body	ANSSI office established by decree 2001-693 and orders 15-02-2002-1 and 15-02-2002-2. Its staff members examine the certification files.
ITSEF	Organization accredited according to the ISO/IEC 17025 reference base and accredited by the certification body to conduct security evaluations for certification under amended decree 2002-535.
Certifier	Staff member of the certification body responsible for examining certification files.
Certificate	It certifies that the example of a product or system complies with the security requirements specified in its security target. It also certifies that the evaluation was carried out according to current rules and standards, with the required levels of competence and impartiality (article 8 of amended decree 2002-535).
Certification	The act of providing assurance of conformity to standards and other normative documents.
Sponsor	Person or organization requesting an evaluation with the objective of obtaining certification.
Executive certification committee	Executive certification committee for security certification of information technology, defined by Chapter III of amended decree 2002-535
Security target	Set of security requirements constituting the certification standard for ITSEC, Common Criteria and ISO/IEC 15408 evaluations.

Acronyms and Abbreviations

SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale (FR)	General Secretary for Defense and National Security (EN)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (FR)	French Cybersecurity Agency (EN)
SOG-IS	Senior Officer Group Information Security	
ETR	Evaluation Technical Report	

CC	Common Criteria	
CSPN	Certification de Sécurité de Premier Niveau (FR)	First Level Security Certification (EN)