	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by:	Version 1.3 – 29.4.2025	Page 1 of 9


# **ILNAS/ANCC/Pr002**

## **Management of Complaints**

Modifications: periodic review


1, avenue du Swing  
L-4367 Belvaux  
Tél.: (+352) 247 743 55

[confiance-numerique@ilnas.etat.lu](mailto:confiance-numerique@ilnas.etat.lu)  
<https://portail-qualite.public.lu>

	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 2 of 9


## Contents

I	Abbreviations .....	3
II	References .....	4
1	Introduction .....	5
1.1	Overview .....	5
1.2	Purpose and scope .....	5
1.3	Terms and definitions .....	5
2	Description of the procedure .....	6
2.1	Foundations .....	6
2.2	Procedure - overview .....	6
2.3	Description .....	7
3	Costs .....	9

	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 3 of 9


## I Abbreviations

ANCC	National Cybersecurity Certification Authority (French: Autorité nationale de certification de cybersécurité)
CAB	Conformity Assessment Body
CB	Certification Body
Commission	European Commission
CSA	CyberSecurity Act
ENISA	The European Union Agency for Cybersecurity
ICT	Information and communication technologies
ILNAS	Luxembourg Institute for standardisation, accreditation, safety, and quality of goods and services (French: Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services)
ITSEF	IT Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
OLCN	Luxembourg Digital Trust Body (French : Organisme Luxembourgeois de la Confiance Numérique)

	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 4 of 9

## II References

- [1] Loi du 4 juillet 2014 portant réorganisation de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services et portant organisation du cadre général pour la surveillance du marché dans le contexte de la commercialisation des produits (hereinafter 'ILNAS law')
- [2] 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 (hereinafter 'Cybersecurity act')
- [3] Loi du 20 décembre 2024 portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS (hereinafter 'National CyberSecurity law')

	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 5 of 9

# 1 Introduction

## 1.1 Overview

ILNAS is placed under the administrative supervision of the Ministry of the Economy of the Grand Duchy of Luxembourg. The legal missions of ILNAS are defined in the ILNAS law [1]. In this context, ILNAS is in charge of carrying out supervision tasks within the meaning of Article 58 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification of information and communications technologies, and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation) and responsible for certification tasks within the meaning of Article 56(6) of the aforementioned Regulation (EU) No 2019/881.

ILNAS has been designated as the NCCA for the Grand Duchy of Luxembourg according to Article 58 of the Cybersecurity Act **Error! Reference source not found.** that is responsible for supervision tasks and certification tasks as defined in the National Cybersecurity law [3][3]. The OLCN has been created for carrying out these supervision and certification tasks. The unit supervises the compliance of manufacturers and providers of ICT products, ICT services, ICT processes, and managed security services and of conformity assessment bodies that are established in the Grand Duchy of Luxembourg.

In the following, we use the acronym NCCA to refer to the OLCN.

## 1.2 Purpose and scope

The purpose of this document is to describe the national supervision scheme of certificate holders, issuers of EU statements of conformity and CABs that are involved in certification activities in the context of the CSA. The scope of the supervision includes conformity assessment activities at the assurance levels “basic”, “substantial” and “high”. The supervision scheme is based upon the rules laid down in the CSA, and it is updated to meet the requirements of European cybersecurity certification schemes (hereinafter, “certification schemes”), associated implementing acts, and the national law, at planned intervals or whenever changes impacting the legal framework require the supervision scheme to be updated.

This document primarily addresses the staff of the NCCA and all the parties involved in the supervision scheme. This document is also intended for anyone that wants to understand the national supervision scheme relating to the CSA.

This procedure will be subject to a peer review, according to Article 59 of the CSA.

## 1.3 Terms and definitions

In this document, the terms and definitions provided in the Cybersecurity Act, its implementing regulations (in particular European cybersecurity certification schemes) and other documentation publicly available on the website of ILNAS apply.

## 2 Description of the procedure

### 2.1 Foundations

The procedure for handling complaints has been defined around the following aspects:

- How complaints from natural and legal persons are handled by the NCCA internally
- Investigation of the complaint to the appropriate extent
- Informing the involved parties of the progress and the outcome of the investigation

### 2.2 Procedure - overview

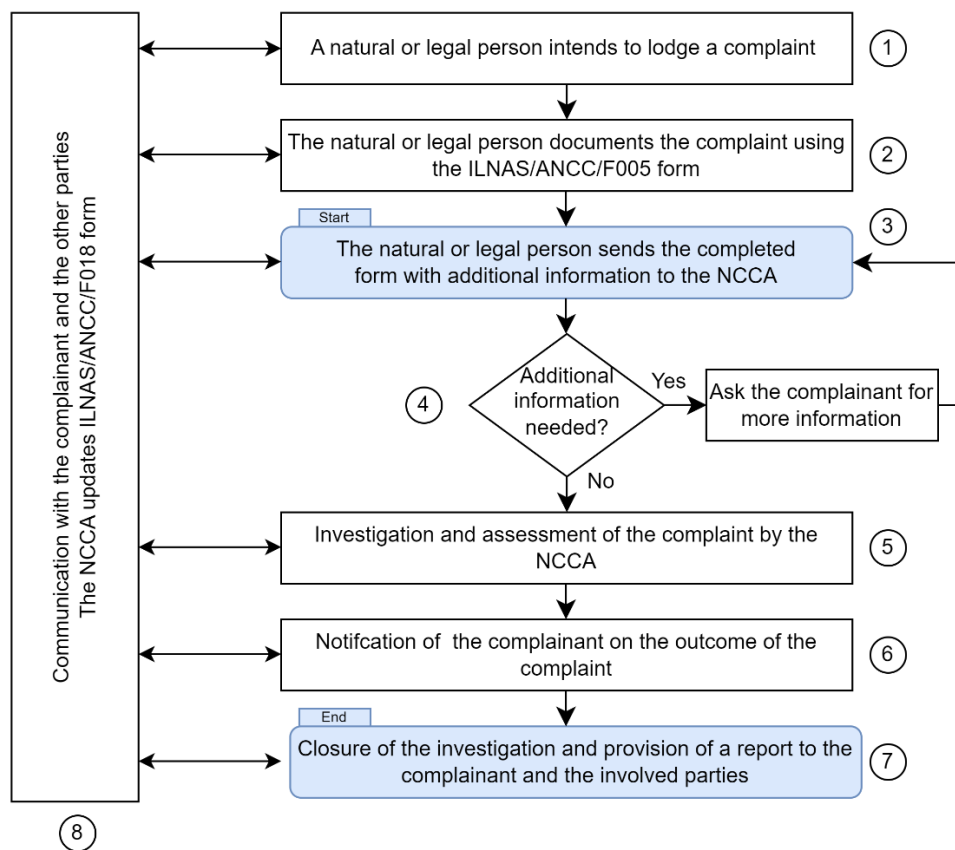


Figure 1 below illustrates the procedure that is followed by the NCCA for handling complaints received by natural and legal persons.

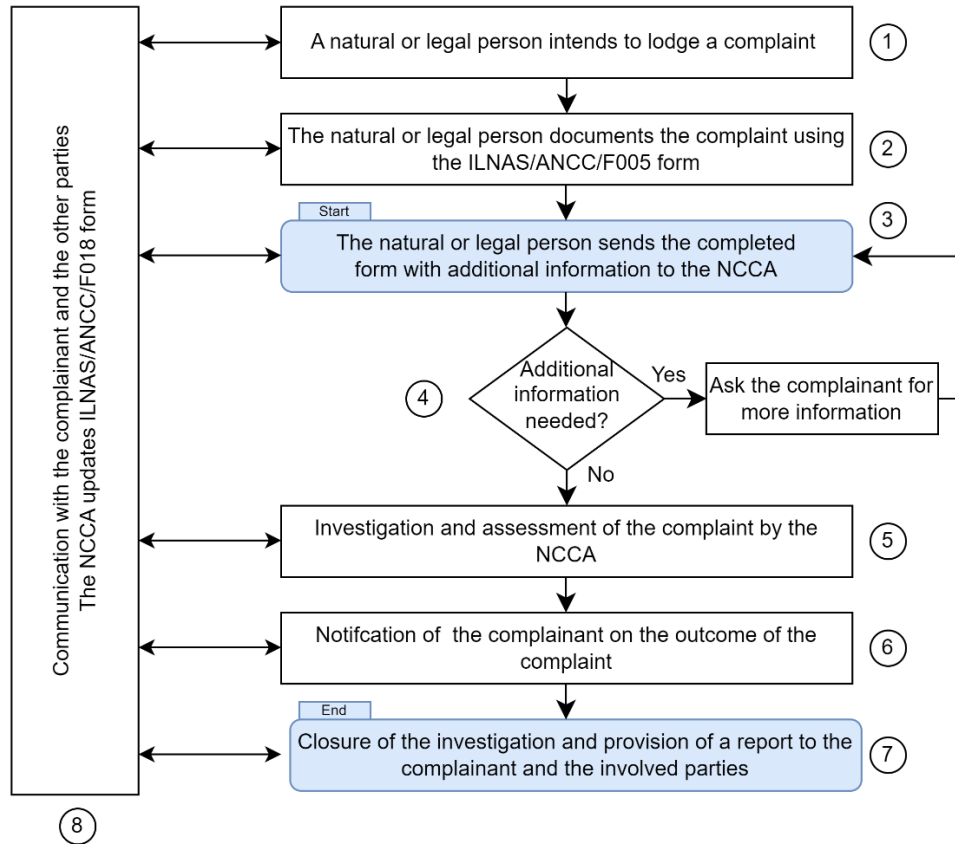



Figure 1: Procedure for handling and managing complaints

## 2.3 Description

- 1) A natural or legal person intends to lodge a complaint concerning activities that fall within the context of the Cybersecurity Act and related European cybersecurity certification schemes
- 2) The natural or legal person documents the complaint using the ILNAS/ANCC/F005 form
  - The ILNAS/ANCC/F005 form should be used to address complaints to the NCCA. Complaints communicated via other means, such as phone or email are also receivable. However, the NCCA will subsequently request the complainant to use this form in order to provide all the necessary information.
  - If necessary, the submitted form may be sent to other public authorities. If this is the case, the NCCA will inform the complainant and the involved parties beforehand.
- 3) The natural or legal person sends the completed form, together with additional documents, if any, to the NCCA (*start of the procedure*)

	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 8 of 9

- At this step, the internal procedure of the NCCA for handling and managing complaints will start.
- The form must be duly completed, dated and signed.
- The form can be sent electronically by email or mailed to the postal address indicated on the form.
- The NCCA will acknowledge the receipt of the form to the sender as soon as possible.

4) If necessary, the NCCA may request further information from the complainant, e.g.,

- when the submitted form was not filled in completely, or
- for deepening the analyses and investigations,
- for additional clarifications.

A first analysis of the complaint is performed at this step.

5) Investigation and assessment of the complaint by the NCCA

- The NCCA will consider the following aspects during its investigation:
  - *the nature of the complaint*
  - *the type of ICT products, ICT services, ICT processes and managed security services*
  - *the parties involved*
  - *the severity of the complaint, its impact and associated risks*
  - *the root cause of the complaint*
- The management of ILNAS will be informed, depending on the nature of the complaint.
- Other public or law enforcement authorities may be notified (e.g., in case of security incidents, issues concerning data protection, etc.).
- ENISA, the European Commission and national authorities from other Member states may be notified as well.
- The duration of the investigation and assessment depends on the nature, severity and scope of the complaint.


6) Notification of the complainant and the other involved parties regarding the outcome of the complaint

- When a possible resolution of the complaint has been found, the NCCA will notify the complainant of the outcome.
- The NCCA will contact the complainant by phone or by e-mail.

7) Closure of the investigation and provision of a report to the complainant and the involved parties (*end of the procedure*)

- The NCCA will prepare a report on the investigation and the overall assessment of the complaint.
- The NCCA will make the report available to the complainant and all the involved parties.
- Each party may request further information from the NCCA regarding the content of the report.
- The investigation will be formally closed.



	<b>Digital Trust Process</b>	
	<b>ILNAS/ANCC/Pr002</b>	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 9 of 9

8) Communication with the complainant and the involved parties

- The NCCA will provide feedback to the complainant and the other involved parties at each step of the procedure.
- The aim is to ensure transparency and trust towards everyone involved in the procedure.
- The NCCA fills in the internal ILNAS/ANCC/F018 form to record key events related to complaints.

### 3 Costs

According to article 7 (7) and (8) from the National CyberSecurity law [3], the detailed costs are available in the ILNAS/ANCC/A003 form.