	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by:	Version 1.3 – 29.4.2025	Page 1 of 11


ILNAS/ANCC/Pr003

Notification and Management of Vulnerabilities

Modifications: periodic review


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

confiance-numerique@ilnas.etat.lu
<https://portail-qualite.public.lu>

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 2 of 11


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	Vulnerability notification procedure.....	6
3	Vulnerability management procedure.....	8
4	Costs.....	11

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 3 of 11


I Abbreviations

ANCC	National Cybersecurity Certification Authority (French: Autorité nationale de certification de cybersécurité)
CAB	Conformity Assessment Body
CB	Certification Body
CERT	Computer Emergency Response Team
CIRCL	Computer Incident Response Center Luxembourg
CNPD	Commission Nationale pour la Protection des Données
Commission	European Commission
CSA	CyberSecurity Act
ENISA	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
GOVCERT	GOVERNMENTAL CERT
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)
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commission
ITSEF	IT Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
OLCN	Luxembourg Digital Trust Body (French : Organisme Luxembourgeois de la Confiance Numérique)

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 4 of 11

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')
- [4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 5 of 11

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.

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 6 of 11

2 Vulnerability notification procedure

The vulnerability notification procedure describes the steps to be taken

- 1) by a holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services, and
- 2) by the body that issued the certificate (the CB or the NCCA-CAB) and, if applicable, its ITSEF, and
- 3) by the NCCA (ILNAS)

when the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services has detected a vulnerability or an irregularity that may cause a non-compliance against applicable requirements.

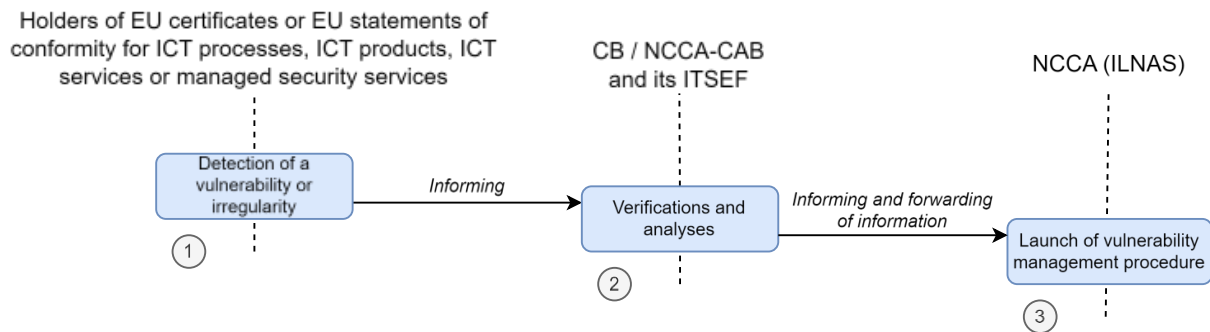


Figure 1: Vulnerability notification procedure

The procedure illustrated in Figure 1 above is based on the dispositions of Article 56 (8) of the Cybersecurity Act and it can be adapted to the requirements of European cybersecurity certification schemes.

1) **Detection of a vulnerability or irregularity**


The holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services detects a vulnerability or any kind of irregularity that might cause a non-compliance to its certified or self-assessed ICT product, ICT service or ICT process or managed security service.

The holder of EU certificates for ICT processes, ICT products, ICT services or managed security services shall inform without undue delay (not later than 72 hours of becoming aware of a vulnerability or irregularity) the body that issued its certificate (CB or NCCA-CAB) and transmit relevant information.

2) **Verifications and analysis**

The CB or the NCCA-CAB and, if applicable, its ITSEF review, verify and analyse the received information. The CB or the NCCA-CAB and, if applicable, its ITSEF shall enforce the applicable requirements.

The CB or the NCCA-CAB and, if applicable, its ITSEF shall inform the NCCA (ILNAS) without undue delay (not later than 72 hours of becoming aware of a vulnerability or irregularity) and shall forward all information on the related case.

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 7 of 11

3) Launch of vulnerability management procedure

As soon as the NCCA is informed about the vulnerability of irregularity by the CB or the NCCA-CAB and, if applicable, its ITSEF, its internal vulnerability management procedure will be launched, which is described in the following section.

3 Vulnerability management procedure

The vulnerability management procedure is used by the NCCA to manage and handle vulnerabilities that have been notified to them. The process is illustrated in Figure 2 below.

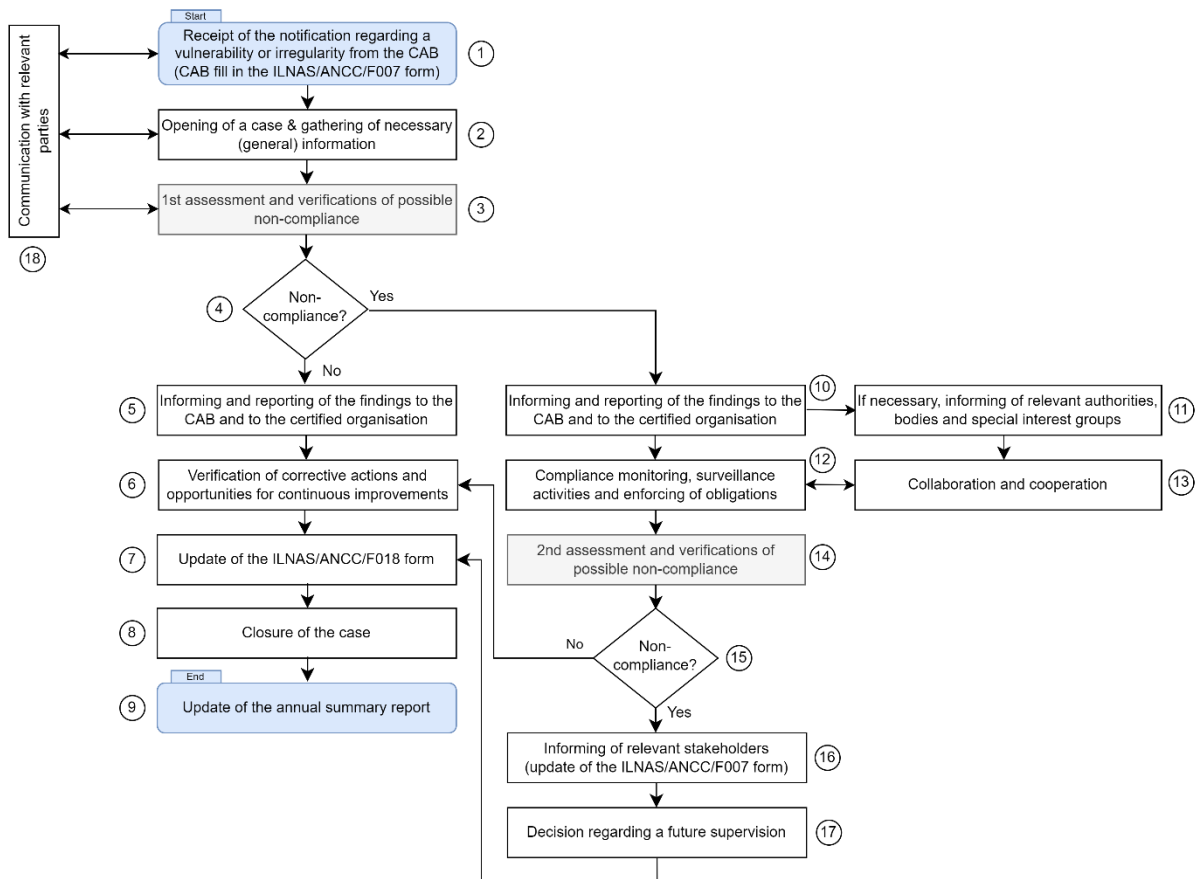



Figure 2: Vulnerability management process

1) Receipt of the notification regarding a vulnerability or irregularity from the CAB

The CAB shall use the ILNAS/ANCC/F007 form to notify the NCCA of any vulnerability or irregularity.

- The NCCA is informed by the CAB on a vulnerability or irregularity detected by the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services, or managed security services;
- The NCCA is also provided with all the relevant information that was initially submitted to the CAB by the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services;
- The NCCA acknowledges the receipt of the notification.

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 9 of 11

An **irregularity** refers to an event that significantly affects the confidentiality, integrity, availability or authenticity of the certified ICT product, ICT service, ICT process, or managed security service. The following aspects might be considered:

- Change management activities causing disruptions to the ICT product, ICT service, ICT process or managed security service, e.g. maintenance activities, migrations of the IT infrastructure, etc.;
- Critical incidents, causing e.g. a data breach or a loss of sensitive information;
- A change in the threat environment;
- Potential business disruptive events, such as the loss of key employees.

2) Opening of a case & gathering of necessary (general) information

Upon receipt of the notification, the NCCA will open a case, which will be used to record all the necessary information regarding the vulnerability or irregularity that has been notified. The NCCA will additionally gather all the necessary information that identifies the concerned organisation.

3) 1st assessment and verifications of possible non-compliance

The NCCA proceeds with a 1st assessment of the notified event with the main objective of verifying whether a non-compliance related to the requirements of the Cybersecurity Act and the related European cybersecurity certification schemes' implementing regulations has occurred or not. The NCCA then prepares a report containing its analysis, findings and results.

4) Compliance or non-compliance

Based on its findings and assessment, the NCCA decides on the further actions.

Compliance

5) Informing and reporting of the findings to the CAB and to the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services


The NCCA sends its report to the CB or the NCCA-CAB and, if applicable, its ITSEF, and to the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services. In this report, the NCCA explains the next steps to be taken by each party.

6) Verification of corrective actions and opportunities for continuous improvement

The NCCA verifies the corrective actions determined and planned by the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services in order to mitigate the risks related to the identified vulnerability or to eliminate the detected irregularities.

Also, when an irregularity was detected that concerns the CAB, the NCCA verifies the corrective actions proposed by the CAB.

7) Update of the ILNAS/ANCC/F018 form

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 10 of 11

The NCCA updates the ILNAS/ANCC/F018 form dedicated to the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services, or the CAB. Each important event is recorded in this form.

8) Closure of the case

The NCCA closes the case and it informs the CAB and the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services.

9) Update of the annual summary report

The NCCA updates its annual summary report with a summary of the case.

Non-compliance

10) Informing and reporting of the findings to the CAB and to the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services (similar to point 5)

The NCCA sends its report to the CAB and to the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services. In the report, the NCCA explains its findings, focusing on the elements that cause the non-compliance of the certified ICT service, ICT product, ICT process or managed security service.

11) If necessary, informing of relevant authorities, bodies and special interest groups

If a non-compliance has been found, then, depending on the situation, the NCCA has the obligation to inform other interested parties, such as:


- Relevant authorities (e.g. law enforcement, data protection, market surveillance);
- Other relevant bodies (e.g. national accreditation bodies, the European Commission, ENISA, the Ministry of the economy, etc.);
- Special interest groups (e.g. CIRCL, Luxembourg House of Cybersecurity, GOVCERT, etc.).

12) Compliance monitoring, surveillance activities and enforcing of obligations

The NCCA supervises and follows the actions of the certified holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services and the NCCA-CAB or CAB. The NCCA enforces the rules of the Cybersecurity Act and related certification schemes.

13) Collaboration and cooperation

During the monitoring of compliance, surveillance activities and enforcement of obligations, the NCCA collaborates, cooperates and exchanges relevant information

	Digital Trust Process	
	ILNAS/ANCC/Pr003	
Approved by: Alain Wahl	Version 1.3 – 29.4.2025	Page 11 of 11

with all the identified interested parties according to step 11. Legislation relating to data protection, in particular GDPR [4], is also considered.

14) 2nd assessment and verifications of possible non-compliance

At the given time specified in European cybersecurity certification schemes or in other legislative acts, the NCCA will proceed to a 2nd assessment and verification concerning the non-compliance detected during the 1st assessment. The aim of the 2nd assessment is to determine whether the non-compliance has been addressed. The NCCA describes its findings in the related report.

15) Non-compliance

Upon finalising its findings, the NCCA determines whether the non-compliance has been treated appropriately, or not.

If the NCCA concludes that there are no further non-compliances, it will progress to step 7 of the procedure.

16) Informing of relevant stakeholders

If the NCCA concludes that the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services is still non-compliant, it will contact and inform relevant stakeholders, which can include:

- ENISA;
- European Commission;
- NCCAs from other member states;
- National accreditation bodies;

(only for public interest) National journal of the Grand Duchy of Luxembourg or in one or more Luxembourg or foreign newspapers.

The aim of this step is to gather as much information as possible for the next step of the procedure.

The NCCA updates the ILNAS/ANCC/F007 form and transmits the information to the relevant stakeholders.

17) Decision regarding a future supervision

Based on the steps 14 and 16, the NCCA will decide whether the holder of EU certificates or EU statements of conformity for ICT processes, ICT products, ICT services or managed security services will remain under supervision. Each involved party will be formally notified about the decision. Subsequently, the NCCA will continue with step 7.

18) Communication with relevant parties

The NCCA continuously communicates with all the involved parties at the beginning of the procedure, in particular from steps 1 to 3. Nevertheless, extensive communication continues to take place throughout the whole procedure.

4 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.