

ACCREDITATION

CONFIANCE
NUMÉRIQUE

SURVEILLANCE
DU MARCHÉ

MÉTROLOGIE

NORMALISATION

ILNAS

Welcome
Bienvenue
Willkommen

Point sur l'accréditation cybersécurité

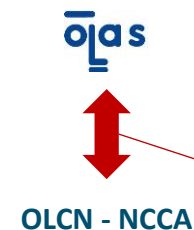
Programme "Critères Communs"

Journée de la Communauté de
l'Accréditation – 03/10/2025

Ministère de l'Environnement, du Climat et du
Développement Durable

Jean Lancrenon
Chargé de mission – Cybersécurité
Organisme Luxembourgeois de la Confiance Numérique, ILNAS





Aujourd'hui,
on va ici.

MISSIONS EN GENERAL

Directement auprès du marché luxembourgeois

- Surveillance des Prestataires de services de confiance dans le contexte du règlement eIDAS
- Maintenance de la liste de confiance du Luxembourg
- Surveillance des Prestataires de Services de Dématérialisation et de Conservation dans le contexte du cadre legal national d'archivage électronique
- National Cybersecurity Certification Authority (NCCA) – Supervision dans le contexte du Cybersecurity Act

CONTACTS

Contacts

- Alain WAHL (Responsable de l'OLCN)
- Michèle FELTZ (Services de confiance)
- Michel LUDWIG (archivage électronique)
- Jean LANCRENON (NCCA)
- Jean-François GILLET (NCCA)
- Department email confiance-numerique@ilnas.etat.lu
- Department phone (+352) 247 743 50
- <https://portail-qualite.public.lu/fr/cybersecurity-act.html>

RÈGLEMENT (UE) 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) no 526/2013 (règlement sur la cybersécurité)

Adopté le 17 avril 2019

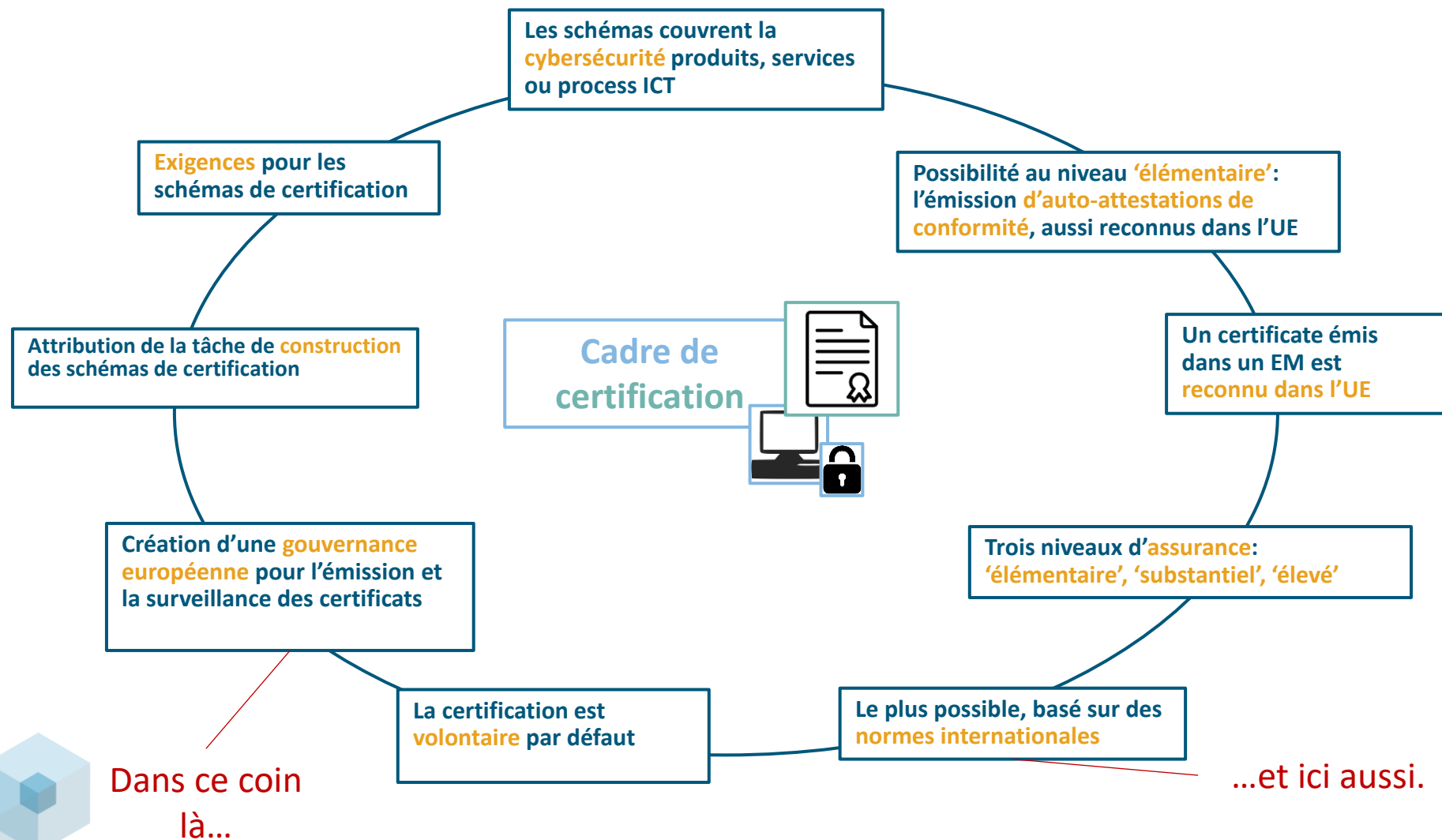
Entré en vigueur en juin 2021

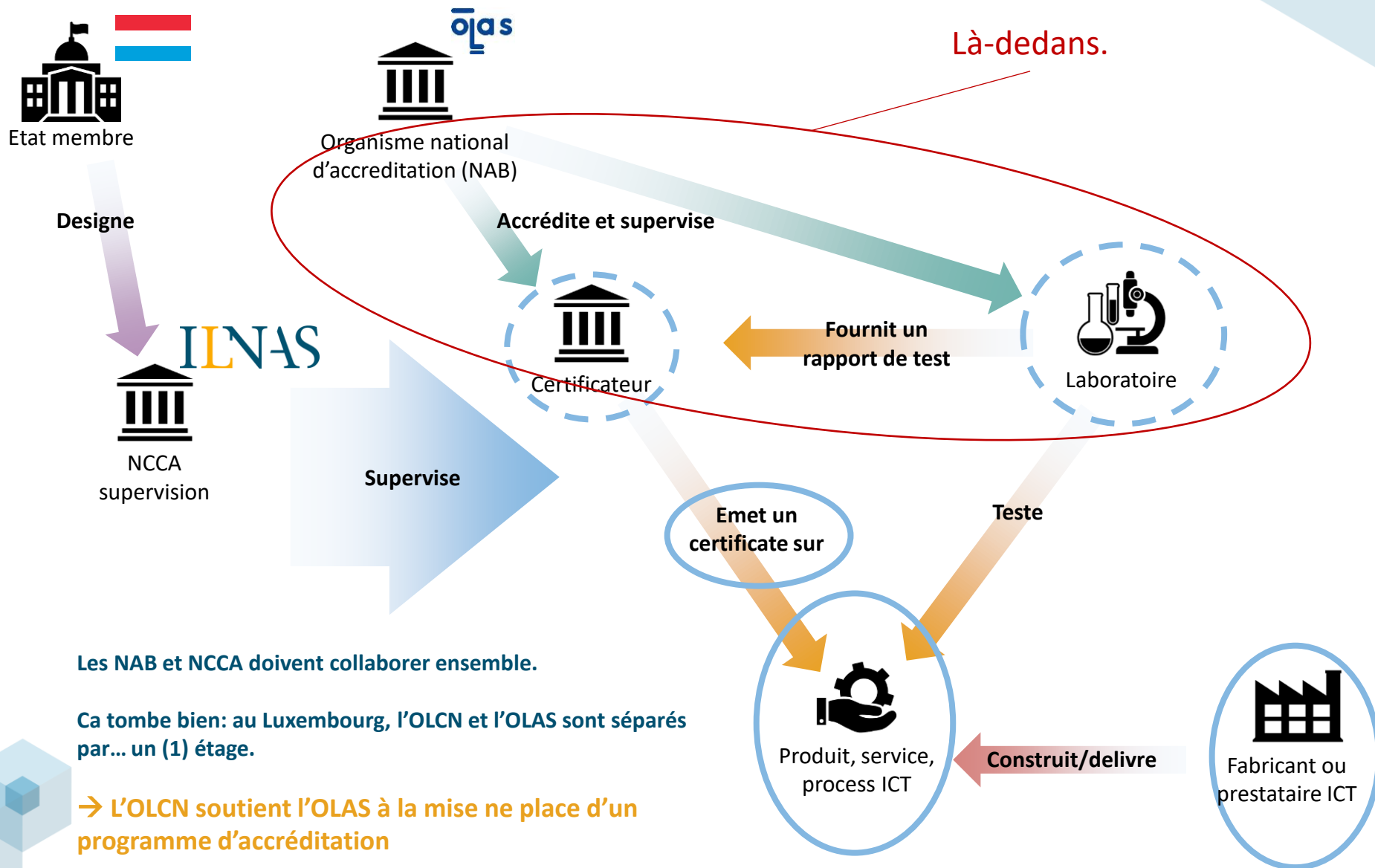


Cadre européen de
certification en
cybersécurité



On va là.





Pour quel schéma de certification ? ? ?

EUCC

C'est où on va.



RÈGLEMENT D'EXÉCUTION (UE) 2024/482 DE LA COMMISSION du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUC)

Premier schéma adopté du CSA

Adopté en janvier 2024

- Pour les produits ICT avec des fonctions de sécurité
- Evaluation de la **cybersécurité** des produits ICT, basée sur les normes 'Critères Communs'
 - [ISO/IEC 15408 series on Information security, cybersecurity and privacy protection — Evaluation criteria for IT security](#) En cours de révision
 - [ISO/IEC 18045 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation](#) En cours de révision
 - Voir aussi le [Common Criteria Portal](#) pour les versions CC et CEM (rigoureusement identiques aux normes internationales)
- **Base d'accréditation des OEC**
 - [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](#)
- **Base de compétences des évaluateurs**
 - [ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements](#) En cours de révision
 - [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](#) En cours de révision
- Couvre les niveaux d'assurance 'substantiel' et 'élevé'
- Il y a beaucoup d'autres documents d'exigences, de guides d'harmonisation pour compléter ces bases, voir le [site dédié de l'ENISA](#)

Ce qui nous intéresse est plutôt ici...



RÈGLEMENT D'EXÉCUTION (UE) 2024/482 DE LA COMMISSION du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUC)

Premier schéma adopté du CSA

Adopté en janvier 2024

- Pour les produits ICT avec des fonctions de sécurité
- Evaluation de la **cybersécurité** des produits ICT, **basée** sur les normes 'Critères Communs'
 - [ISO/IEC 15408 series on Information security, cybersecurity and privacy protection — Evaluation criteria for IT security](#) En cours de révision
 - [ISO/IEC 18045 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation](#) En cours de révision
 - Voir aussi le [Common Criteria Portal](#) pour les versions CC et CEM (rigoureusement identiques aux normes internationales)
- **Base d'accréditation des OEC**
 - [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](#)
- **Base de compétences des évaluateurs**
 - [ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements](#) En cours de révision
 - [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](#) En cours de révision
- Couvre les niveaux d'assurance 'substantiel' et 'élevé'
- Il y a beaucoup d'autres documents d'exigences, de guides d'harmonisation pour compléter ces bases, voir le [site dédié de l'ENISA](#)

...mais il faut d'abord comprendre un peu ça.



INTERNATIONAL
STANDARDISO/IEC
15408-1Fourth edition
2022-08**Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —****Part 1:
Introduction and general model***Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —**Partie 1: Introduction et modèle général*

Le modèle général
d'utilisation du
référentiel

INTERNATIONAL
STANDARDISO/IEC
15408-2Fourth edition
2022-08**Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —****Part 2:
Security functional components***Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —**Partie 2: Composants fonctionnels de sécurité*

Les composants de types
1) d'exigences de sécurité
fonctionnelle et 2)
d'exigences d'acquisition
d'assurance

La méthodologie d'organisation
et de déroulement de
l'évaluation avec le formalisme
de la 15408

INTERNATIONAL
STANDARDISO/IEC
15408-3Fourth edition
2022-08**Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —****Part 3:
Security assurance components***Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —**Partie 3: Composants d'assurance de sécurité*INTERNATIONAL
STANDARDISO/IEC
18045Third edition
2022-08**Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security — Methodology
for IT security evaluation***Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information — Méthodologie pour l'évaluation de sécurité*

Objectif: *"The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software.*

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs." – Introduction, 15408-1:2022

Comparabilité d'évaluations

- Formalisme de description de spécifications cybersécurité, en matière fonctionnelle et d'assurance : 15408-1,2,3(,4,5)
- Encodage et suivi de méthodologie d'évaluation : 18045



INTERNATIONAL
STANDARD

ISO/IEC
15408-1

Fourth edition
2022-08

Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —

Part 1:
Introduction and general model

Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —

Partie 1: Introduction et modèle général

- Comment décrire son produit: “**Security Target**” (**document**) (et comment décrire une catégorie de produits: “**Protection Profile**”)
 - Spécification du **problème de sécurité** (objectifs, menaces, environnement d'operation...)
 - Spécification des composants nécessaires pour **répondre au problème de sécurité**
 - Justification des choix (“tracing”)

Le ST est une spécification documentaire formelle du produit dans le langage de la 15408, produite par le fabricant.

Aussi : Utilisation de, et operations autorisées sur, les composants fonctionnels/d'assurance;
Modèle de ST/PP; opérations modulaires sur les PP; modes de conformance à des constructions de PP



INTERNATIONAL
STANDARDISO/IEC
15408-2INTERNATIONAL
STANDARDISO/IEC
15408-3Fourth edition
2022-08Fourth edition
2022-08Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —Part 2:
Security functional componentsSécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —

Partie 2: Composants fonctionnels de sécurité

Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —Part 3:
Security assurance componentsSécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —

Partie 3: Composants d'assurance de sécurité

Distinguer entre “fonctionnel” et
“assurance”:

- **Fonctionnel:** Composant technique qui contribue une mesure de sécurité (e.g. “mécanisme d'authentification”)
- **Assurance:** Composant qui permet de gagner en confiance en le fait que la sécurité est en place (e.g. “existence de description architecturale décrivant le mécanisme d'authentification”)

FAU: Security Audit

FCO: Communication

FCS: Cryptographic support

FDP: User data protection

FIA: Identification and Authentication

FMT: Security management

FPR: Privacy

FTP: Protection of the [product] security functionality

FRU: Resource utilization

FTA: [Product] access

FTP: Trusted paths/channels

APE: Protection Profile evaluation

ACE: Protection Profile Configuration evaluation

ASE: Security Target evaluation

ADV: Development

AGD: Guidance documents

ALC: Life-cycle support

ATE: Tests

AVA: Vulnerability assessment

ACO: Composition

INTERNATIONAL
STANDARDISO/IEC
15408-2Fourth edition
2022-08Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —Part 2:
Security functional components*Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —**Partie 2: Composants fonctionnels de sécurité*INTERNATIONAL
STANDARDISO/IEC
15408-3Fourth edition
2022-08Information security, cybersecurity
and privacy protection — Evaluation
criteria for IT security —Part 3:
Security assurance components*Sécurité de l'information, cybersécurité et protection de la vie
privée — Critères d'évaluation pour la sécurité des technologies de
l'information —**Partie 3: Composants d'assurance de sécurité*

La notion de dépendance : “**Pour avoir composant A, il faut composant B**”

- Très important pour l'assurance
- Permet de hiérarchiser formellement et clairement la profondeur d'une évaluation en gain en assurance
- Conduit aux “**Evaluation Assurance Levels**” (EAL)

14.3.5 AVA_VAN.3 Focused vulnerability analysis

Dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

INTERNATIONAL STANDARD	ISO/IEC 15408-2	INTERNATIONAL STANDARD	ISO/IEC 15408-3
	Fourth edition 2022-08		Fourth edition 2022-08
Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components		Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components	
Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 2: Composants fonctionnels de sécurité		Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 3: Composants d'assurance de sécurité	

Les EAL :

- **7 niveaux**, du moins profond (1) au plus profond (7)
- **Paquets prédéfinis** de niveaux de profondeur d'évaluation
- On ajoute des composants d'assurance ou on incrémente la hiérarchie des dépendances

EAL 7 : Formally verified design and tested

EAL 1 : Functionally tested

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: ST evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
ATE: Tests	ASE_TSS.1 TOE summary specification
	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security model policy
AGD: Guidance documents	ADV_TDS.6 Complete semi-formal modular design with formal high-level design presentation
	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Measurable life-cycle model
ASE: ST evaluation	ALC_TAT.3 Compliance with implementation standards – all parts
	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
ATE: Tests	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
	ATE_COV.3 Rigorous analysis of coverage
AVA: Vulnerability assessment	ATE_DPT.4 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
	AVA_VAN.5 Advanced methodical vulnerability analysis

EAL 4 : Noyau de système d'exploitation de PC
Dernier EAL "rétroactivement applicable à un produit"

INTERNATIONAL
STANDARDISO/IEC
18045Third edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité

Structure :

- Une structure qui suit les classes d'assurance de 15408-3
- Définit des **unités de travail** ("work units") pour l'évaluateur correspondant aux composants d'assurance présents dans le ST
- Chaque unité de travail présente des exigences d'actions pour l'évaluateur, sur base d'input fourni par 1) le fabricant et 2) l'éléments d'entrée d'autres unités de travail

The evaluator *shall produce*

The evaluator *shall devise*

The evaluator *shall examine*

The evaluator *shall record*

The evaluator *shall check*

The evaluator *shall conduct*

The evaluator *shall determine*

The evaluator *shall perform*

The evaluator *shall report*

INTERNATIONAL
STANDARD

ISO/IEC
18045

Third edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

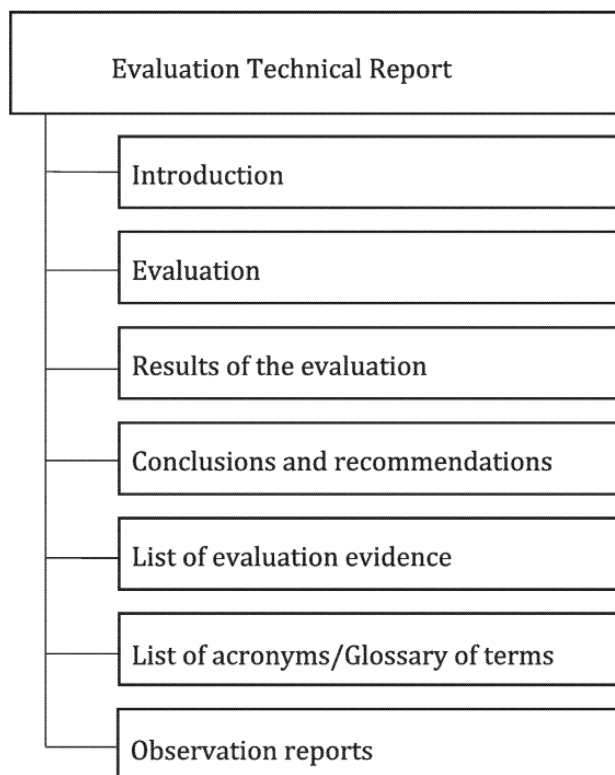
Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité

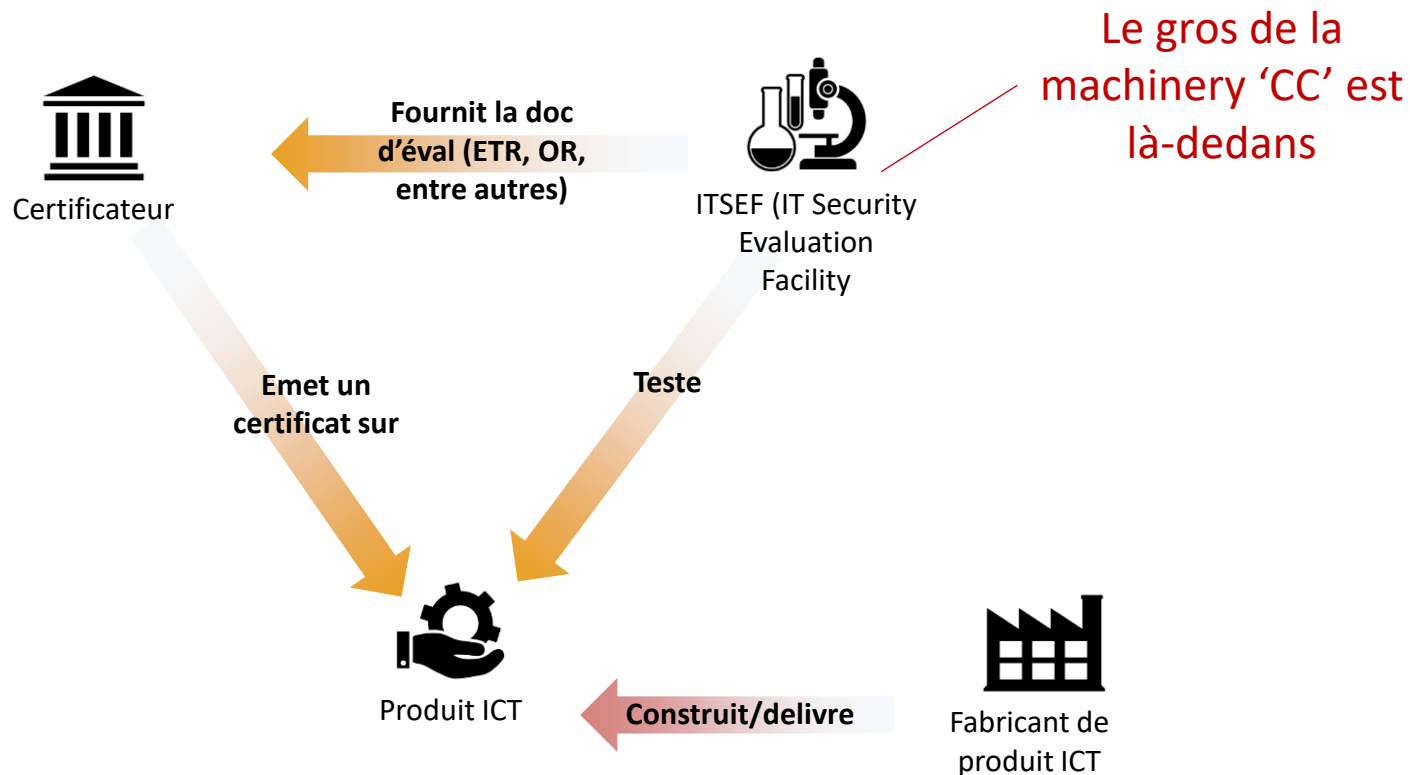
Output supplémentaire:

- Il peut y avoir un rapport par classe d'assurance
- *La documentation des tests, en particulier des tests de vulnérabilité*

Principal élément de sortie :

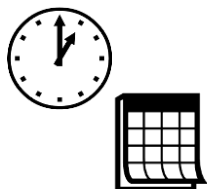
- *'Evaluation Technical Report' (ETR) avec un verdict global*
- *'Observational report(s)' (ORs)*





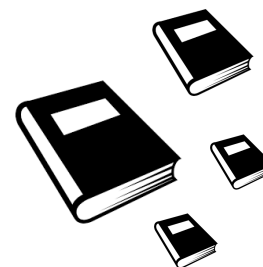
Une évaluation 'Critère Communs' c'est généralement :

CHER. *Peut de chiffrer en multiples de €10k ou €100k.* € € €



LONG. *Se déroule sur un période de mois; peut dépasser une année.*

DENSE. *Un ETR, c'est plusieurs dizaines de pages; des rapports annexes peuvent en faire ~100.*



Comment on accrédite ce truc?*

*Sans faire exploser les coûts et les temps d'audit, s'entend.



Problème à résoudre : Définir un déroulé d'audit plausible

- Domaine *nouveau* pour l'OLAS
- Il nous faut faire de la *17065 pour les certificateurs* et de la *17025 pour les ITSEFs*
- On commence par les ITSEFs 
- Informations à l'entrée:
 - Toutes les normes
 - La documentation EUCC
 - Documentation 'CC' d'autres pays qui en font depuis longtemps
 - Discussions avec d'autre pays
 - Discussions avec des ITSEFs

On va regarder le cas d'un ITSEF primo-accédant à l'accréditation 17025

Un audit d'accréditation en 2 grandes phases

1ère phase: Système et compétences “sur le papier”

- Système de management 17025
- Entretiens avec le personnel

2ème phase: Examen d'une évaluation pilote

- Une vraie évaluation 'CC' avec un vrai client est lancée
- Au cours de l'évaluation, des “checkpoints” sont ponctuellement vérifiés par l'équipe d'audit



*1ère phase: Système et compétences "sur le papier"***Travail de
l'accréditeur**

Audit du système de management **2+2 jours**
+ Entretiens structurés des évaluateurs **1 jour**

Rapport partiel
d'audit
½ jour

**Travail de
l'ITSEF**

Audit du système de management, et de la compétence du personnel

Définition d'un projet pilote

2ème phase: *Examen d'une évaluation pilote*

Comment définit-on les checkpoints?

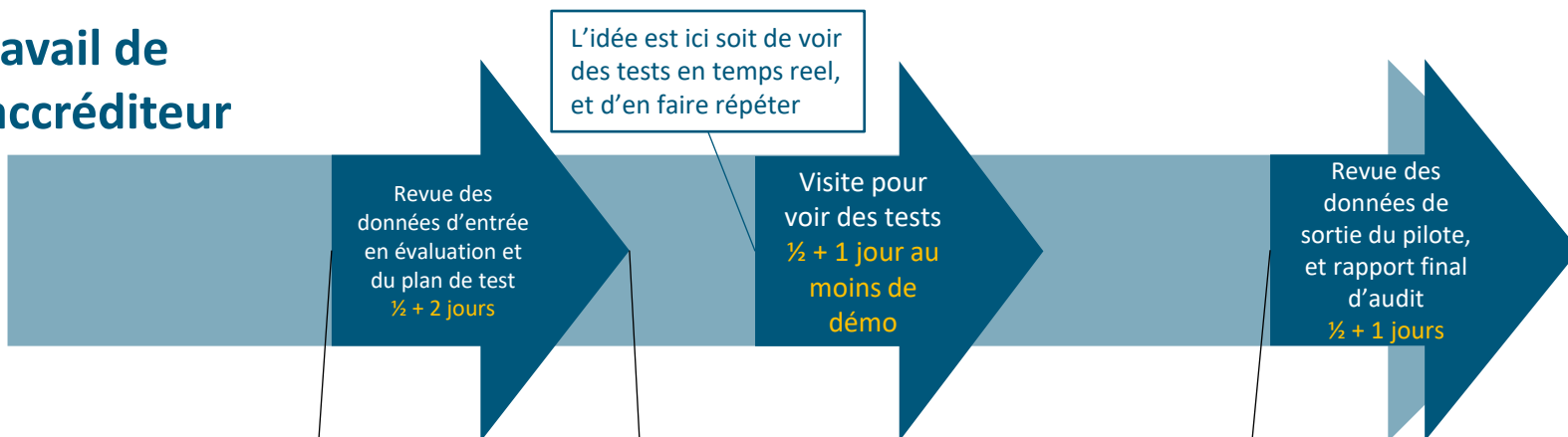
- L'idée de base est que la qualité générale de la grande majorité des unités de travail est capturée par les tests et la qualité des rapports finaux, notamment par le jeu des dépendances
- Beaucoup du travail fait dans les classes d'assurance sert à nourrir les tests fonctionnels et de vulnérabilité → On va focaliser sur cette documentation d'entrée aux tests, le plan de test, et les tests eux-mêmes.
 - 1er CP: La documentation réunie pour les tests + le plan de test
 - 2ème CP: Un ou plusieurs tests eux-mêmes
 - 3ème CP: La documentation finale

Il faut quand même échantillonner un peu, donc il faut des compétences techniques + du savoir 15408...

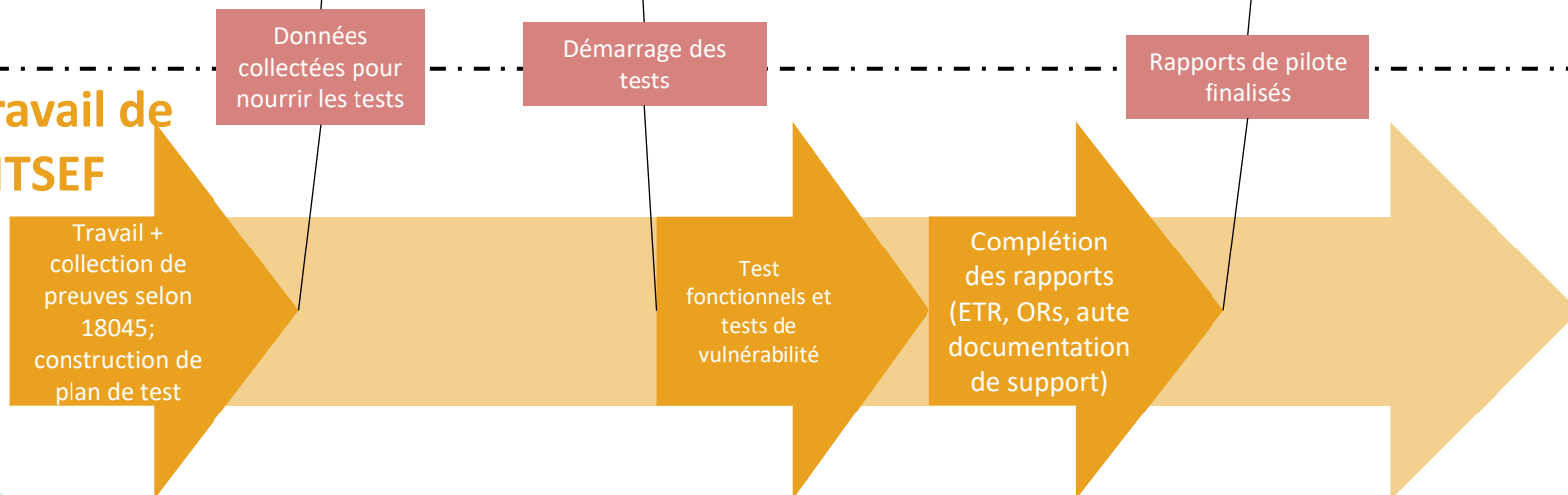


2ème phase: *Examen d'une évaluation pilote*

Travail de l'accréditeur



Travail de l'ITSEF



- On est sur au moins **13 jours d'audit**
 - Plausible
 - Commensurable avec ce qui se fait en matière de "ITSEF licensing" dans les cadres du CCRA ou du SOG-IS)
 - Descend à 6.5 dans le cadre d'un renouvellement
- Il faut des compétences "**système**", des compétences **15408-18045-EUCC**, et des **compétences techniques** (pentester + domaines techniques potentiels)
 - Note: un pentester ne connaît pas forcément la 15408...



- Les procédures et annexes OLAS *ne sont pas finalisées*; elles sont en cours de revue. → Les procédures pourraient (certainement) changer
- On travaille sur le cas des certificateurs selon la 17065
- L'OLAS va avoir besoin *d'auditeurs*
- Ce premier programme d'accréditation EUCC pourra *servir de base pour d'autres programmes "cyber"*, e.g. dans le cadre du CRA ou ailleurs

Voilà.







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