ETSI Security Week 2020

EUROSMART

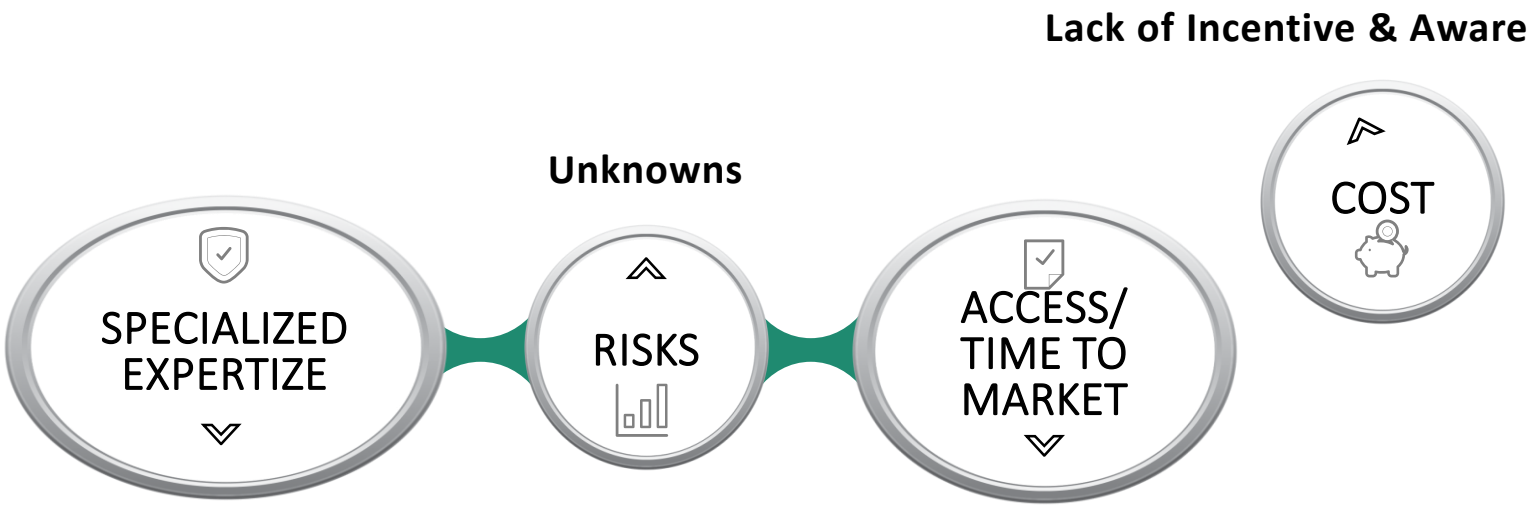
The Voice of the Digital Security Industry

E-IoT-SCS
Eurosmart
IoT Device Certification Scheme

RED ALERT LABS
IoT Security

Roland Atoui | Managing Director | Red Alert Labs

Vendors Pain !



Buyers/Users/Service Providers Pain !

CERTIFICATION → TRUST

"**TRUST** should be further **strengthened** by offering information in a **transparent** manner on the **level of security** of ICT products, ICT services and ICT processes …"

"An **increase in trust** can be facilitated by **Union-wide CERTIFICATION** providing for **common cybersecurity requirements** and **evaluation criteria** across national markets and sectors."

Cybersecurity Act – Section (7)

AT EUROSMART WE HAVE PREPARED :

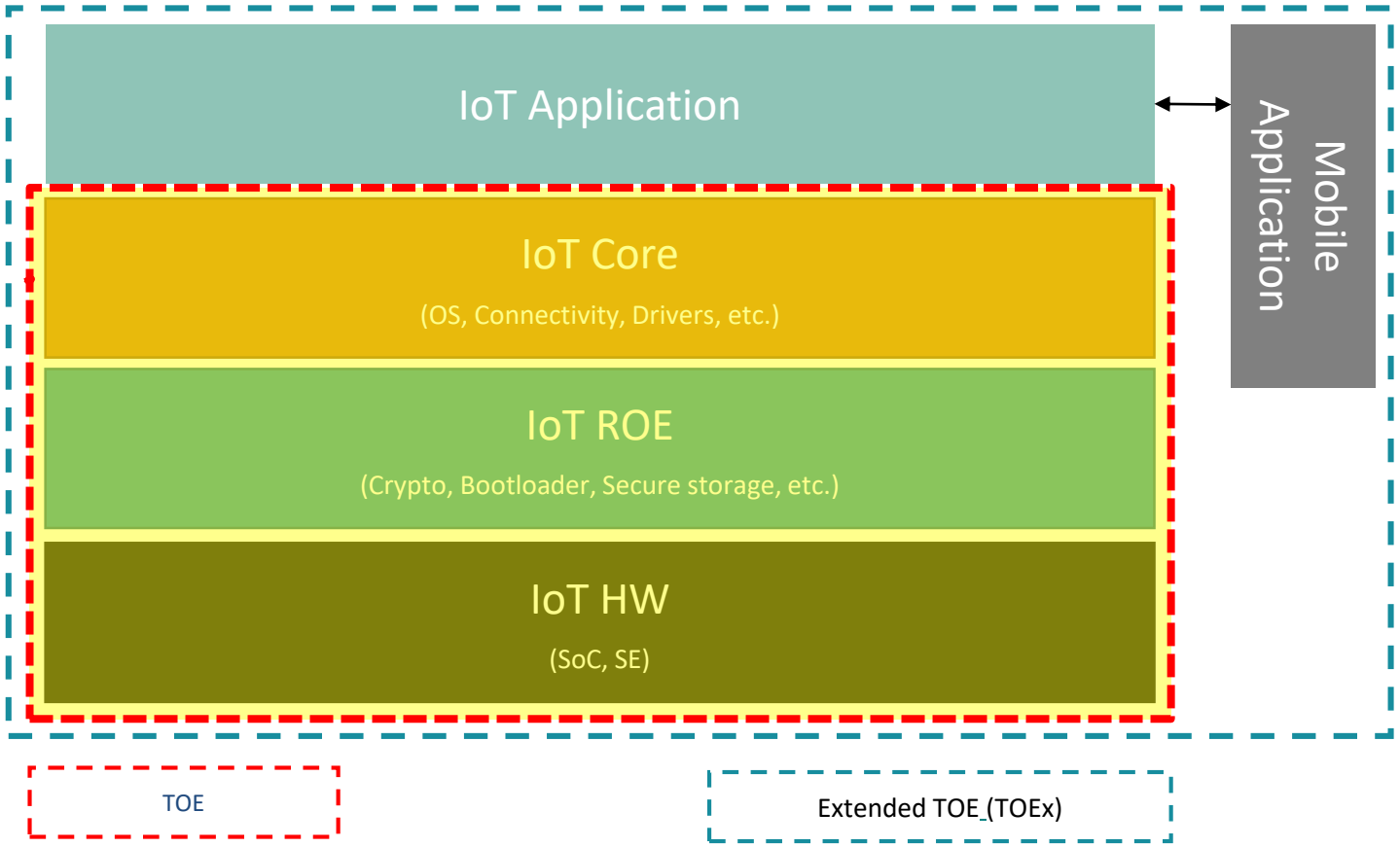
WITH THE NEW EU CSA REGULATION WE NEED A NEW CERTIFICATION SCHEME FOR IOT TO TACKLE :

- **Cost, time, validity**
  - **Can't be applied to the 50 Billion IoT product market ! Not enough resources to do that…**
- **Subjective**
  - **What is the credibility of the evaluation lab/pentester/etc. ?What does secure mean? Can we compare more or less secure products?**
- **Scope**
  - **Silo Approach - they often cover part of the problem, specific to an industry (banking, ID) but security & privacy is now a concern of every business and citizen.**
- **Poor Security Definition**
  - **There is no common and holistic approach to define security requirements per profile taking into account the threat model & risks due to the intended usage**

3 Security Assurance Levels – Focusing on Substantial

- **Basic**
  - Minimize the known basic risks of incidents and cyberattacks
- **Substantial**
  - Minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources
- **High**
  - Minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources

MODULAR TOE/DUT



RISK-BASED IoT MARKET VERTICALS

HIGH

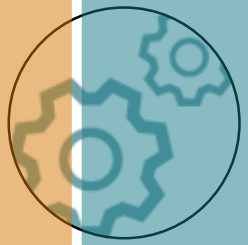
SUBSTANTIAL

BASIC

Critical

- Impacts on Safety…

➔ on special government interest



Industrial

- Impacts on Availability…

Entreprise

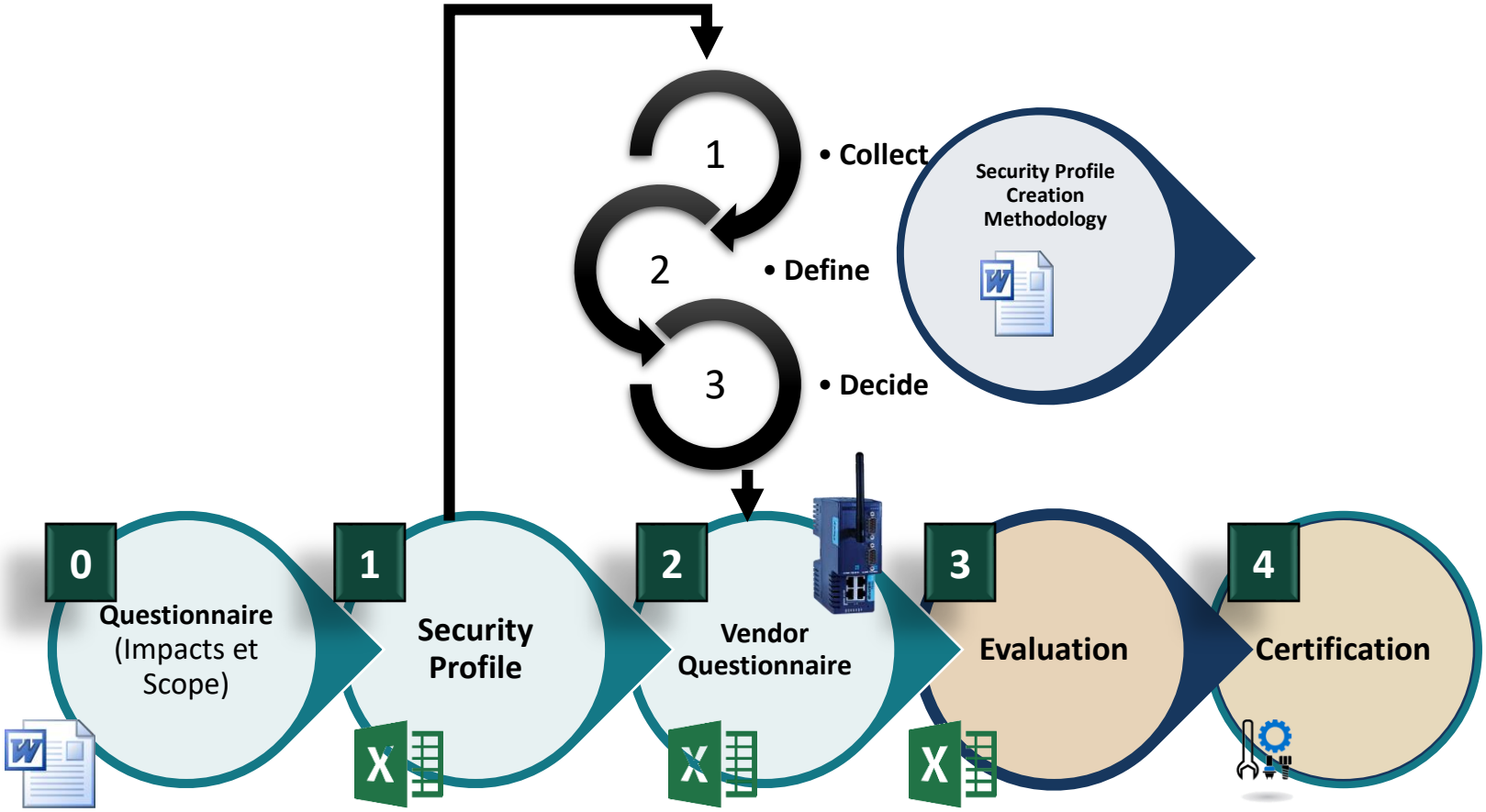
- Financial Impacts…

Consumer

- Impacts on Privacy

Impacts Prioritization

VENDOR's STEPS



A Risk-Based quick approach to create a security profile which looks like this:

EUROSMART
The Voice of the Digital Security Industry

security profile

CATEGORY *Remote Terminal Unit (RTU)*

DOMAIN *INDUSTRIAL*

USAGE
* *Collect Measurements from sensors*
* *Execute logic & control calculations*
* *Modify processes using control commands*
* *Communicate with external applications/devices*
* *Admin functions to configure RTU functionalities*

ASSUMPTIONS
* *No -Secured Physical Location*
* *Yes -Data-in-Transit encryption*
* *No -Admin Interface authentication*
* *No -Credentials & Cryptographic Keys protection*
* *No -Secured debug ports*

ASSETS
* *Process Control-Command*
* *Data-in-Transit*
* *Admin Interface*
* *Data-at-Rest*
* *OS/Kernel/Firmware*
* *Configuration Data*
* *Credentials & Cryptographic Keys*

SECURITY FEATURES
* *Malformed input management*
* *Secure authentication on administration interface:*
* *Access control policy*
* *Configuration access control*
* *Secure communication*
* *Command authorization*
* *Secure storage of secrets*
* *Secure Update*
* *Logs integrity*
* *Secure Boot and Trusted Boot*

Threat Id	Threat	Asset	Asset Value	Vulnerability	Impact	Likelihood	Total Risk	Security Goals	Security Requirements	Security Assurance Activities
T_FMN_01	Modifying the configuration of the RTU	Device Configuration	Integrity, Availability, Authenticity	WEAK AUTHENTICATION. IMPROPER ACCESS CONTROL	Severe	Very Likely	SUBSTANTIAL	SECURITY DATA MANAGEMENT; IDENTIFICATION & AUTHENTICATION	EIA_SF.10; EIA_SF.68; EIA_SF.69	SEE SF_REQUIREMENTS
T_FMN_02	Destroy, Remove or Steal RTU	Physical Device	Availability	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL	EIA_SF.23; EIA_SF.24 EIA_SF.25; EIA_SF.26 EIA_SF.63	SEE SF_REQUIREMENTS
T_FMN_03	Replacement of original RTU with a compromised one	Physical Device	Integrity, Authenticity	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL PHYSICAL SECURITY SECURE INTERFACES & NETWORK SERVICES	EIA_SF.54; EIA_SF.83	SEE SF_REQUIREMENTS

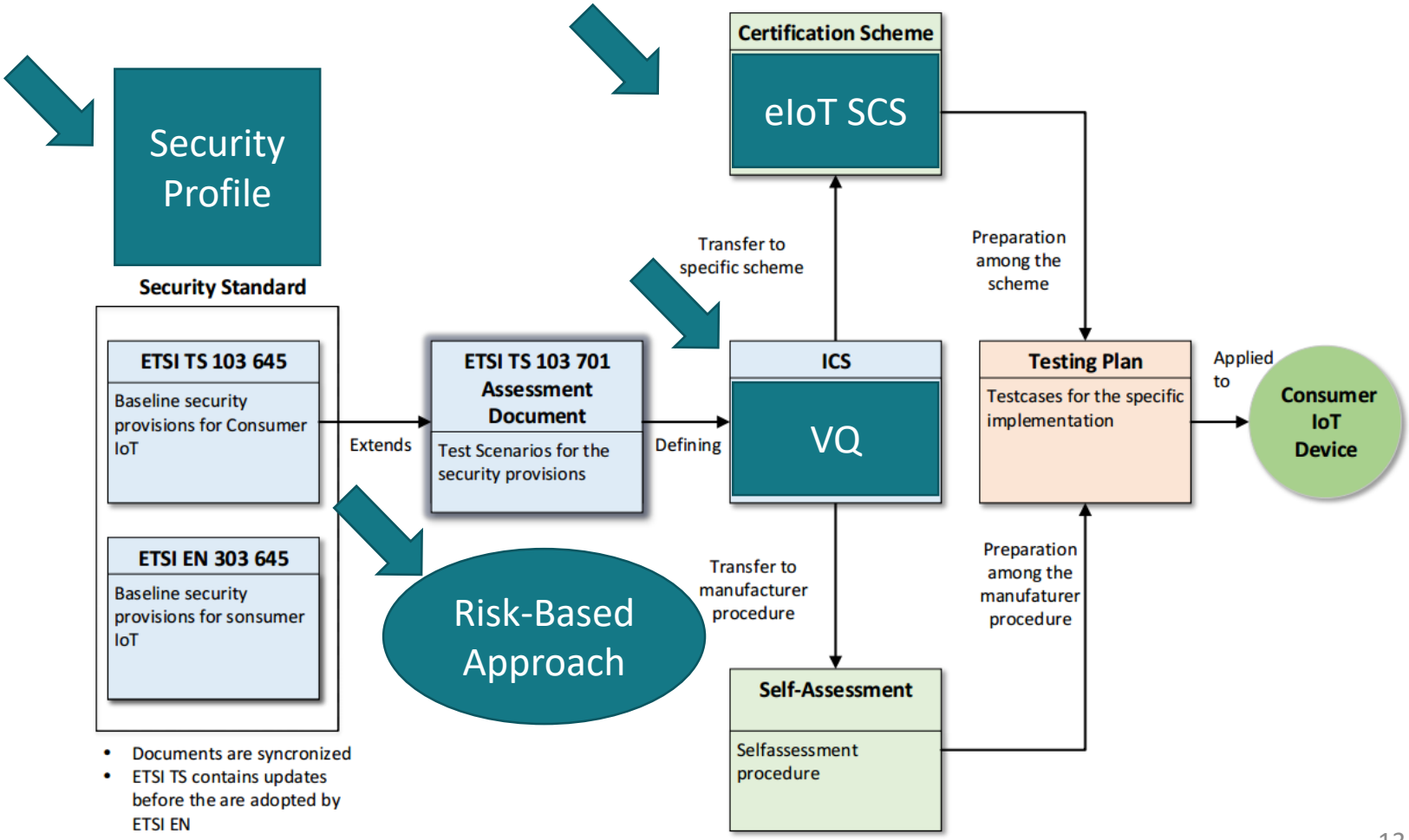
RISK-BASED - SECURITY ASSURANCE ACTIVITIES

SUBSTANTIAL

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting
MODERATE (3)				
MINOR (2)			VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning

- **Conformity Analysis** (Doc Review, Source Code Review, Composition Analysis, Security Functional Testing)
- **Vulnerability Analysis** (Scanning, Basic Robustness Testing, Advanced Robustness Testing, Non-Intrusive Pentesting)

HOW EN 303 465 and TS 103 701 ARE USED ?



EN 303 465 Security Profile | Mapping

ETSI Provision	ETSI Provision Details	Security Goals	Description	Security Requirements	Ref
4.1 No universal default passwords	Provision 4.1-1	Identification and Authentication	Ensure the legitimacy of the applicant for access to the product (user and / or machine)	Mandatory change of default password & username at first-login	EIA_SF.16
				Uniqueness of the identifier	EIA_SF.18
4.2 Implement a means to manage reports of vulnerabilities	Provision 4.2-1			The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.	EIA_FR.10
				The developer shall document flaw remediation guidance addressed to IoT device users. This guidance shall describe a means by which IoT device users report to the developer any suspected security flaws in the IoT device	EIA_FR.12
	Provision 4.2-2			The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	EIA_FR.3
	Provision 4.2-3			As part of flaw remdiation policies a set of actions must be defined to fix the flaw securely in IoT devices supporting remote software update.	EIA_FR.5
				Establish a comprehensive and well-defined process for disclosure of vulnerabilities.	EIA_FR.6

CERTIFICATION EXPECTED DURATION
BASIC

0 MAN/DAYS (ETSI EN 303 465)		• **Security Profile Creation (Per domain (consumer, enterprise, industrial…)**
	1-2 MAN/DAYS	• **Vendor Questionnaire Analysis** • **Installation of the product** • **Conformity Analysis (docs)**
	0.5 MAN/DAYS	• **Conformity Assessment/Doc Review** • **Evaluation Report Review** • **Certificate Issuance**
0 +	**1.5-2.5** MAN/DAYS	

EUROSMART
The Voice of the Digital Security Industry

CERTIFICATION EXPECTED DURATION SUBSTANTIAL

5-12 MAN/DAYS

- **Security Profile Creation**

2-5 MAN/DAYS

- **Vendor Questionnaire Analysis**
- **Installation of the product**
- **Conformity Analysis**

5-10 MAN/DAYS

- **Risk-Based Vulnerability Analysis**
- **Evaluation Report Review**
- **Certificate Issuance**

5-12 + 7-15 MAN/DAYS

Pre-defined by the **Security Profile**

EUROSMART
The Voice of the Digital Security Industry

The END…

E-IoT-SCS KEY TAKEAWAYS

- Open Source (https://www.eurosmart.digital/eurosmart-iot-certification-scheme/)
- Supported Several Industrials (Vendors, Labs, TICs) and by ENISA (https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii)
- Built-In Risk Analysis adapted to IoT
- Full Compliance with the EU Cybersecurity Act - Article 54
- BASIC assurance relies completely on ETSI EN 303 465 and TS 103 701 and partially for the SUBSTANTIAL level
- Simple process solving both vendors and users pain

EUROSMART
The Voice of the Digital Security Industry

EUROSMART

The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Eurosmart

Rue de la Science 14b | 1040 Brussels | BELGIUM

Tel. +32 2 880 36 35