TIC COUNCIL

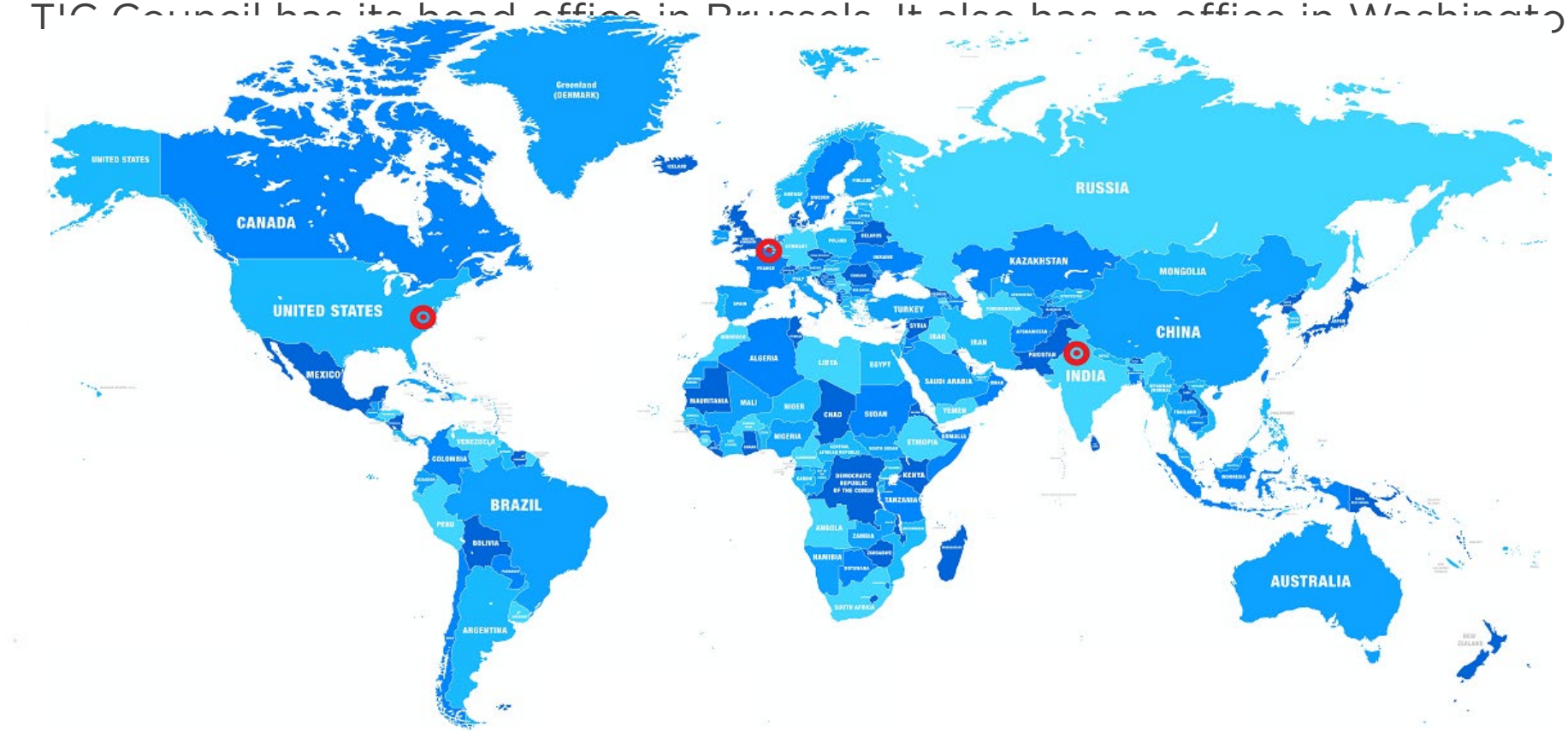
THE INDEPENDENT VOICE OF TRUST

TIC Council Webinar
The contribution of the TIC sector to cybersecurity: implementation opportunities and challenges of the European Cybersecurity Act

TIC Council

The Independent Voice of Trust

- Born from the merger of IFIA and CEOC
- ~90-member companies & organizations active in more than 160 countries (HQ mapped)
- TIC Council has its head office in Brussels. It also has an office in Washington and



TIC Council Mission

As the voice of the global independent testing, inspection and certification industry, the TIC Council engages governments and key stakeholders to advocate for effective solutions that protect the public, support innovation and facilitate trade.

The TIC Council works with its members to promote best practices in safety, quality, health, ethics and sustainability

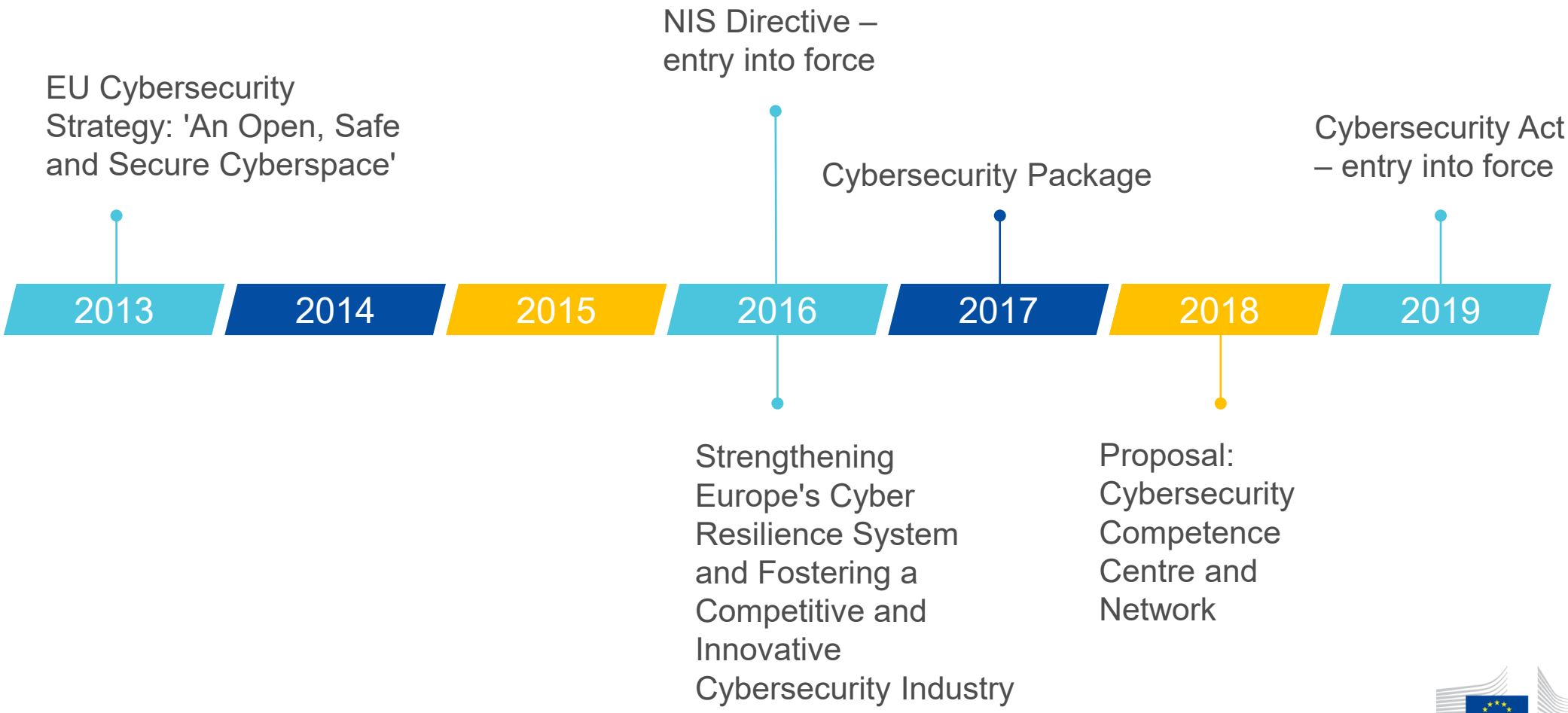
Cybersecurity certification in the EU

Webinar: The contribution of the TIC sector to cybersecurity: Implementation opportunities and challenges of the European Cybersecurity Act

DG CNECT.H2 Cybersecurity and Digital Privacy Policy

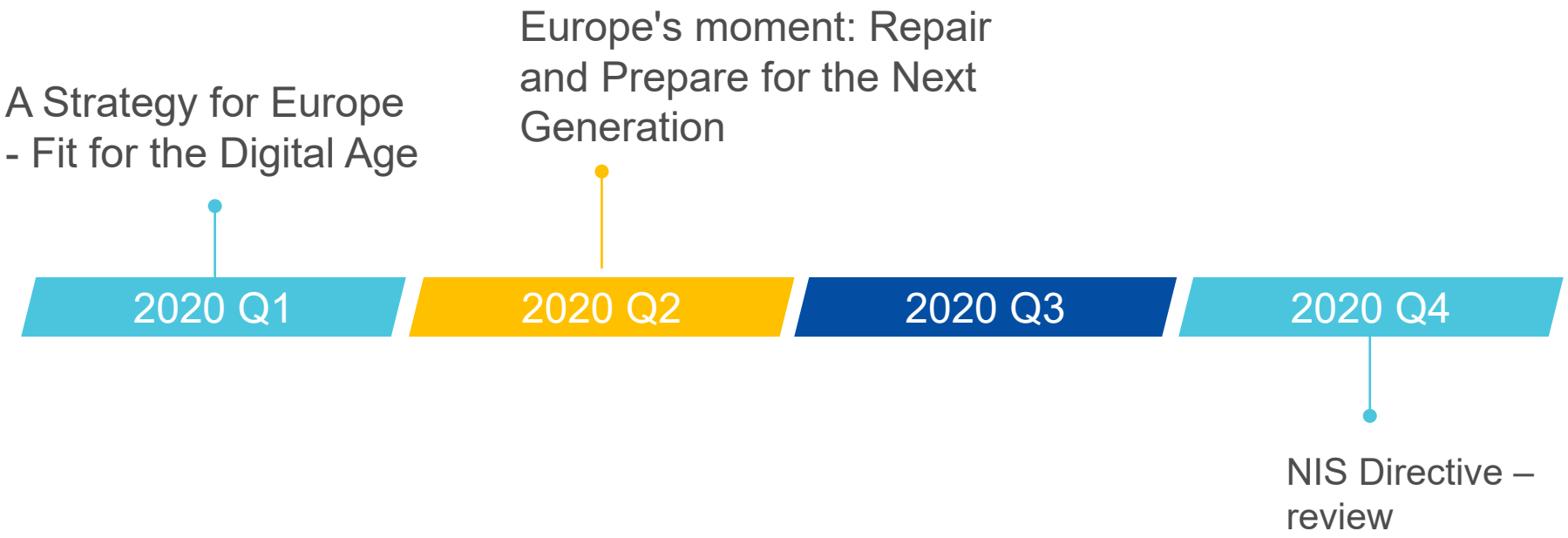
Aristotelis Tzafalias

Continuous policy response to increasing digitalisation and the evolving threat landscape



European Commission

A busy year ahead



European Commission

European Cybersecurity Certification Framework

Digitalisation of society leads to greater need for cyber secure products and services

A common European approach to cybersecurity certification in the Single Market

Fit for purpose, voluntary, European Cybersecurity Certification Schemes

European Commission

European cybersecurity certification framework – state of play

Cybersecurity Act

- Entry into force June ‘19

Candidate Schemes

- “SOG-IS MRA”
- Cloud services

Advisory groups

- ECCG - established
- SCCG - soon

Union Rolling Work Programme for European cybersecurity certification

- Publication 2020

European Commission

Union Rolling Work Programme for European cybersecurity certification

- Strategic priorities
  - Standardisation
  - Security by design (including activities performed to design, develop, deliver or maintain an ICT product);
  - Risk Based Assurance
  - International cooperation

European Commission

Union Rolling Work Programme for European cybersecurity certification

- Requests for future candidate scheme taking into account
  - Existing national schemes
  - National or EU policy
  - Market demand
  - Emerging threats

European Commission

Thank you

European Commission

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity certification: keeping abreast with the Cybersecurity Act

Dr Andreas Mitrakas
Head of Unit “Data security and standardisation”

TIC Council Webinar

18 | 06 | 2020

EU'19-20

Agenda

- Policy areas in data security and stand
- Key activities
- Bridgi

PRIORITIES

Programme

Common values and the rule of law

Competitiveness and social inclusion

- Single market
- Wellbeing and skills
- Trade policy

nomic union

e leadership

ssions reduction targets

ehensive security

ernal action

urity and defence cooperation

rid and cyber threats

Other key issues

- Migration
- Multiannual financial framework

A Europe that protects

The European Union considers the security of its citizens to be an issue of of utmost importance. Hence, the Croatian Presidency will work on strengthening internal security, providing more effective control of external borders, ensuring full interoperability of IT systems, and strengthening resilience to external threats, as well as hybrid and cyber threats. Our common goal remains to find a comprehensive solution for a asylum policy. The Croatian Presidency will focus on further establishing t and justice, founded on common values, democracy and the rule of law.

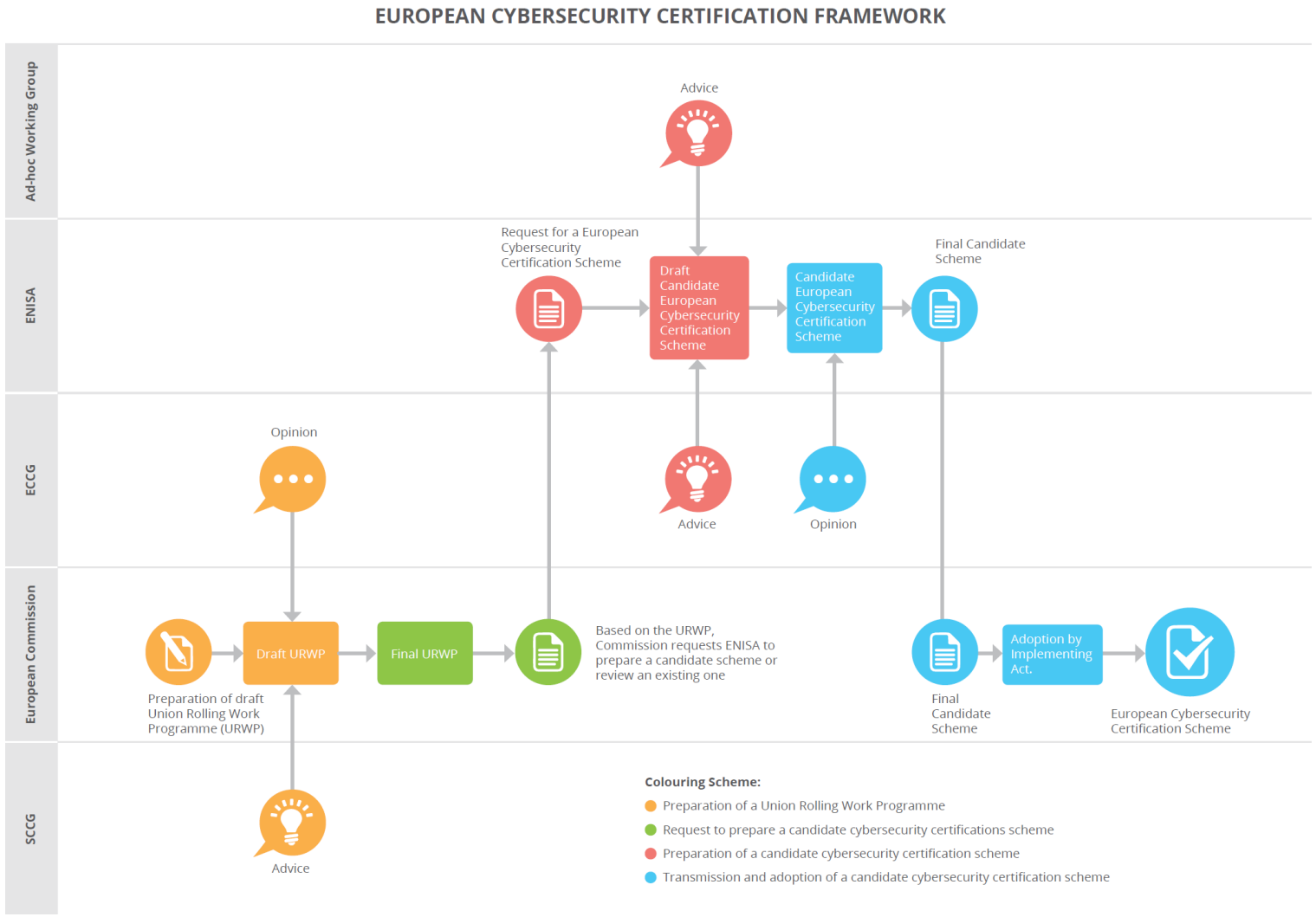
pean Union Agency for Cybersecurit
nology cybersecurity certification and
No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

Certification framework: *Roles*

Ad-hoc working group	• Representatives of the community, invited by ENISA ED • Advises ENISA while preparing a specific candidate scheme
ENISA	• In charge of drafting candidate schemes • Leads the preparation work
ECCG	• European Cybersecurity Certification Group • Representatives of the Member States (National Authorities) • Member States implement schemes
European Commission	• Coordinates the work on schemes through requests to ENISA • Implementing acts related to the candidate schemes • Manages comitology
SCCG	• Stakeholders Cybersecurity Certification Group • Representatives of the community, advises on work programme

Stakeholders' interactions



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Ad hoc WG on SOG-IS MRA Successor Certification Scheme Kick off meeting

Philippe Blot
Data security and standardisation Unit, AhWG Chair

AhWG Kick off Meeting

11 | 2019

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CLOUD SERVICES AD HOC WORKING GROUP *KICK-OFF MEETING*

ENISA Certification Team

05 | 03 | 2020

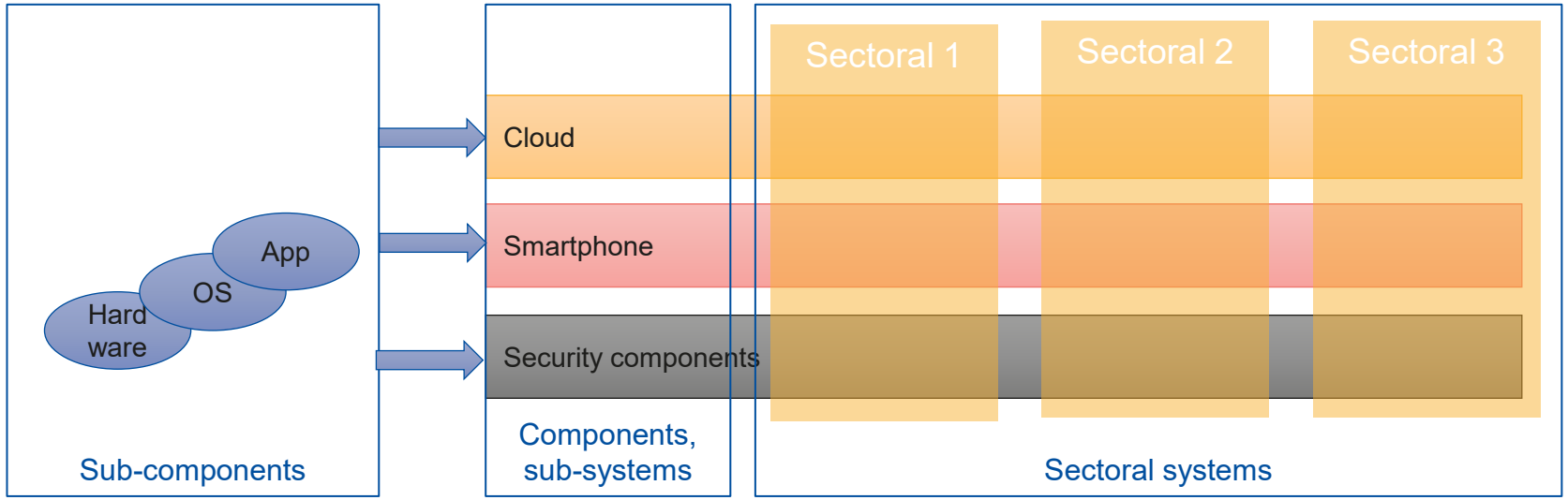
Synergies across horizontal and sectoral schemes

Sectoral schemes benefit from a broad availability of certified components

- Reduces effort for scheme development and evaluation/certification
- Minimizes vendor's cost to address the new market

Consequence:

- Key components should be covered first by PP / certification schemes



Challenges and opportunities for the implementation

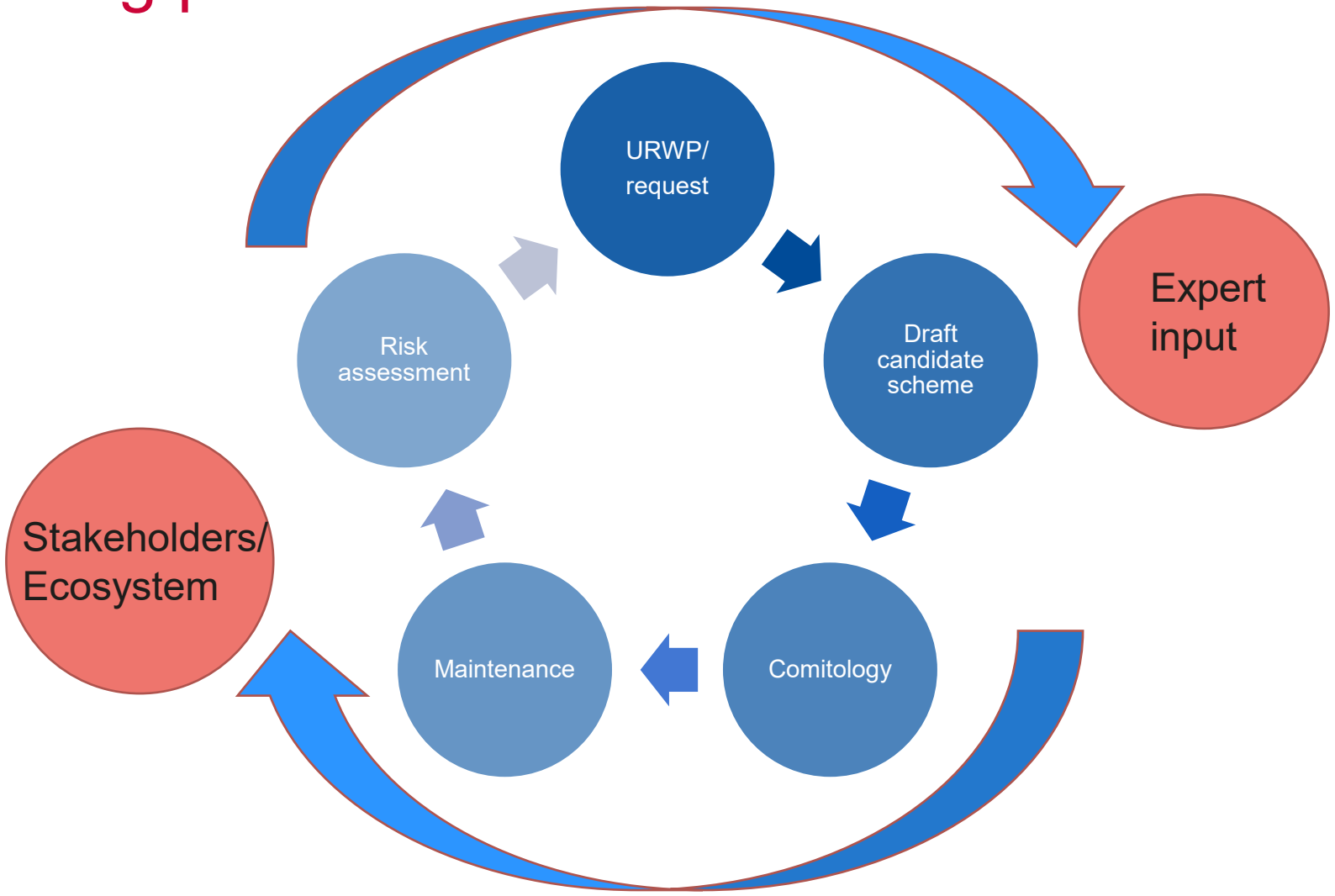
New investment to meet the challenges of the framework
New competition conditions with new entrants in the area of the TIC members

Broader market scope
Public procurement opportunities
Know how and new entrants in the market

Niche opportunities in relation to assembly and distribution

Public interest needs to be defined, quantified and taken into account

Getting the big picture



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

Vasilissis Sofias Str 1, Maroussi 151 24

Attiki, Greece

- +30 28 14 40 9711
- info@enisa.europa.eu
- www.enisa.europa.eu

TIC Council Webinar

Implementation opportunities and challenges of the European Cybersecurity Act

18th June, 2020

INFOCLASS: RESTRICTED
TLP: AMBER

DIGITAL TRUST SERVICES

WHEN YOU NEED TO BE SURE

SGS

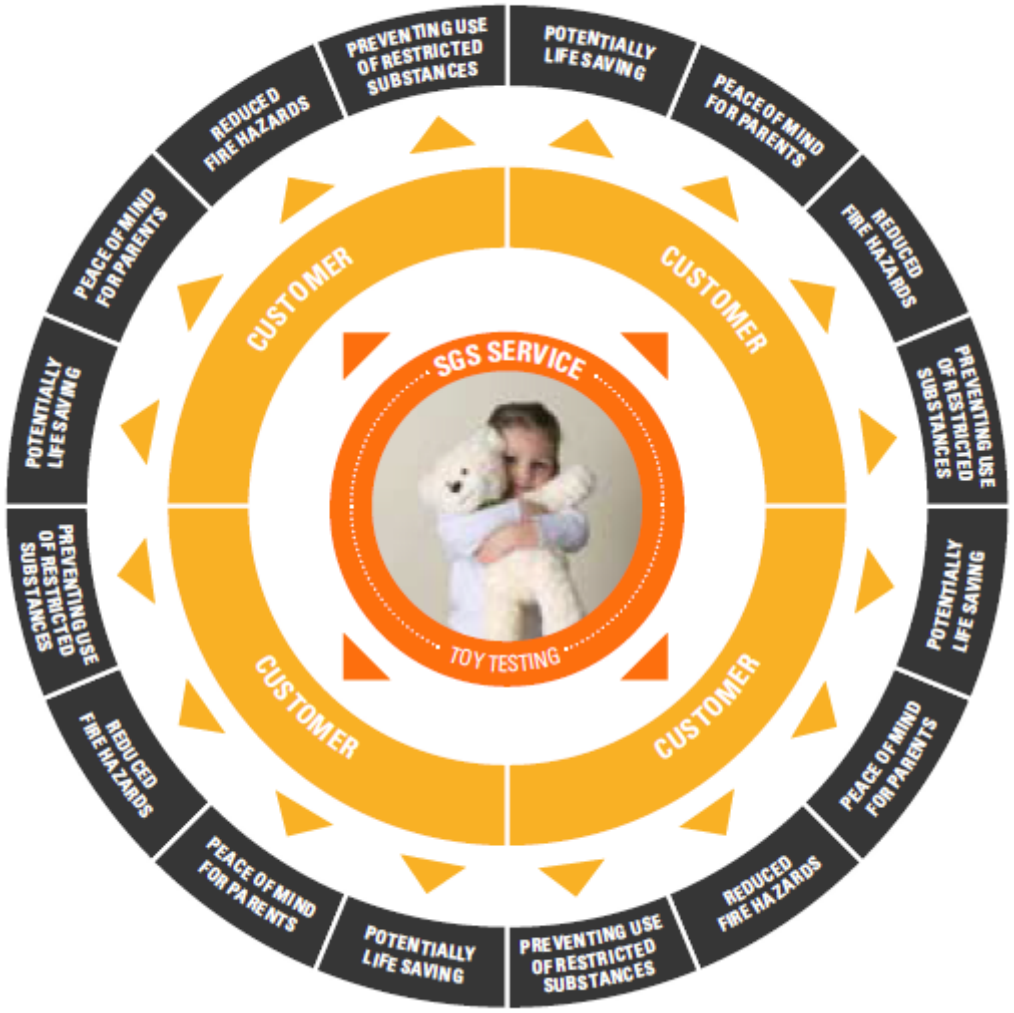
TIC VALUE TO SOCIETY

OUR SERVICES
INSPECTION
TESTING
VERIFICATION
CERTIFICATION
TRAINING
CONSULTANCY
OUTSOURCING
ANALYTICS

OUR BENEFITS
QUALITY
SAFETY
REDUCED RISK
EFFICIENCY
PRODUCTIVITY
SPEED TO MARKET
TRUST
SUSTAINABILITY

Our services bring a tremendous amount of value to society by helping our customers to be more efficient and productive while improving safety and achieving their sustainability objectives.
Our customers therefore create a multiplier effect of our value to society

EXAMPLE MULTIPLIER EFFECT OF OUR SERVICES



OUR STAKEHOLDERS

We create value to society for and through our stakeholders

EMPLOYEES AND SUPPLIERS
We add value to our employees by offering them training, nurturing their potential and encouraging them to work across multiple functions and geographies during their careers. We offer our suppliers financial strength that adds stability to their businesses and brings indirect benefits to society.

INVESTORS
We create value for our investors by being a robust, sustainable business with a 140-year track record. Our transparency, strong leadership and commitment to long-term sustainability make us a sound investment.

CUSTOMERS
We provide our customers with leading services, which helps make their businesses more efficient, profitable and sustainable. This value is passed on to society in the form of job security for employees, higher quality products and better environmental management.

GOVERNMENTS AND INDUSTRIES
We add value to the industries we operate in by driving supply chain innovation. We also provide services that directly support governments around the world being a key element on conformity assessment schemes

CONSUMERS
Consumers benefit from the services we provide our customers because they are able to trust the products and services they buy. From a product's quality and safety to its authenticity, our services help protect consumers.

COMMUNITIES AND THE PLANET
We help nurture the communities we operate in and strongly support disaster relief efforts. Our sustainability endeavors are recognized as being among the very best – both regionally and in the TIC industry. Through our services and operations, we attempt to protect our planet and its limited resources.

WHY IS ALL SO COMPLEX?

Software creator

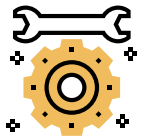
- Their product cannot be certified in the end of the manufacturing so they need strategies to certify while creating the software.
- They don't control in which hardware the software will run all time.
- Connected software need permanent patching and updates, to be sure no flaws are present. Only way to achieve that is performing regular checks.
- They can receive reputational damage.
- They are market segment dependent.

Corporate User

- They are learning the cybersecurity risks while being impacted (reactive).
- Largely exposed to hackers and malicious user that use the existing flaws on subcomponents, devices, software, communications, cloud and digital services.
- They need to demonstrate robustness of their IT systems and cybersecurity and data management.
- They activities, while not digital, are impacted by cybersecurity and reputational damage.
- They are segment oriented.

Governments

- Moved by consumers motivations.
- Concerned by industry protection and strategic considerations.
- Conformity assessment oriented.
- They are themselves target for attacks.
- They are market segment agnostic.



Manufacturer of a subcomponent

- Don't know is which device the subcomponent is going to be use.
- They represent the worst case scenario in any vulnerability, since they use to be impossible to fix after market.
- They don't use to receive reputational damage.
- They are market segment agnostic.

Manufacturer of a device

- Receives a lot of subcomponents from different suppliers.
- Certification is problematic, since they don't receive all info from subcomponents. Complex devices can only be certified based on subcomponents certified.
- They need to have cybersecurity on their factories to avoid installing malware on their devices during manufacturing (OT Robustness).
- They need to have certified processes of manufacturing to evidence they handle properly the life cycle.
- They receive the reputational damage.
- They are market segment oriented.

Provider of Communications & Cloud/Digital based services

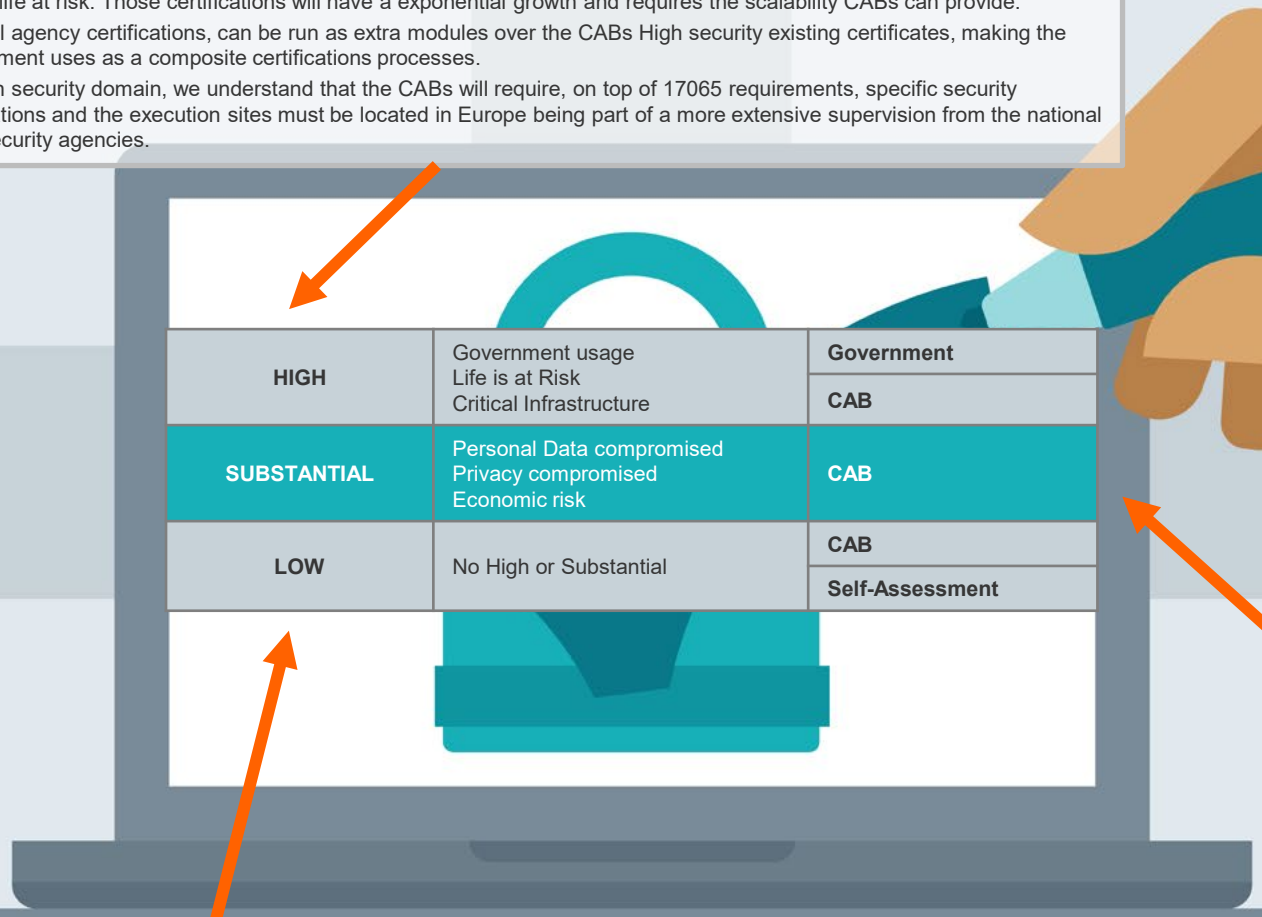
- They provide hosting, computing, communications and storage for a number of ecosystems of connected devices.
- They cannot warrantee all devices connected neither all software running under those, is cybersecure.
- They receive the reputational damage.
- They are market segment agnostic.

Consumers

- Moved by privacy and data security concerns.
- Highly unaware of how to protect himself, looks to buy cybersecurity on products, software's and services.
- They are market segment agnostic.

RISK LEVEL AND CAB INVOLVEMENT

- We consider that on high security level, the certification must also be done by a CAB in order to be compliant with EU regulation 765.
- We understand the need that any EU Government may have the interest to protect certain aspects of national sovereign in terms of retain the capability on Cybersecurity testing by its own.
- We believe that both realities can coexist if the following questions are considered:
  - A national agency, having the required skills, can perform the certification, for those products government/security/defense sensitive for their country.
  - A national agency, not having the skills, can rely on a trusted CAB to perform same process on its country.
  - High security domain is also needed on certain activities, that beside industry driven, can be on the critical infrastructures or put the life at risk. Those certifications will have a exponential growth and requires the scalability CABs can provide.
  - National agency certifications, can be run as extra modules over the CABs High security existing certificates, making the Government uses as a composite certifications processes.
  - For high security domain, we understand that the CABs will require, on top of 17065 requirements, specific security certifications and the execution sites must be located in Europe being part of a more extensive supervision from the national cybersecurity agencies.



HIGH	Government usage Life is at Risk Critical Infrastructure	**Government** **CAB**
SUBSTANTIAL	Personal Data compromised Privacy compromised Economic risk	**CAB**
LOW	No High or Substantial	**CAB** **Self-Assessment**

- We consider that on substantial, the CABs will play the role of performing the whole certification.
- Substantial level, depending on the use cases finally foreseen around this level, could be also limited to testing to be perform on European territory.
- The systematic around the Accreditation process, will follow completely the Regulation 765 prescriptions.

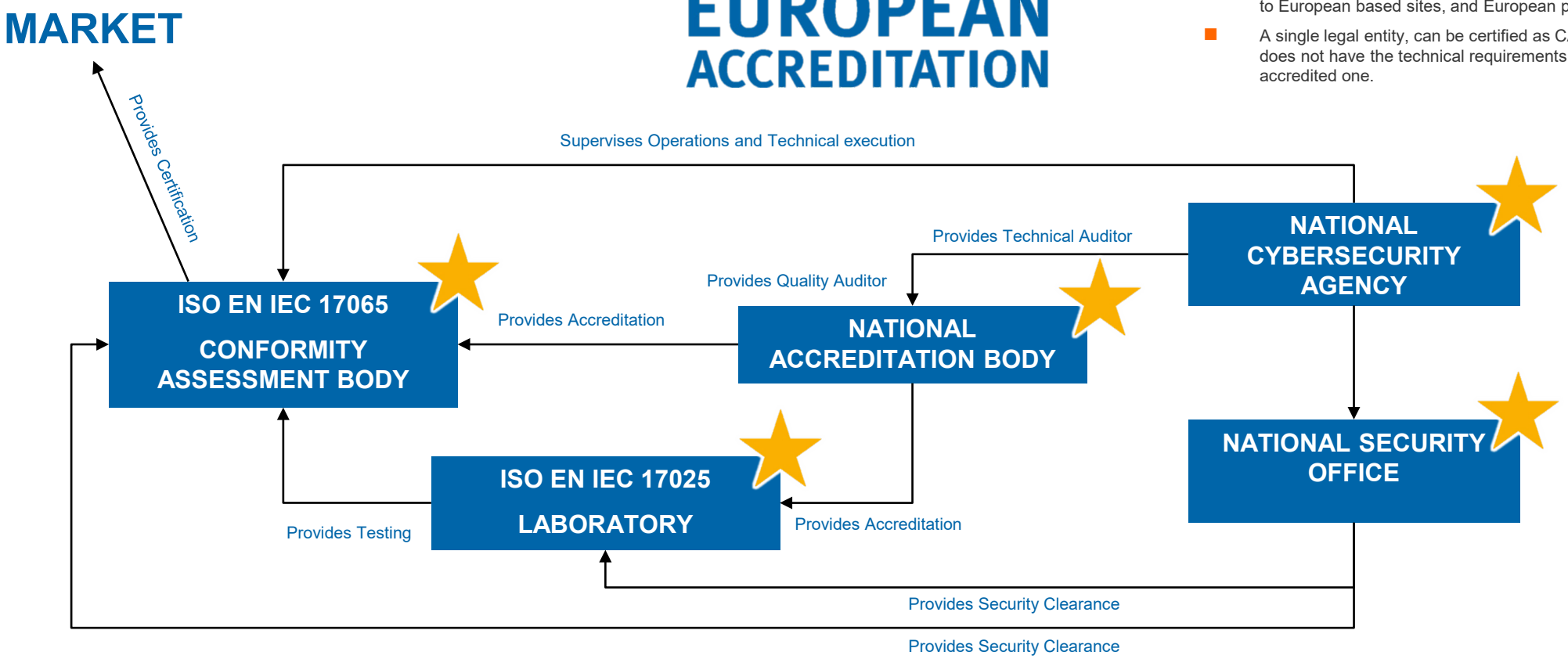
- For the low level, and based on existing experience on other schemes, market driven, will be two processes:
  - CAB: a manufacturer, request a type approval, for a specific product.
  - Self Assessment: a company, with a management certificate of cybersecurity of their manufacturing process, is able to generate their own certificates for their products.

HOW WE PROPOSE TO ACCREDIT?

The usual set up of recognized Accreditation process under the regulation 765 is the one to be used for the Cybersecurity Act. The process needs to be streamlined to be able to handle complexities of the cybersecurity.

EUROPEAN ACCREDITATION

- Not all National Security agencies can deliver Technical auditors for all levels.
- A National Accreditation Body of a Member State, can request support from a National Cybersecurity Agency from a third EU Country with the required skills.
- Any Conformity Assessment Body and Laboratory, must have (depending of the risk level he is applying for):
  - Company Security Clearance
  - Site Security Clearance (1 per site)
  - Personnel security Clearance (all personnel involved on operations).
- Security Clearance requirements, it's the most easy process to limit the activity to European based sites, and European personnel depending on the level.
- A single legal entity, can be certified as CAB and Laboratory. Incase a CAB does not have the technical requirements, they must use the test results from a accredited one.



- ISO EN IEC 17065 accreditation is per risk level.
- ISO EN IEC 17025 Accreditation is per standard and risk level

WHAT STANDARDS TO BE USED?

SGS POSITION

RISK	USAGE	CERTIFICATE ISSUED	SECURITY CLEARANCE	STANDARD	
HIGH	Government usage Life is at Risk Critical Infrastructure	Government CAB	Yes, min EU secret equivalent	Common Criteria (or ISO IEC 15408 compliant)	
SUBSTANTIAL	Personal Data compromised Privacy compromised Economic risk	CAB	Yes, min EU confidential	LINCE/BZG/CSPN	Common Criteria (or ISO IEC 15408 compliant)
LOW	No High or Substantial	CAB	Not required	LINCE/BZG/CSPN	
		Self-Assessment	Not required	IEC 62443 or ISO EN IEC 27032	

- We believe that an excessive number of vertical specific standards to be considered within the Cybersecurity Act should be avoided due to significant overlaps of requirements, methodologies, but also components covered.
- We are vertical agnostic, and we believe that we need to have less standards, covering standardization needs horizontally instead of vertically. Sub component manufacturers cannot have the view of where a certain product ends up, so standards need to consider this real world situation.
- Complex products will require to be built on top of certified components and sub components. A layered and modular approach is required starting on semiconductor level with strong security architectures implemented delivering strong certified trust anchors, that can be leveraged up to system level having appropriate certification schemes per integration step.

COMMON CRITERIA

- Common Criteria (or ISO IEC 15408 compliant) can be used for high or substantial.
- To handle more vertical specifics, we only need to work on more Protection Profiles
- Usage of Common Criteria needs to get tailored towards use cases
- More flexibility required in regards to re-use of evidence (e.g. during compositions)

LINCE/BSZ/CSPN

- Merge all basic European certification schemes into one standard.
- Get recognized by CEN CENELEC as one EN standard allowing it to be used as per Regulation 765 (Conformity Assessment Schemes can only use standards maintained or recognized by CEN CENELEC or ETSI as the only two European standardization bodies)
- Develop set ups per required vertical
- Incorporate composition model (seamless bottom up)
- Recognition program for certified components/sub-components (fragmented)

LOW RISK

- If it's a certification process based on module G of Decision 768 (specimen testing), the LINCE/BZG/CSPN will be used.
- If it's a self assessment, can be based on a company that holds a IEC 62443 or ISO EN IEC 27032 certificate.

CONCLUSIONS

- We need to have less number of standards, but able to be use in several verticals and product families.
  - Having different requirements in different EU regulations can create confusion and lack of interoperability.
  - Sectorial standards and proprietary ones, can create fragmentation and be misleading in regards the security attributes of any device.
- TIC Industry can play a role, helping regulators and member states to have the scalability to handle demand at global level.
  - Accreditation and Security controls, will be needed in the certification entity to be able to issue certificates.
  - Time to market, will be paramount to have a global reach. TIC sector can help on this, with the experience on other fields, where same constrains are face.

THANKS

For more questions:

DIGITALTRUSTSERVICES@SGS.COM

DIGITAL TRUST SERVICES

WHEN YOU NEED TO BE SURE

SGS

Follow us online

@TICCouncil

TIC Council

Wikipedia page:
Testing, inspection and certification

TIC-Council.org