

SURVEILLANCE
DU MARCHÉ

ACCREDITATION

CONFIANCE
NUMÉRIQUE

MÉTROLOGIE

NORMALISATION

ILNAS

Welcome
Bienvenue
Willkommen

The Cybersecurity Act and the role of ILNAS

06/10/2022, Belval

Jean Lancrenon

Chargé de mission – *Département Confiance Numérique, ILNAS*

10/10/2022



Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[Here](#)

Adopted on 17 April 2019

Fully entered into force on 28 June 2021

Two major parts



Main objectives: Increase cybersecurity in the Union and support the digital single market

Status, governance, structure

ENISA's mandate as the European cybersecurity agency is made permanent

Chapters 3 to 6 give its broad organization

Scope, objectives

Cybersecurity

Knowledge center

Support to Member States, the Union

Research

Capacity building, education

Improving the EU's general cybersecurity level



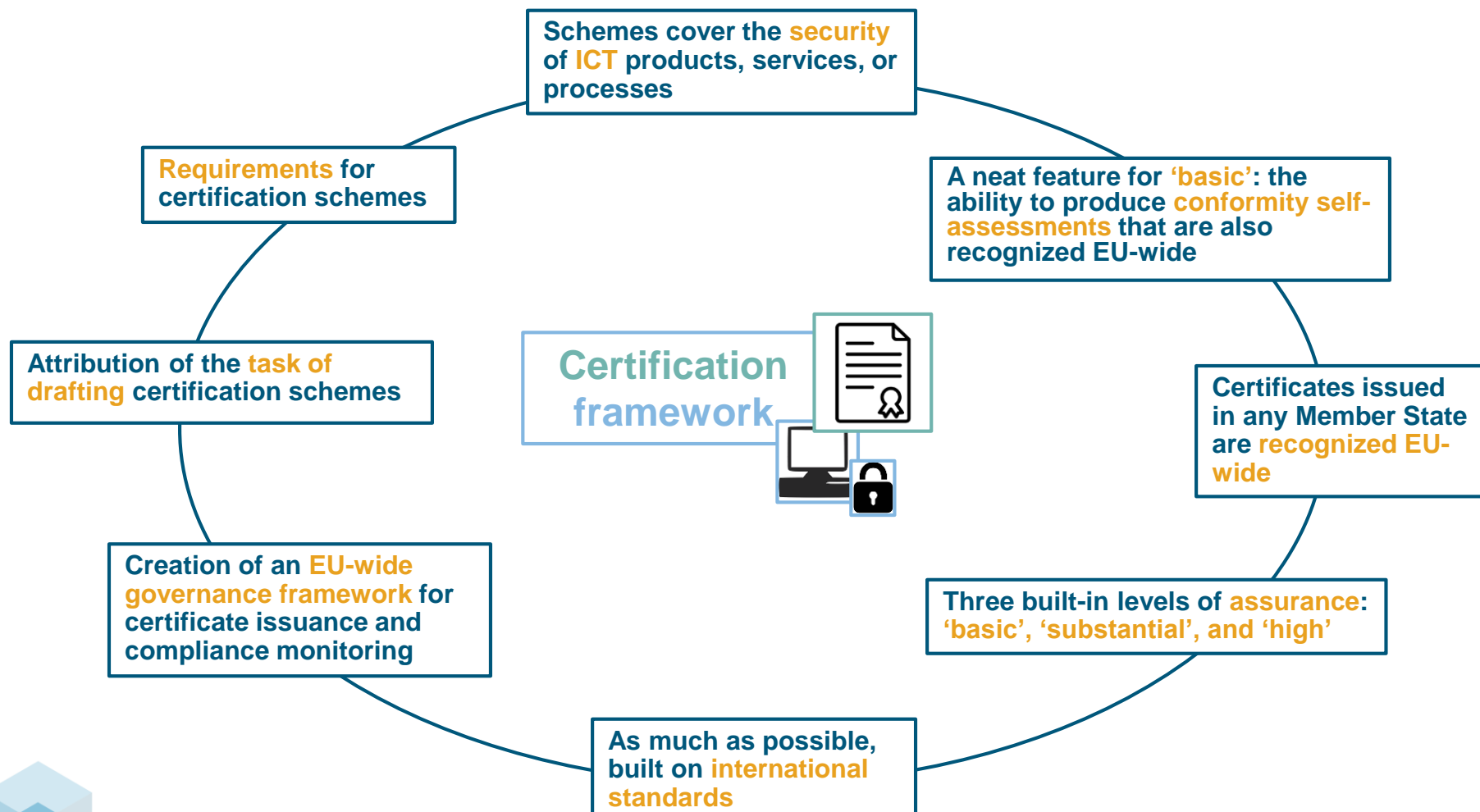
Specific tasks in the CSA

Article 8 Market, cybersecurity certification, and standardization

Article 20(4) on ad hoc working groups

Article 22 Stakeholder Cybersecurity Certification Group (SCCG)

[Visit ENISA \(online\) here.](#)



Union level



- Commission prepares topics (Union Rolling Work Program) supported by SCCG
- ENISA drafts schemes
- Commission approves and launches schemes with implementing acts
- ECCG (European Cybersecurity Certification Group) issues opinions on schemes

National Level

E.g.:



- Each MS appoints at least one NCCA to supervise and/or certify
- National Accreditation Bodies accredit the CABs
- CABs are welcome to be private sector entities
- The private sector (manufacturers) produce scheme-conform products/services/processes
- Manufacturers MAY issue declarations of conformity self-assessment (where the schemes allow it)
- Manufacturers MAY ask to get certificates from accredited Conformity Assessment Bodies (CABs)

By default, certification/conformity self-assessment is voluntary, unless specified by Union or Member State law

Planned deactivation of any existing national cybersecurity certification scheme covering the same topic



European
Commission

Adopts



Implementing
Act

“Prepare a
scheme on
topic X”

Final scheme



Drafts

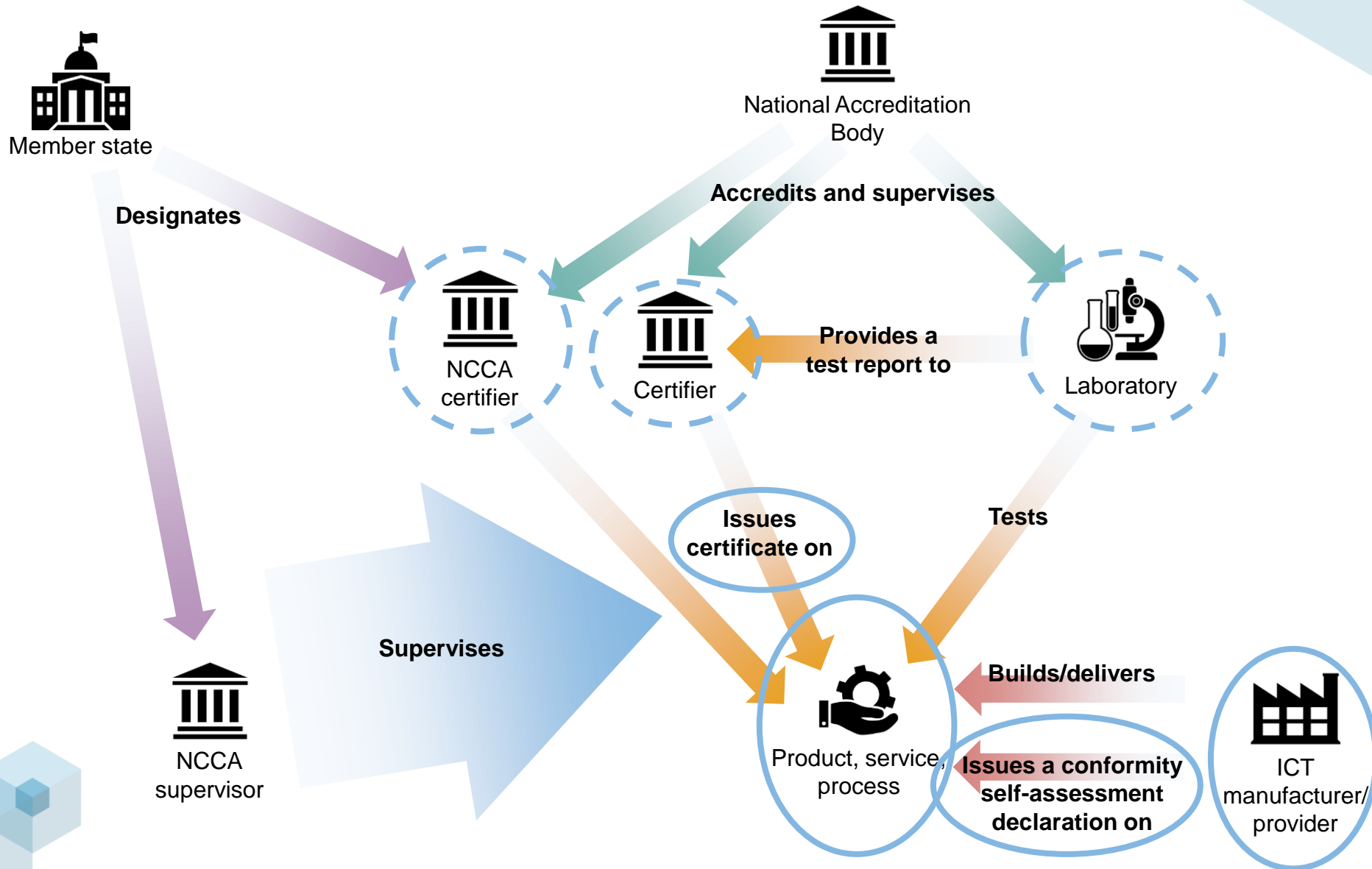
Feedback

Ad hoc Working
Group

Stakeholders



Certification scheme
following CSA format
(Art. 54)



The certification framework: What does a scheme look like?

Article 54(1), paragraphs a) to v)

22 elements

(a) the **subject matter** and scope of the certification scheme [...]

(d) where applicable, one or more **assurance levels**

(e) an indication of whether **conformity self-assessment** is permitted under the scheme

...and **others**...

(c) references to the **international, European or national standards** applied in the evaluation [...] or other cybersecurity requirements [...]

(g) the **specific evaluation criteria and methods** to be used, including types of evaluation [...]

(f) where applicable, specific or **additional requirements** to which **conformity assessment** bodies are subject [...]

(j) **rules for monitoring compliance** of ICT products, ICT services and ICT processes [...]



Certification scheme following CSA format

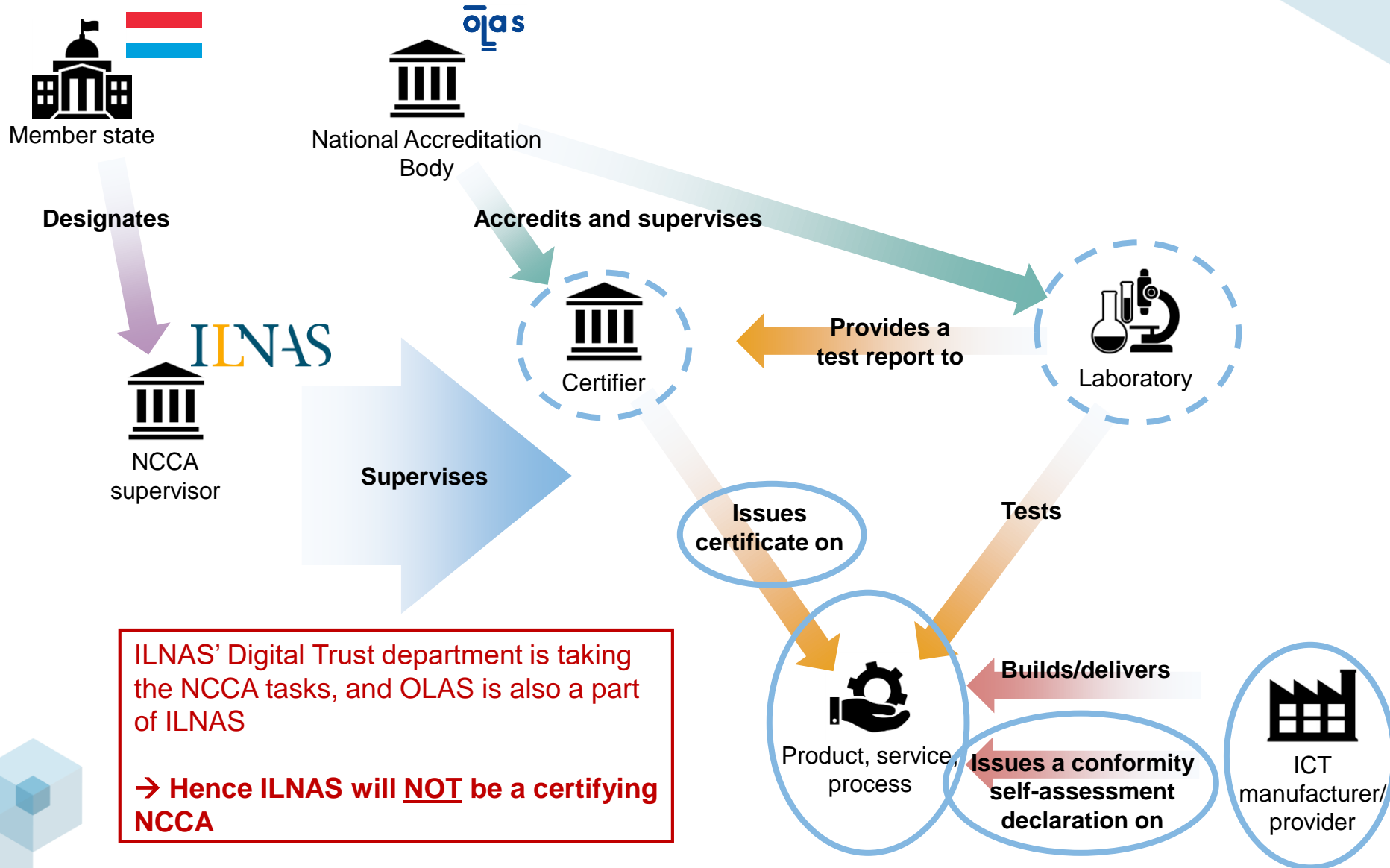
(p) the content and the **format** of the European cybersecurity certificates and the EU statements of conformity [...]

(q) the **period** of the availability of the EU **statement of conformity** [...]

(r) maximum **period** of validity of European cybersecurity **certificates** [...]

- Common Criteria based European candidate cybersecurity certification scheme (EUCC)
- [Final version May 25th, 2021](#)
- For IT products
- Product evaluation based on the Common Criteria standards
 - [ISO/IEC 15408 series on Information security, cybersecurity and privacy protection — Evaluation criteria for IT security](#) Revised in 2022. Now 5 parts
 - [ISO/IEC 18045 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation](#) Revised in 2022
 - See also the [Common Criteria Portal](#) for the publically available versions (“CC” and “CEM”) Not yet synched with the new ISO/IEC revisions
- Conformity assessment body accreditation
 - [ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services](#)
 - [ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories](#)
 - [ISO/IEC TS 23532-1:2021 Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408](#)
- Evaluator competence
 - [ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements](#) Under revision
 - [ISO/IEC 19896-3:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators](#) Under revision
- Assurance levels covered are ‘substantial’ and ‘high’ (so, no conformity self-assessment possible), with a detailed mapping of these to the Common Criteria assurance components
- Expect the EU Commission’s implementing act either at the end of 2022, or at the “very beginning” of 2023...







MISSIONS

Directly in the Luxembourg market

- Monitor that schemes' rules are being respected by products, processes, and services that are certified or the subject of a conformity self-assessment
- Cooperate with other market surveillance authorities
- Collaborate actively with OLAS to monitor CAB activity and if needed give authorizations

Within CSA governance

- Participate in the ECCG
- Collaborate with the Commission and other NCCAs in sharing knowledge and for continuous improvement of schemes

ACTIVITIES AND CONTACTS

Ongoing

- Updating the DTD documentation to accommodate supervision requests
- Collaborating with OLAS to cooperate efficiently in CAB supervision

Contact info

- Alain WAHL (Head of the Digital Trust department)
- Jean-François GILLET and Jean LANCRENON
- Department email supervision-cybersecurite@ilnas.etat.lu
- Department phone (+352) 247 743 50
- <https://portail-qualite.public.lu/fr/cybersecurity-act.html>



Thank you
Merci
Danke

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 - 01 · Fax : (+352) 24 79 43 - 10

E-mail : info@ilnas.etat.lu

www.portail-qualite.lu