ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

POLICIES & STRATEGIES

CERTIFICATION FRAMEWORKS

DATA PROTECTION

SECURITY CHALLENGES

5G, eSIM IoT, AI

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

THE EU CYBERSECURITY AGENCY

Toward a European Certification Framework

Eric VETILLARD
Lead Certification Expert

28 | 02 | 2020

SECURITY CERTIFICATION IN EUROPE

LINCE CSPN BSZ

MISSION OF ENISA

To contribute to the emerging EU framework for the certification of products, services and processes

To draw up **certification schemes in line with the Cybersecurity Act** providing stakeholders with a sound service that adds value to the EU while supporting the framework

Key outputs

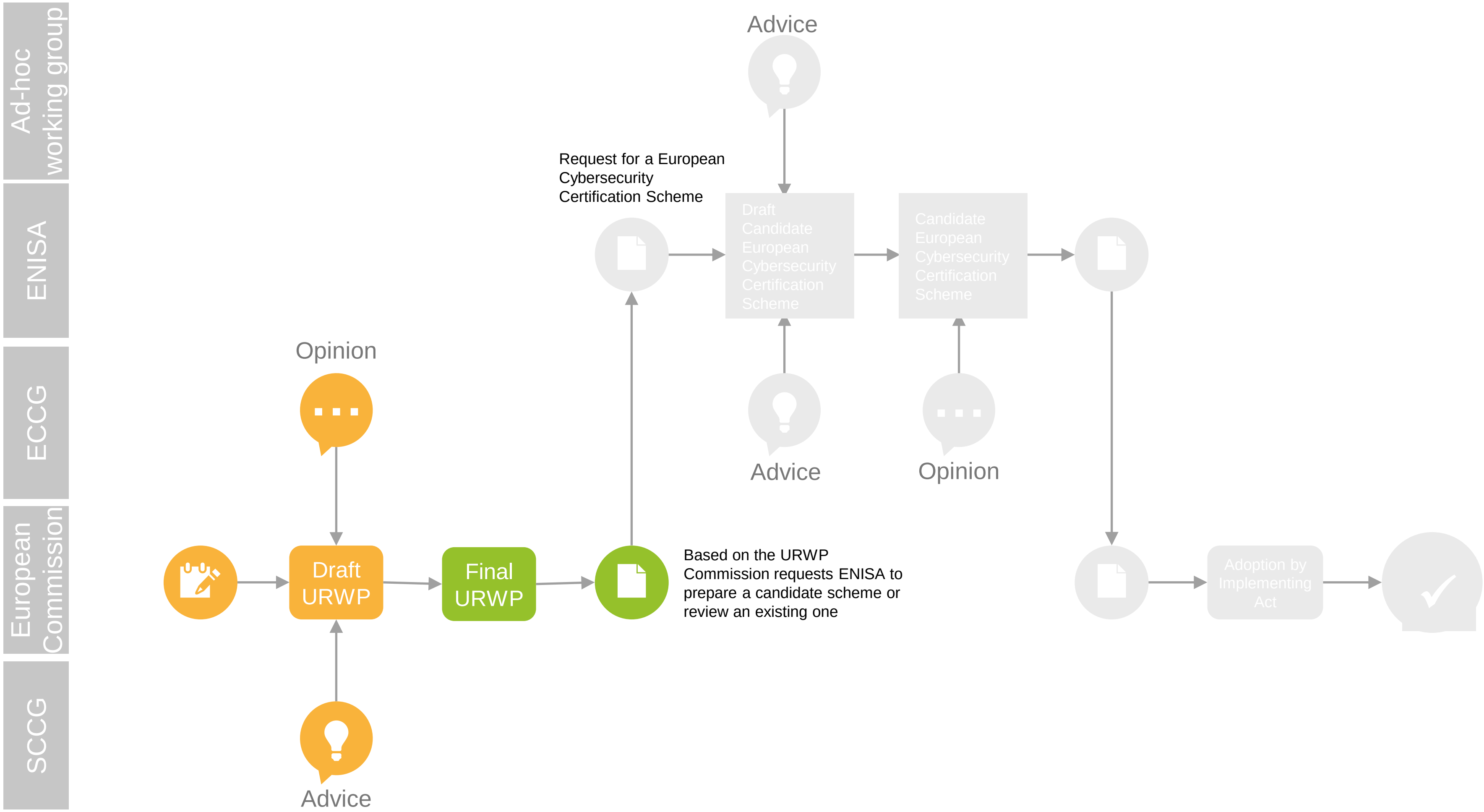
- Draft and finalised candidate certification schemes products, services and processes
- Secretariat support (SCCG) and Co-chair SCCG (w/ Commission)
- Support the Commission to Chair ECCG
- Support review of adopted certification schemes
- Implement and maintain CSCF public website
- Support peer review between national cybersecurity certification authorities
- Advice on market aspects relevant to cybersecurity certification

BUILDING A CERTIFICATION SCHEME

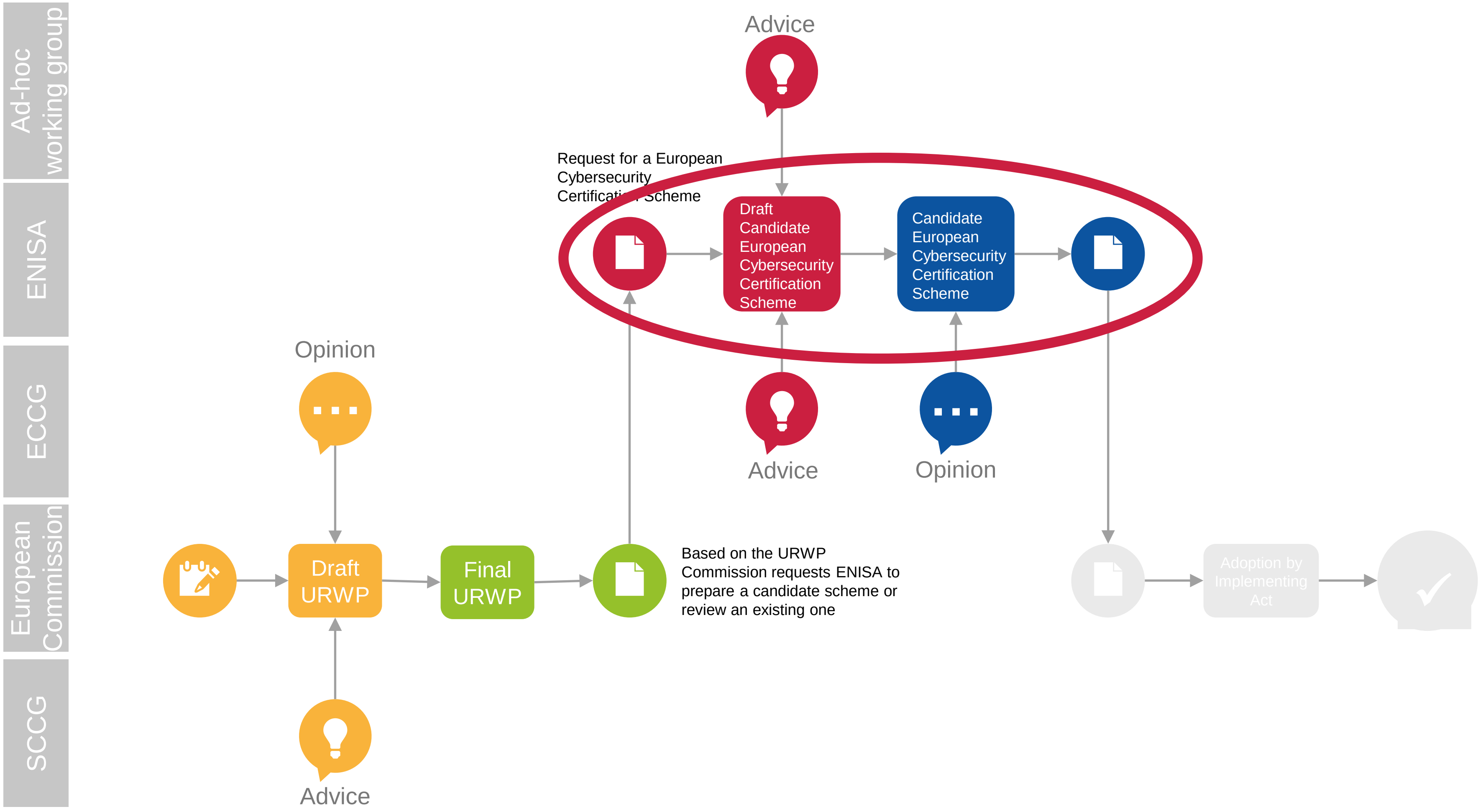
CERTIFICATION SCHEME
WHO'S WHO

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

CERTIFICATION SCHEME *PLANNING*


Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Opinion
Advice
Opinion
Draft URWP
Final URWP
Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one
Adoption by Implementing Act
Advice

CERTIFICATION SCHEME *PREPARATION PROCESS*


Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Opinion
Advice
Opinion
Draft URWP
Final URWP
Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one
Adoption by Implementing Act
Advice

WHAT IS IN A CYBERSECURITY CERTIFICATION SCHEME?

a. Subject matter and scope

b. Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme

c. References to the international, European or national standards applied in the evaluation, and if not available to technical specifications

d. One or more assurance levels

e. An indication whether conformity self-assessment is authorized

f. Specific requirements for the CABs

g. Specific evaluation criteria and methods to be used

h. The information necessary for the evaluation or otherwise to be made available by the applicant

i. If applicable, the conditions of use of marks and labels

j. Rules for monitoring compliance of certified and self-assessed products

NEW!

k. Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope

l. Rules concerning the consequences for products that have been certified or self-assessed and do not comply

m. Rules concerning how previously undetected vulnerabilities should be reported and handled

n. Rules concerning the retention of records by CABs

o. Identification of national and international schemes with the same scope

p. Content and format of the certificates and EU statements of conformity

q. The period of the availability of EU statements of conformity and related documentation

r. Maximum period of validity of certificates

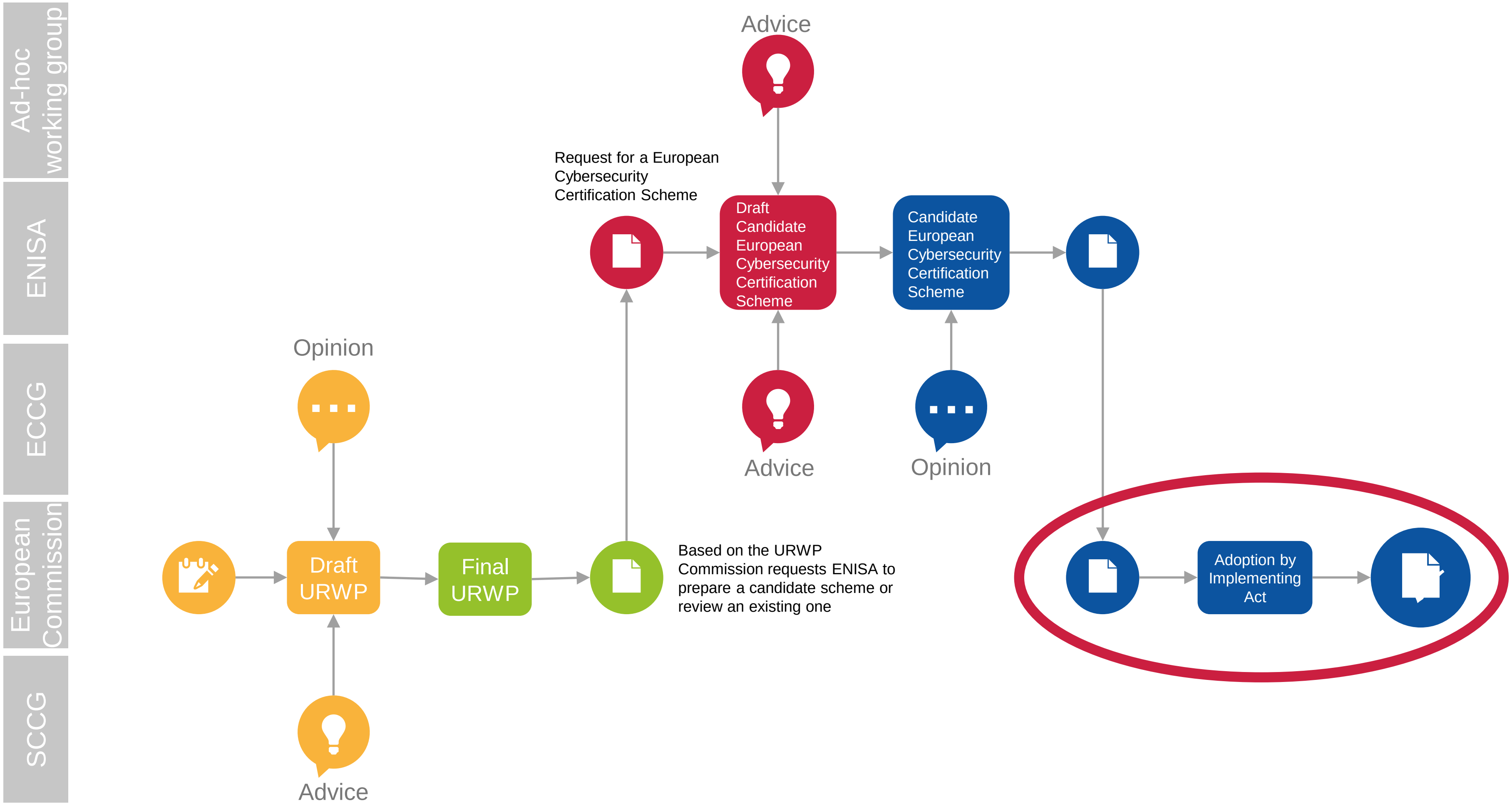
s. Disclosure policy for certificate issuance, withdrawal, amendment

t. Conditions for mutual recognition with third countries

u. Where applicable, rules for peer assessment

v. Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

MAKING THE SCHEME INTO LAW


Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Advice
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Opinion
Advice
Opinion
Draft URWP
Final URWP
Advice
Adoption by Implementing Act

Request for a European Cybersecurity Certification Scheme

Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one

ONGOING SCHEMES

TWO REQUESTS RECEIVED

Successor to SOG-IS

Request received in July, work has actively started

- Already two meetings of the ad hoc working group
- Third meeting on March 10-11

Cloud Services

Request received in November, work starting

- Ad hoc working group is ready
- Kick-off meeting on March 5-6

Successful Contributions

- Close to 200 applications to ad hoc working groups
- Strong member state participation in both groups

SOME CHALLENGES AHEAD

Successor to SOG-IS

Inheriting a long history and fitting it in a new framework

- Some aspects need to be revised
  - The Cybersecurity Act provides a rather detailed list of requirements
- For instance, continued assurance
  - Not a normal practice in the current SOG-IS world
  - Requires significant changes and in-depth discussions
- Also, the transition needs to be well prepared

Cloud Services

Building a fragmented space with no leading scheme

- No reference list of controls
  - A reference must be built
- Different assessment methodologies available
  - Also need to cohabit with other, related security assessments
- And, of course, the Cybersecurity Act requirements
  - Continued assurance, transition, levels, self-assessment

ABOUT SCHEMES
3 ASSURANCE LEVELS

a. Subject matter and scope

b. Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme

c. References to the international, European or national standards applied in the evaluation, and if not available to technical specifications

d. One or more assurance levels

e. An indication whether conformity self-assessment is authorized

f. Specific requirements for the CABs

g. Specific evaluation criteria and methods to be used

h. The information necessary for the evaluation or otherwise to be made available by the applicant

i. If applicable, the conditions of use of marks and labels

j. Rules for monitoring compliance of certified and self-assessed products

k. Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope

l. Rules concerning the consequences for products that have been certified or self-assessed and do not comply

m. Rules concerning how previously undetected vulnerabilities should be reported and handled

n. Rules concerning the retention of records by CABs

o. Identification of national and international schemes with the same scope

p. Content and format of the certificates and EU statements of conformity

q. The period of the availability of EU statements of conformity and related documentation

r. Maximum period of validity of certificates

s. Disclosure policy for certificate issuance, withdrawal, amendment

t. Conditions for mutual recognition with third countries

u. Where applicable, rules for peer assessment

v. Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

FROM BASIC TO HIGH

	Basic	Substantial	High
Review of technical documentation	Mandatory		
Review to demonstrate the absence of publicly known vulnerabilities		Mandatory	Mandatory
Review to demonstrate the correct implementation of the security functionalities		Mandatory	Mandatory
Review to demonstrate the correct implementation of the security functionalities *at the state-of-the-art*			Mandatory
Assessment of resistance to skilled attackers through penetration testing			Mandatory
Self-assessment and EU statement of conformity	Optional	Forbidden	Forbidden

Requirements from the Cybersecurity Act

FROM BASIC TO HIGH

	Basic	Substantial	High
Review of technical documentation	Mandatory	**Implicit?**	**Implicit?**
Review to demonstrate the absence of publicly known vulnerabilities	**Optional**	Mandatory	Mandatory
Review to demonstrate the correct implementation of the security functionalities	**Optional**	Mandatory	Mandatory
Review to demonstrate the correct implementation of the security functionalities *at the state-of-the-art*	**Optional**	**Optional**	Mandatory
Assessment of resistance to skilled attackers through penetration testing	**Optional**	**Optional**	Mandatory
Self-assessment and EU statement of conformity	Optional	Forbidden	Forbidden

INTENTION

RESISTANCE
RESILIENCE

Requirements from the Cybersecurity Act

CORRECTNESS
EFFECTIVENESS

A FRAMEWORK IN THE BUILDING

We are in the very first steps of the framework, and there is much more to come

The Union Rolling Work Programme is expected in June.

- Drafting has started, the SCCG should hold its first meeting very soon.
- The first schemes will be available in 2021

The SOG-IS successor candidate should be delivered around June

- An Implementing Act could be finalized by the end of 2020
- The cloud services candidate should be available end of 2020

A first evaluation will come in 2023

- With questioning about regulation three years after starting a scheme

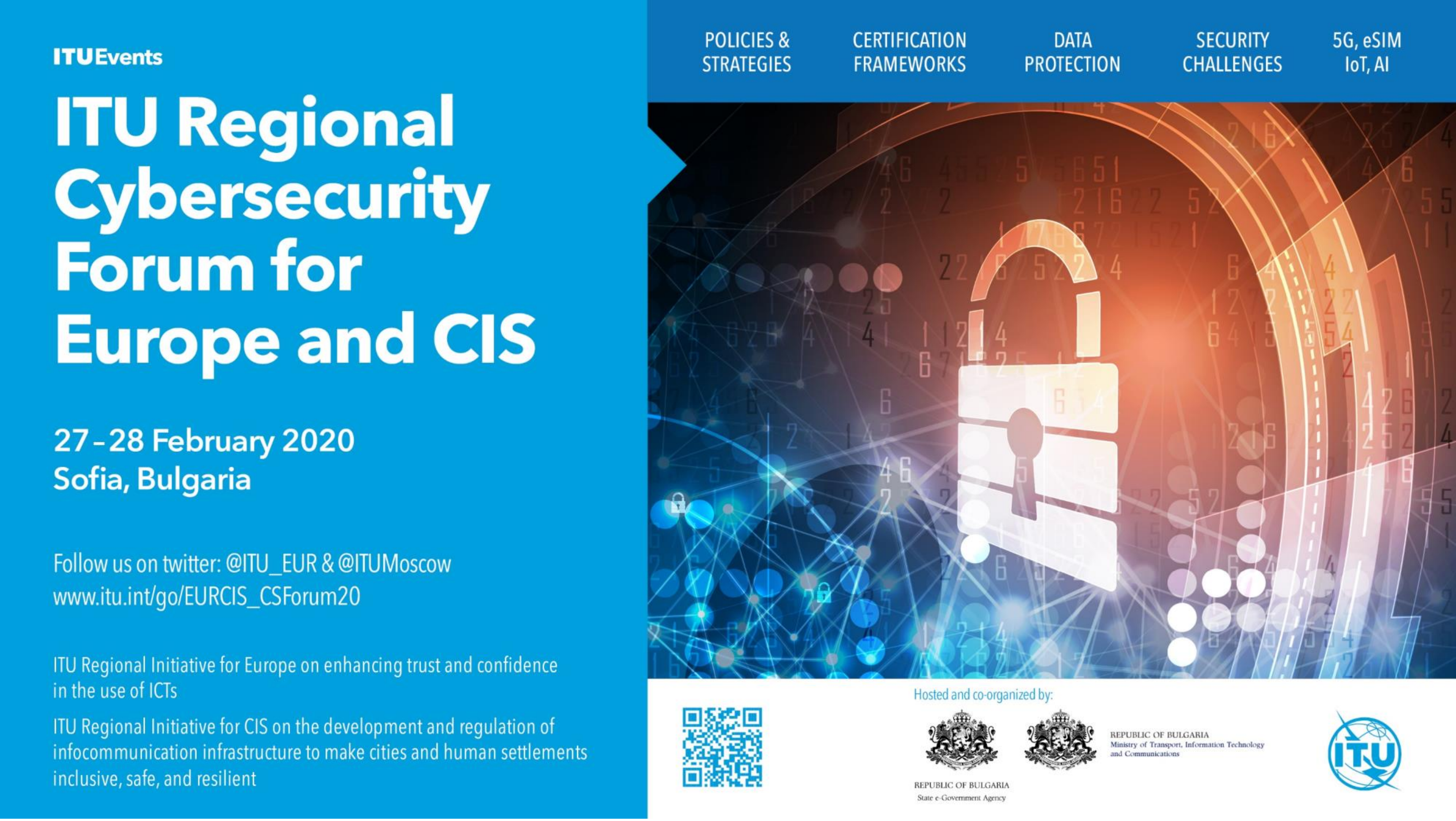
THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

📱 +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europe.eu



ITUEvents

ITU Regional Cybersecurity Forum for Europe and CIS

27–28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU