

I. Scope

This Security Manual covers the independent assessment and certification of ICT products, services and processes by [CB Name/CB certification department], based at [CB Address], under **ISO/IEC 17065**.

The certification body performs conformity assessment activities for ICT products, processes and services under ISO/IEC 17065. Where applicable, management systems certification activities are conducted under ISO/IEC 17021-1 within the authorised scope.

II. Normative references, terms and definitions

Unless noted, all terms and definitions used in this manual and supporting documents are as given in current revisions of normative documents ISO/IEC 17000 — Conformity assessment — Vocabulary and general principles, and ISO/IEC 17065 — Conformity assessment — requirements for bodies certifying products, processes and services.

Note: Other normative references relating to specific EU schemes are covered in the relevant procedure document, see Annex A – Management system documentation.


Normative references include the following:

- ISO/IEC 17000:2020
- ISO/IEC 17065:2012
- Cybersecurity Act (EU) 2019/881
- Cyber Resilience Act (EU) 2024/2487
- EU Cybersecurity Certification Scheme on Common Criteria (EUCC)
- ISO/IEC 17021-1:2015 where applicable

III. Certification activities

[Introduction of the CB and its activities]

This Security Manual covers [CB Name] in its role as a Conformity Assessment Body (CAB) providing certification services for ICT products, services and processes under ISO/IEC 17065. The management system covered in this Security Manual is established as documented under VIII.

	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	2 of 16	

The policies defined in this Security Manual and the associated management system documentation are adopted to support EU certification schemes as follows.

Department	Accreditation standard	Scheme code	Scheme name
Certification	ISO/IEC 17065	###	EUCC Scheme
Certification	ISO/IEC 17065	###	CRA

IV. General requirements

1. Legal responsibility

[CB Legal Status]

2. Certification agreement

Upon acceptance of the quotation, clients enter into a contract agreement ([CA-01-01](#)) with the certification body. The contracts cover each location in the case of multi-site registrations. These contract agreements are adjusted to ensure that they are legally enforceable in the country of jurisdiction. The responsibilities of the certification body and the client are specified in the clauses contained in each contract.

3. Use of licences, certificates and marks of conformity

Control of the ownership, use and display of licences, certificates, marks of conformity and certification indicators, including the management of incorrect or misleading references, is governed by [MK-01-01](#) (see ISO/IEC 17030:2021 for guidance).

4. Management of impartiality

The certification body's top management has published a statement of commitment on the importance of impartiality in conducting its activities on the [CB Name] website.

5. Commercial, financial or other pressures to compromise impartiality

[mechanism to ensure commercial, financial or other pressures DOES NOT compromise impartiality].

6. Process to identify and mitigate risks to impartiality

The process to identify and mitigate risks to impartiality is documented under [IMP-01-01](#). This process includes risks that arise from its activities, from its relationships, or from the relationships of its personnel. A relationship presenting a risk to impartiality of the certification body can be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing (including branding), and payment of a sales commission or other inducement for the referral of new clients.

7. Liability and financing

[Insurance cover details]

[financial probity reviews process]

8. Non-discriminatory conditions

The certification body's services are available to all applicants whose activities fall within the scope of its operations. Access to certification services is not conditional upon the size of the client or membership of any association or group, nor is certification conditional upon the number of certifications already issued. There shall be no undue financial or other conditions.

The certification body may decline to accept an application for certification, or to maintain a certification agreement, where there is fundamental or demonstrated reasons to do so, such as the client participating in illegal activities, having a history of repeated non-compliance with certification or product requirements, or similar client-related issues.

The certification body confines its requirements, evaluation, review, decision and surveillance (if any) to those matters specifically related to the scope of certification.

9. Confidentiality

The certification body has legally enforceable agreements with all staff, contract staff and outsourced suppliers regarding confidentiality. Procedures cover IT security and file security. All premises are protected. Access is restricted to authorised persons, including staff and accompanied visitors.

All information pertaining to a client (other than information the client makes publicly available or when agreed between the client and the certification body) is considered proprietary information and is regarded as confidential. The certification body informs clients in advance of the information it intends to place in the public domain, such as registered company status.


If the certification body is obliged by law or authorised by contractual arrangements (such as with the accreditation body) to release confidential information, the organisation will, unless prohibited by law, be notified of the information provided. The process for safeguarding client confidential records is documented under [CONF-01-01](#).

10. Publicly available information

The certification body makes the following information available through the ENISA website:

- Information about and reference to its certification schemes, including processes for granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification.
- Annual reports which outline the means by which the certification body obtains financial support and general information on the fees charged to applicants' clients.
- The use of the certification body's name and certification mark or logo or certificate number.
- Processes for handling requests for information, complaints and appeals.

A description of the rights and duties of applicants and clients are documented under the certification agreement ([CA-01-01](#)).

	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	5 of 16	

V. Structural requirements

1. Organisation structure and top management

[organisational structure and chart]

2. Mechanism for safeguarding impartiality

Mechanisms for safeguarding impartiality are documented under [IMP-01-01](#).

VI. Resource requirements

1. Certification body personnel

The certification body employs or contracts personnel to cover its operations related to the certification of ICT products, processes and services. Personnel are evaluated against specified criteria for the functions they are engaged to perform. All personnel are informed and aware that all information obtained or created during the performance of product certification activities shall be kept confidential, except as required by law or by the product certification scheme.

2. Management of competence

The competence evaluation procedure is documented under [RES-01-01](#). This procedure is aligned with the ENISA State of The Art documents and the Guidelines of ENISA.

3. Contract with personnel

All personnel involved in certification activities operating under this management system are required to sign a contract with the certification body, committing to:

- Comply with the rules defined by the certification body including those relating to confidentiality and independence from commercial and other interests.

- Declare any prior and/or present association on their part or the part of their employees with a supplier/designer of products, a provider/developer of services or an operator/developer of processes.
- Reveal any situation known to them that may present a conflict of interest.

This information is used as input into identifying risks to impartiality as documented under [IMP-01-01](#).

4. Resource evaluation

The process for selecting, training and formally authorising auditors, and for selecting technical experts (where necessary) used under this management system, is documented under [RES-01-01](#), describing how the competencies of personnel are evaluated initially and on an ongoing basis.

All external resources used by the certification body for the purpose of providing certification services are engaged through a signed contract agreement which addresses confidentiality and impartiality.

For all outsourced activities, the certification body:

- Takes full responsibility for the outsourced activities;
- Ensures that the outsourced body and the individuals that it uses are not involved in such a way that the credibility of their results could be compromised;
- Has documented how bodies providing outsourced activities are qualified, assessed and monitored;
- Maintains a list of approved providers of outsourced services;
- Implements corrective actions for any breaches of contract for which they become aware;
- Informs the client in advance of outsourcing activities in order to provide the client with an opportunity to object.

Decisions for granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification are never outsourced.

VII. Process requirements

Scheme-specific procedures are listed in Annex A – Management system documentation.

1. Application and Application review

Enquiries, Applications and Contract Review procedure (SM-01-02) describes the application and application review process, including the contract review process.

2. Evaluation (where applicable)

Evaluation activities are outsourced to the ITSEFs as documented under SM-01-03a for EUCC and SM-01-03b for the CRA.

3. Review

The technical review process is documented under SM-01-03a and SM-01-03b.

4. Certification decision


The certification decision-making process is documented in SM-01-03a and SM-01-03b. Certification decisions are taken by personnel who are independent of the evaluation or assessment activities.

5. Certification documentation

Following successful completion of an assessment, the client will be issued a certificate which clearly states the following:

- The name and address of the certification body;
- The date certification is granted, which will not precede the date on which the certification decision was completed;
- The client's name and address;
- The scope of certification;
- The expiry date of the certification;
- Any other information required by the product certification scheme. Certificate templates are documented under [SM-01-04](#).

The certificate includes the signature of the Head of Department, or authorised delegate acting on their behalf. Certificates are only issued after a decision to grant or extend the scope of certification has been made, the certification requirements have been fulfilled,

	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	8 of 16	

and the certification agreement has been completed or signed by both the certification body and the applicant/certificate holder.

6. Directory of certified products/processes/services

The certification body makes information on issued certifications available through the ENISA repository for EU certificates, accessible here [-link-](#).

The repository provides the following:

- Identification of the product;
- The standard(s) and other normative document(s) to which conformity has been certified;
- Identification of the client;
- The validity of the certification.

7. Surveillance

Surveillance procedures are documented under SM-01-03a for EUCC and SM-01-03b for CRA.

8. Changes affecting certification

When the certification scheme introduces new or revised requirements that affect the client, the certification body shall ensure these changes are communicated to all clients. The certification body shall verify the implementation of the changes by its clients and shall take any actions required by the scheme. The procedure for the review of changes affecting certification of ICT products is documented under SM-01-03a and SM-01-03b.

Changes initiated by the client include, but are not limited to, vulnerability handling of certified products, updates to products, new releases and others. The process specific to vulnerability handling of certified products is documented under VH-01-01a for EUCC and VH-01-02b for CRA.

9. Termination, reduction, suspension/withdrawal of certification

The certification body will determine the appropriate course of action in response to nonconformity with the certification scheme requirements arising from surveillance



activities or changes affecting certification, e.g. vulnerability handling. These actions may include:

- Continued certification subject to conditions, e.g. Increased surveillance, further evaluation and additional certification review
- Reduction of the certification scope to exclude nonconforming product variants
- Suspension of certification pending remedial action by the client
- Withdrawal of certification

Certification may also be terminated at the client's request.

If certification is withdrawn or terminated, the certification body must modify certification documents, public information and authorisations for the use of marks and logos, etc., to ensure that the withdrawal or termination of certification is clearly reflected and that there is no indication that the product remains certified.

If a scope of certification is reduced, the certification body must make all necessary modifications to formal certification documents, public information and authorisations for the use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.

If certification is suspended, the [person assigned to this role by the CB] must formulate and communicate the following to the client:

- Actions needed to end suspension and restore certification for the product(s) in accordance with the certification scheme;
- Any other actions required by the certification scheme.

If certification is reinstated after suspension, the certification body must make all necessary modifications to formal certification documents, public information and authorisations for the use of marks, etc., in order to ensure that all appropriate indications show that the product continues to be certified.

If a decision to reduce the scope of certification is made as a condition of reinstatement, the certification body must make all necessary modifications to formal certification documents, public information and authorisations for the use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.

Scheme-specific requirements for termination, reduction, suspension and withdrawal of certification are documented under SM-01-03a and SM-01-03b.

10. Records

The certification body maintains records on assessments and other certification activities for all clients, including all organisations that submitted applications, and all organisations audited, certified, or with certification suspended or withdrawn. These records are securely maintained to ensure that the information is kept confidential in accordance with [CONF-01-01](#). Client records are stored electronically for not less than 10 years.

11. Complaints and appeals

A complaint is an expression of dissatisfaction relating to:

- The conduct of the certification body,
- The certification process,
- Interactions with the certification body or its personnel,

A complaint may be made by:

- A certification applicant,
- A certificate holder,
- A laboratory,
- Any other interested party.

An appeal is a formal request by a certification applicant or certificate holder for reconsideration of a certification decision taken by the certification body, including:

- Refusal to certify,
- Conditional certification,
- Suspension,
- Withdrawal,
- Non-renewal.

For the avoidance of doubt, this complaints process addresses dissatisfaction with the **certification body's own certification activities** (e.g. conduct, communication and process execution) and does **not** constitute a mechanism to challenge or change a certification decision. Only an **appeal** submitted by a certification applicant or certificate holder can trigger a formal reconsideration of a certification decision. Accordingly, the certification body will process complaints to ensure impartiality, independence and traceability, but a complaint alone does not alter the certification outcome.

Upon receipt, the certification body must acknowledge a written complaint or appeal submitted through its publicly available channels. The certification body conducts an initial triage to confirm whether the matter relates to its certification activities and therefore falls within the scope of this procedure. Where a submission primarily concerns **product non-compliance on the market, regulatory enforcement**, or other matters under the remit of a **Market Surveillance Authority (MSA)**, the certification body will inform the submitter that such matters are handled by the competent authority and, where practicable, provide the relevant contact route.

For complaints and appeals confirmed to be within scope, the certification body must appoint a competent person who is independent of the activities concerned to investigate the matter and make evidence-based determinations. The outcome and supporting records must be documented in the certification body's systems, and the complainant or appellant must be notified of the result. This process does not replace, limit or pre-empt any separate investigation, corrective action request or enforcement activity carried out by an MSA; however, the certification body will cooperate with competent authorities where required by law or by the applicable scheme.


Complaints or reports intended for, or arising from, **market surveillance** (e.g. alleged regulatory non-compliance of products placed on the market) are handled by the competent MSA and are outside the scope of the certification body's internal complaints and appeals procedure, except where the matter also relates directly to the certification body's conduct or a certification decision.

Scheme-specific requirements for complaints and appeals are documented under SM-01-03a and SM-01-03b.

VIII. Management system requirements

The certification body has established, documented and maintains a management system to fulfil the requirements of ISO/IEC 17065 and the schemes for cybersecurity certification of ICT products, processes and services. The vision, mission and values of the certification body are available under ~~##-##-##~~.

The Heads of Department have been appointed with responsibilities and authority that include ensuring that the processes and procedures needed for the management system in their respective areas are established, implemented and maintained, and reporting to top management on the performance of the management system and any need for

	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	12 of 16	

improvement (see Annex B – Organisation chart and scheme specific roles and responsibilities).

All relevant documentation, processes and records are controlled and referenced within the system as documented in this Security Manual.

All personnel involved in product certification activities have access to the management system documentation and related information applicable to their responsibilities.

The management system documentation is detailed under Annex A – Management system documentation.

1. Control of documents and records

Procedures addressing the control of documents and records are documented under [SM-01-04](#).

2. Management review

Management review is conducted annually as per [SM-01-05](#).

3. Internal audit

Procedures for conducting internal audits are documented under [SM-01-06](#).

4. Preventive and corrective actions

Procedures for the management of preventive and corrective actions are documented under [SM-01-07](#).

5. Review and continuous improvement

The relevance of the management system documentation will be reviewed:


- At management review meetings,
- Upon changes in schemes, legislation or regulations,
- Upon publication of relevant guidance by ENISA, where applicable

The certification body may define and monitor key performance indicators (KPIs) to support management review, evaluate process effectiveness and identify opportunities for continual improvement.

Annexes

Annex A – Management system documentation

Document Name	Description
CA-01-01	Contract agreement
MK-01-01	Use of licences, certificates and marks of conformity
IMP-01-01	Impartiality
CONF-01-01	Confidentiality
RES-01-01	Management of competence and resources
SM-01-01	Security Manual (this document)
SM-01-02	Enquiries, Applications and Contract Review
SM-01-03a	Assessment process for EUCC
SM-01-03b	Assessment process for CRA
VH-01-01a	Vulnerability Handling for EUCC
VH-01-02b	Vulnerability Handling for CRA
SM-01-04	Control of documents and records
SM-01-05	Management review
SM-01-06	Internal audit
SM-01-07	Management of preventive and corrective actions

	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	14 of 16

Annex B – Organisation chart and scheme specific roles and responsibilities

[organisation specific]

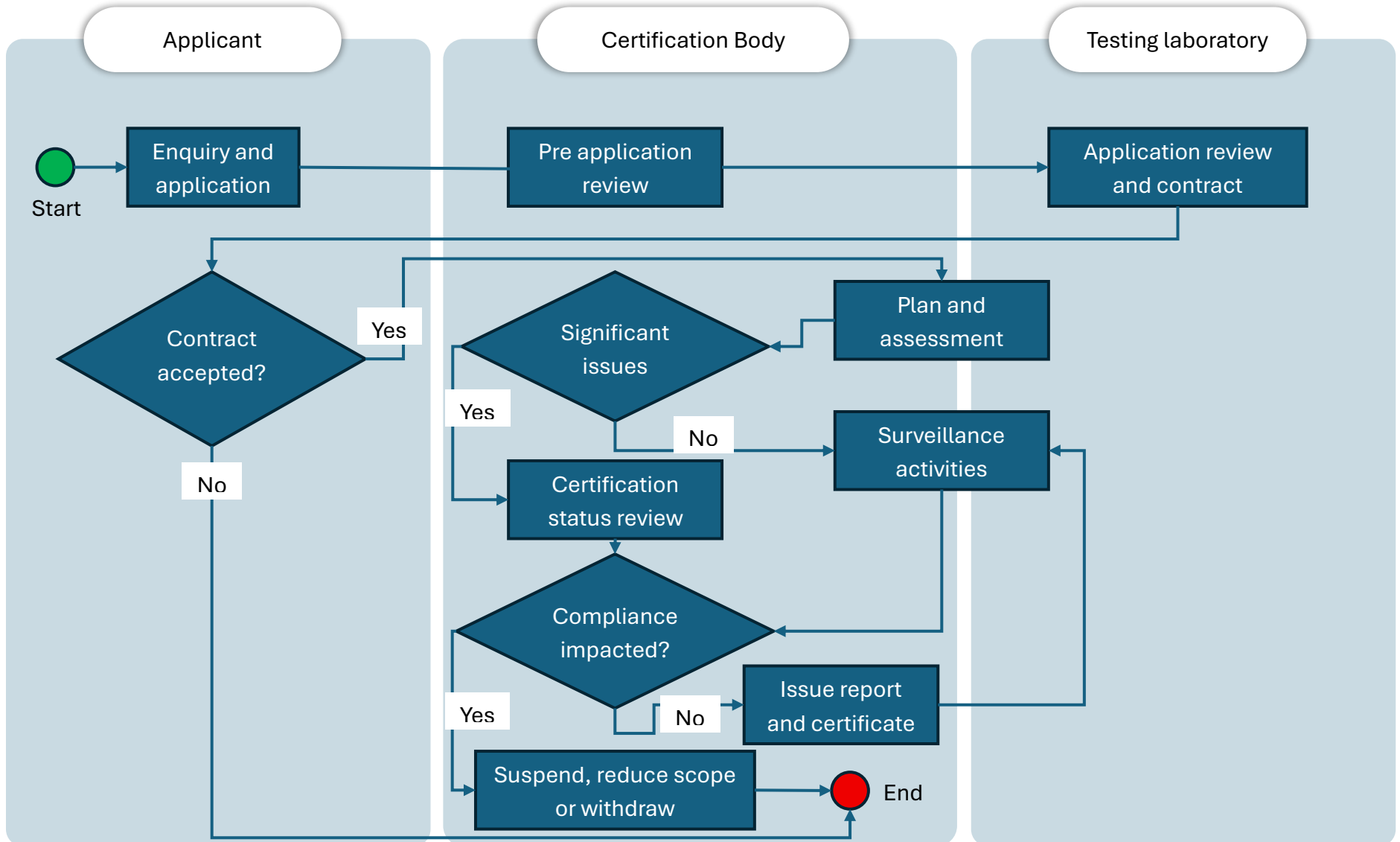





Certification Security Manual

Document:	TB-SM-01-01
Revision:	2.0
Date issued:	DD-MM-YYYY
Owner:	To be determined
Page:	15 of 16

Annex C – Process flow



	<h1>Certification Security Manual</h1>	Document:	TB-SM-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	16 of 16

Version History

Version	Date	Author	Summary of changes	Status
1	10-03-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	28-05-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments	Approved

