RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PART1-T11**

TeleTrusT: The European Cybersecurity Act and its impact on US companies

MODERATOR: **Prof. Dr. Norbert Pohlmann**
Director of the **Institute for Internet Security - if(is)** /
Chairman of **IT Security Association Germany - TeleTrusT**

PANELISTS: **Dr. Steve Purser,**
Head of Core Operation Department,
European Union Agency for
Cybersecurity (**ENISA**)

Matthias Intemann
Certification of Software/COTS Prod.,
Federal Office for Information
Security (**BSI**)

Sergio Lomban
VP Trust Services, **SGS**
Société Générale de Surveillance SA

Positioning ENISA's Activities

1

RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

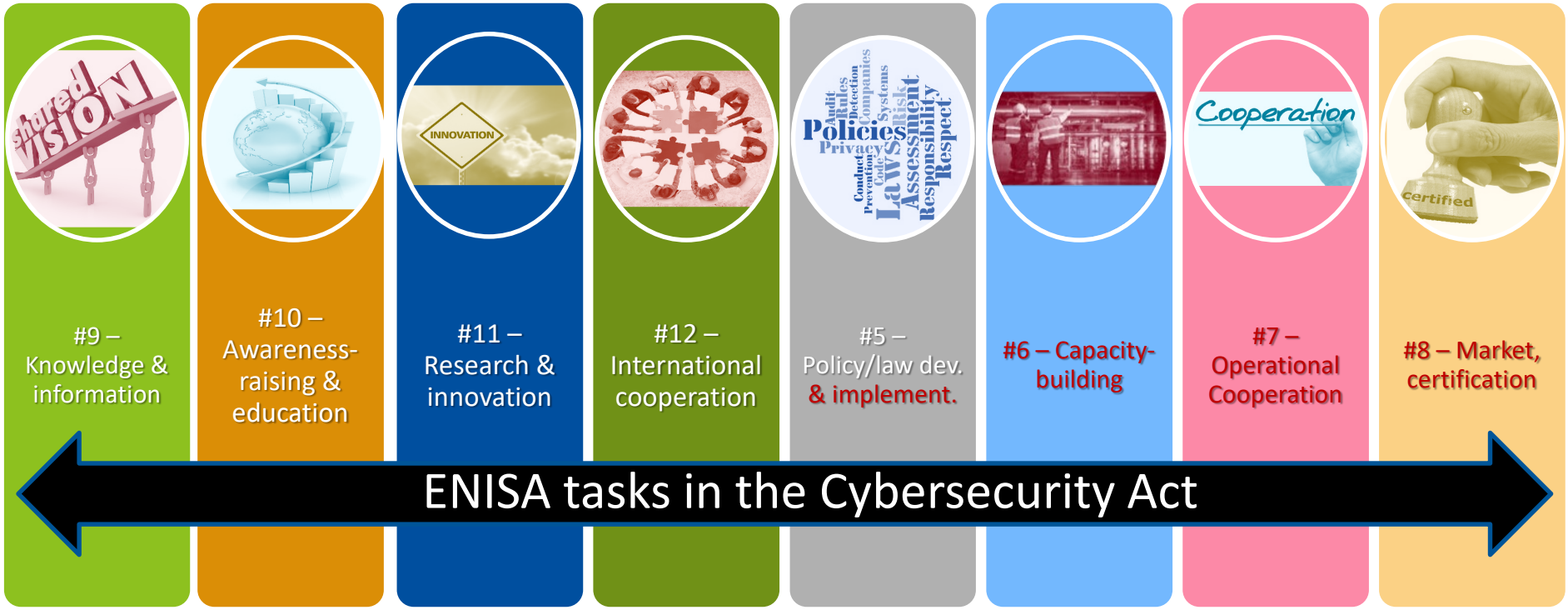
2

SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3

'HANDS-ON' WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE

The Cybersecurity Act (CSA) tasks



Cybersecurity Certification Framework

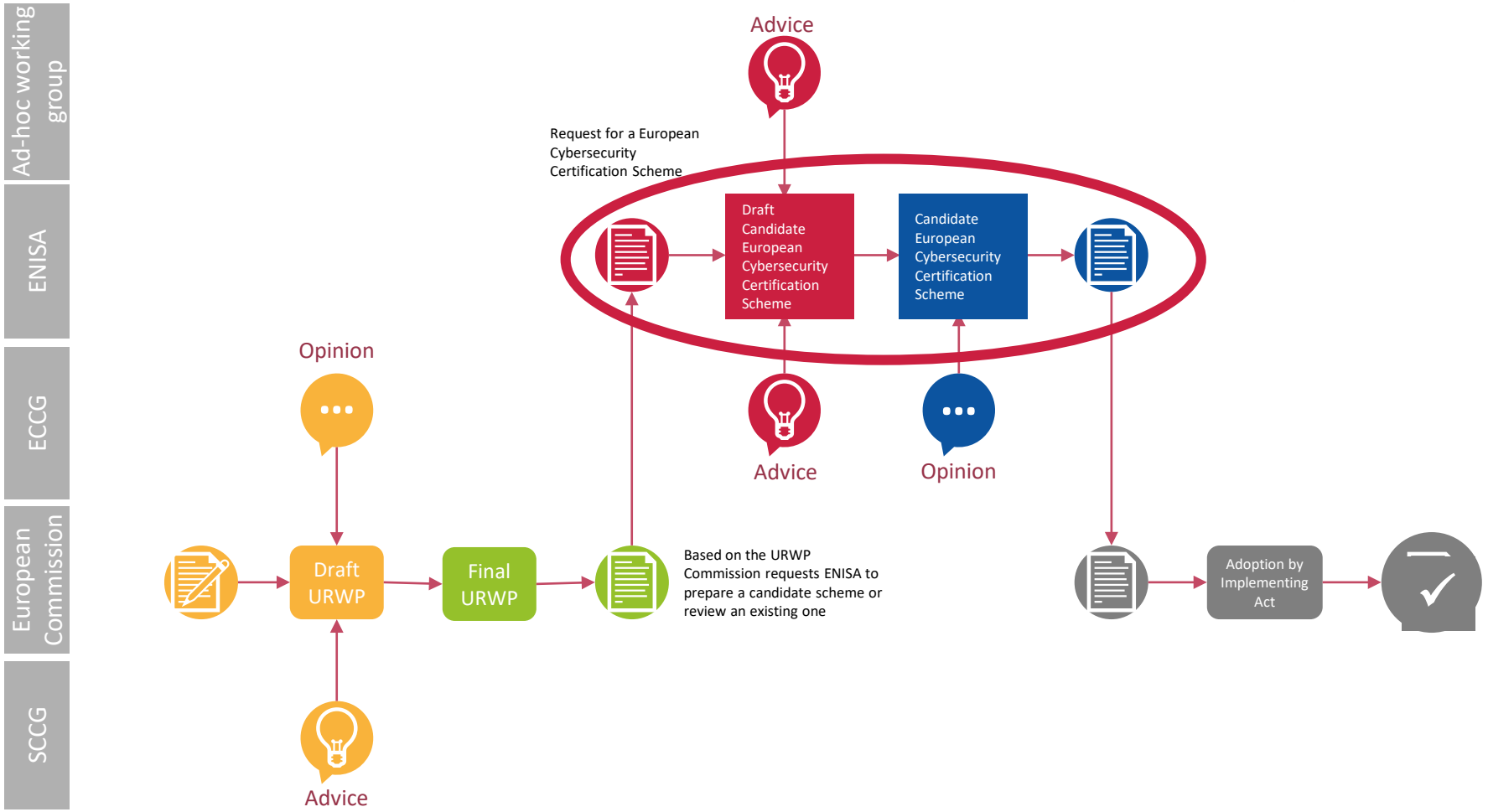
- **Addresses market fragmentation**
  - Products, services, processes
- **Presents a voluntary and risk-based approach**
- **Defined assurance levels** (Basic, Substantial, High)
- **Role for Member States**
  - Propose preparation of a candidate scheme
  - Involvement through European Cybersecurity Certification Group (composed of national certification supervisory authorities)
  - Involved in the procedure for adoption of an implementing act
- **Clear separation of tasks in line with Regulation (EU) 765/2008**
- **First request (transposition of SOGIS-MRA) received June 2019**

ENISA & the EU Cybersecurity Certification Framework

- **Prepare candidate schemes or review existing ones, on the basis of**
  - Rolling Work Program (RWP)
- **Maintain a dedicated website providing information on**
  - EU cybersecurity certification schemes
  - National certification schemes replaced by EU ones
  - A store of EU statements of conformance
- **Additionally, potentially provide guidance on such areas as**
  - Conformity self assessment
  - Cybersecurity information for certified products, services and processes
- **Project on requirements for an IT system to support ENISA's task in EU Certification Framework – concluded in August 2019**
  - Report on technical specifications
  - Report on functional and non-functional requirements

Certification Scheme

Preparation Process



EU Member state Tasks

NCCA

„National Cybersecurity Certification Authority“

- **Designated by Member State** to be responsible for **supervision** and **enforcement** according to CSA
- Handle **complaints** and impose **penalties**
- Support national **accreditation** body
- **Independent** of the entities it supervises
- Participate to and cooperate in **ECCG**

NCCA CB

- Issues certificates for assurance level „high“
- Subject matter expert

Standardization of Scheme Evaluation Methodologies

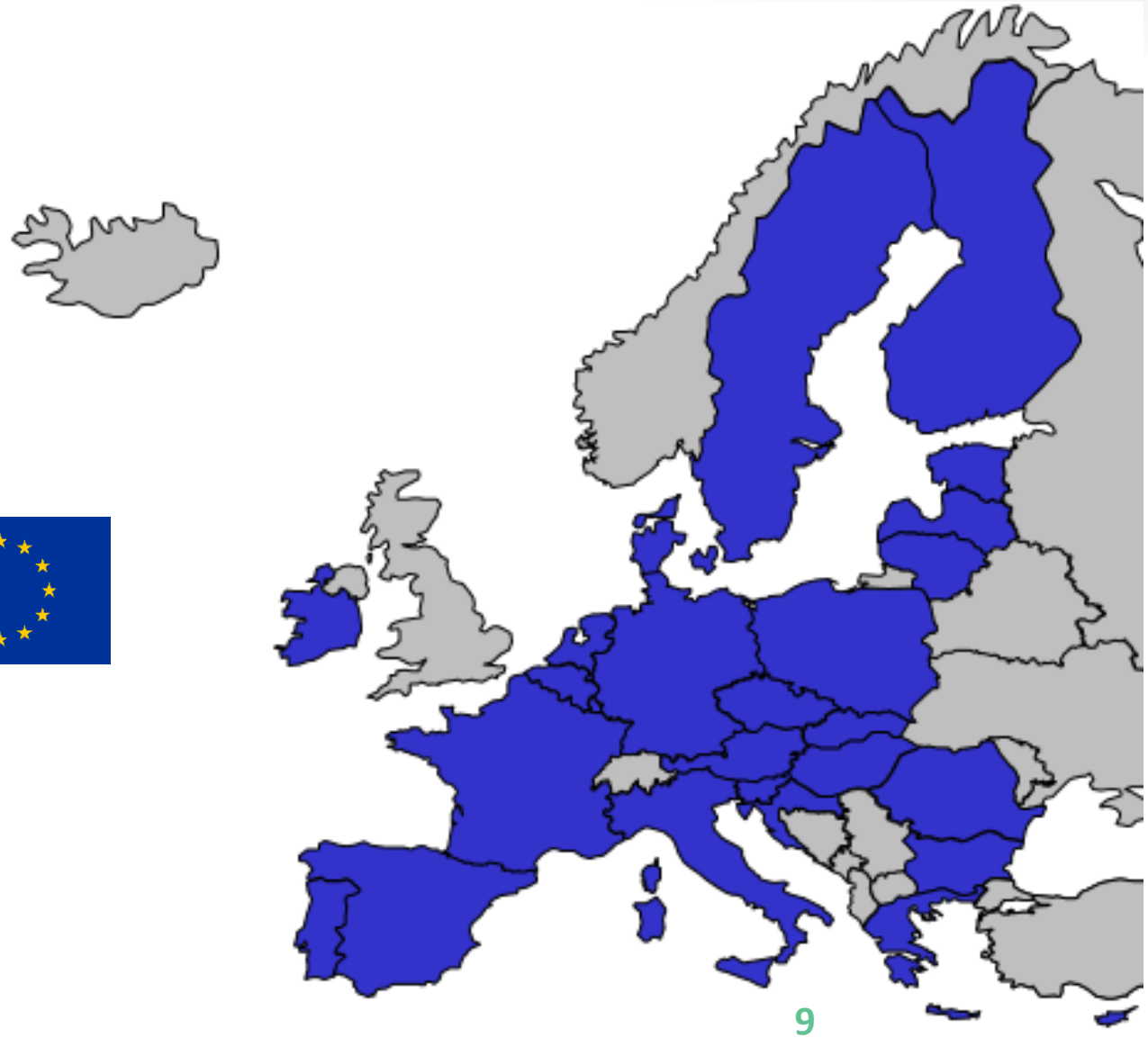
European Standardisation Organisation

- Definition of generic Security Requirements
- Generic standard on Evaluation Methodology
- Definition of Interface to Certification

European Legislation

- Scheme Formalities
- Competence Requirements for CAB
- Scheme Refinements of Methodology, e.g. on Crypto Assessment
- Mutual Recognition with third parties

EU Member States



What You Have Learned Today

- **The EU** supported by its agency **"ENISA"** is implementing a comprehensive cybersecurity framework: **"European Cyber Security Act"**
- **Protecting** future IT systems - from **critical infrastructures** to any **consumer's IoT device** in all sectors
- **Europe increases the level of IT security requirements for any vendor** who wants to offer his products and solutions on **EU markets**.

Visit the German Pavilion at North Expo Hall, Booth 5671

The partners of the German Pavilion at RSA® Conference 2020

achelos the experts in eID
Avira
betasystems
bdr BUNDESDRUCKEREI
comforte
cryptoVision
Cryptshare
digitronic net Specialist for data security & strong 2-factor-authentication
DriveLock
eco ASSOCIATION OF THE INTERNET INDUSTRY
G DATA
genua A Bundesdruckerei Company
HORNETSECURITY
IFASEC
infodas
itWatch GmbH
MATRIX42
MB CONNECT LINE remote maintenance solutions
MTG
QuoScient
ROHDE&SCHWARZ Cybersecurity
boxcryptor
secunet
SoSafe Cyber Security Awareness
T
TÜVIT TÜV NORD GROUP