ENISA’s roles and functions under the NIS Directive

Art. 19 - incident reporting for trust service providers

Dr. Dan Tofan| NIS Expert

ENISA NLO Meeting | 8th June 2016

European Union Agency for Network and Information Security

Summary

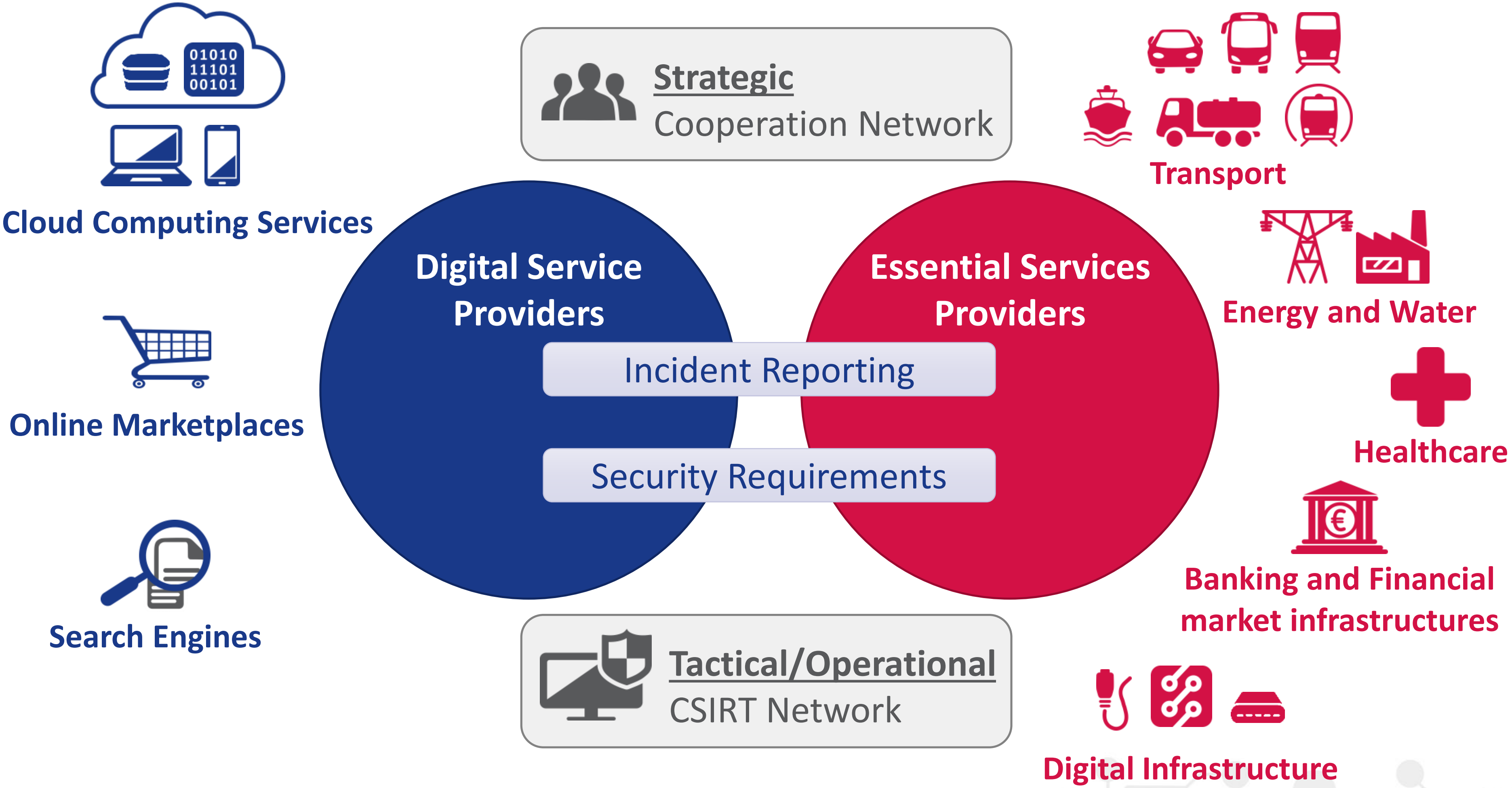
01 **About the NIS directive**

02 ENISA projects related to the NIS directive

03 Art. 19 – incident reporting for trust service providers

The NIS Directive

National Cyber Security Strategies



Strategic
Cooperation Network

Digital Service Providers

Essential Services Providers

Incident Reporting

Security Requirements

Tactical/Operational
CSIRT Network

Cloud Computing Services

Online Marketplaces

Search Engines

Transport

Energy and Water

Healthcare

Banking and Financial market infrastructures

Digital Infrastructure

NIS directive

Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

Status: EU Parliament and EU Council reached an agreement, possible adoption August 2016.

Provisions:

- Obligations for all MS to adopt a national NIS strategies and designate national authorities.
- Creates first EU cooperation group on NIS, from all MS.
- Creates a EU national CSIRTs network.
- Establishes security and notification requirements for operators of essential services (ESP) and digital service providers (DSP).

General role of ENISA

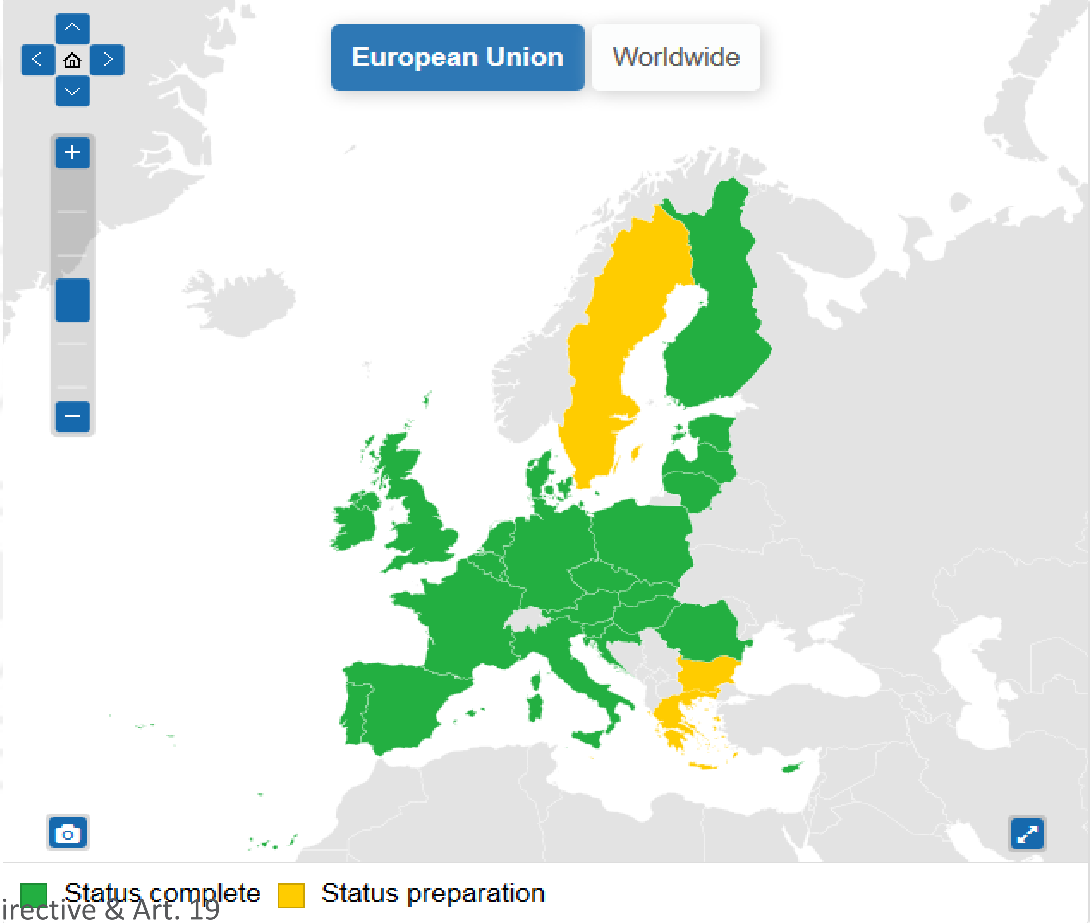
- Assistance for MS and the EU Comm by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance for MS in developing national NIS strategies.
- Participation within the EU NIS Cooperation Group.
- Support EU Comm in developing security and notification requirements for ESP and DSP.
- Assistance for MS in developing national CSIRTs.
- Elaborate advices and guidelines regarding standardization in NIS security, together with MS.

ENISA’s role in the Cooperation Group

- As part of the group, ENISA will directly support with:
  - exchange of best practices
  - capacity building in NIS
  - assistance in identification of ESPs
- Other tasks that fall within the group are:
  - provide strategic guidance for the activities of the CSIRT network
  - discuss modalities for reporting notifications of incidents
  - examine on an annual basis the incident summary reports
  - periodically review of the functioning of the Directive
  - discuss with representatives from the relevant European Standardisation Organisations, the standards referred to in the directive.

ENISA’s role in NIS strategies

- Work already done in this area, we will provide additional support if needed, for updating and improving NIS strategies.



ENISA's role in developing security and notification requirements

- Incident reporting schemes and minimum security measures are required by the directive for:
  - ESP (energy, transport, financial, health, water, digital) and
  - DSP (search engines, cloud computing, online market places).
- Based on previous experience (mandatory incident reporting in telecom) ENISA is already providing support to EU Comm in developing the implementing acts.

ENISA’s role in ESP

- ESPs (energy, transport, financial, health, water, digital) should report to the designated authorities incidents related to the security of their services and take appropriate security measures according to the level of risk.

- identification of ESPs devolves into the obligations of MS, ***but ENISA can assist within this process, as previous work has already been done in this area***.

- Future work is envisaged in this area, in ENISA WP2017 (Guidelines for identification of ESP, Guidelines for Incident reporting for ESP, Security measures for ESP).

ENISA’s role in DSP

- DSPs (search engines, cloud computing, online market places) are also imposed incident notification obligations and optional security measures.

- Within 1 year following the adoption of the NIS Directive, EC with ENISA, will develop two implementing acts to facilitate the uniform application of these obligations by MS across EU.

- Based on previous experiences ENISA will support EC with the following projects:

- Guidelines for incident reporting within the NIS directive (DSP)
- Security measures for DSPs in the context of NIS directive

ENISA’s role in standardization

- The NIS directive encourages the use of European or internationally accepted standards and/or specifications relevant to security of networks and information systems.

- ENISA, together with MS, shall elaborate advice and guidelines regarding standardization in NIS security.

National CSIRTs

(For easier reading we refer to national CSIRTs in the context of this presentation simply as "CSIRT" or "dedicated CSIRT".)

- **Article 7** of the Directive gives the framework for CSIRTs.
- **Article 8b** of the Directive covers the CSIRT Network.
- **Annex 1**. Requirements and tasks of the CSIRT. This Annex gives a list of tasks that a MS' CSIRT has to perform.
- **Annex 2**. Sectors and entities. This Annex lists the sectors and subsectors that need to be covered by each country's Information Security Strategy and CSIRTs.

CSIRT network (article 8b)

- Why (paragraph 1):
  - in order to developing confidence and trust between Member States
  - To promote swift and effective operational cooperation
- Composition (paragraph 2):
  - representatives of the Member States' CSIRTs
  - CERT-EU (CSIRT for EU institutions)
  - European Commission (as observer)
  - ENISA (secretariat and active support).
- Tasks (paragraph 3):
  - Exactly how the group will perform its tasks is up to the group itself, as stated by paragraph 5.
  - It means that the group will determine its own priorities, with input from the Collaboration Group.
  - ENISA will support the group by making appropriate proposals.
- Periodic review (paragraph 4):
  - The form and content of the report are not defined yet.
  - This will need to be negotiated between the CSIRT network and the cooperation group.
  - ENISA will help producing the report, and the group will have to approve it.
- Rules of procedures (paragraph 5):
  - The group will need to determine its governance structure and terms of reference.
  - ENISA, as secretary and support, can provide input to the group and come up with proposals.

Summary

01 NIS directive

02 **ENISA 2016 projects related to the NIS directive**

03 Art. 19 – incident reporting for trust service providers

NIS Directive related projects

1. Guidelines for implementing mandatory incident reporting for DSPs
2. Guidelines for implementing security requirements for DSPs

Incident reporting

1. Objective 1: Provide a comprehensive guideline to all stakeholders involved on how to implement incident reporting for DSPs.
2. Objective 2: Contribute to the IA on incident reporting (EU Comm)

Incident reporting – expected results

<DEFINING THE HOW/>

1. Incident reporting framework/model/workflow within the context of the NIS directive

<DEFINING THE WHAT/>

2. Identification of DSP’s and their services Incidents that fall under the NIS directive

<DEFINING THE WHEN/>

3. Parameters used to measure impact of incidents

4. Defining the significant impact

<DEFINING THE WHO/>

5. About national authorities

Incident reporting - approach

1. Desktop research
2. Survey with DSPs
3. Survey with national authorities
4. Validation workshop (approx. Sept.-Oct.)
5. + permanent collaboration with EC.
6. + participation in EC informal expert group
7. + participation in the Cooperation Group + CSIRTS network

Security requirements for DSPs

Scope

- Provide input to the MS to assist them in the implementation of the NIS Directive.

Objectives

- Define baseline security requirements for DSPs;
- Map the security objectives with ENISA's maturity levels* providing practices and evidences for each level of maturity.
- Map the identified security measures with well-known standards

* ENISA Maturity Levels	
Level 1	Security measures are implemented at an early stage
Level 2	Security measures are implemented according to industry standard
Level 3	Security measures are implemented in an advanced way and are monitored and tested on a regular basis

Methodology

- Validate CCSM security objectives with ENISA's cloud expert group.
- Identify additional security objectives through BSI C5, CSA OCF.
- Survey and interview online market places and search engines on their security objectives. Identify additional or lessen requirements based on CCSM.

Security objectives

SO1 Information Security Policy

SO2 Risk Management

SO3 Security Roles

SO4 Security in Supplier Relationships

SO5 Background checks

SO6 Security knowledge and Training

SO7 Personnel changes

SO8 Physical and Environmental Sec

SO9 Security of supporting utilities

SO10 Access control to NIS

SO11 Integrity of NIS

SO12 Operating procedures

SO13 Change management

SO14 Asset management

SO15 Security incident detection and response

SO16 Security incident reporting

SO17 Business continuity

SO18 Disaster recovery capabilities

SO19 Monitoring and logging policies

SO20 System test

SO21 Security assessments

SO22 Checking compliance

SO23 Cloud data security

SO24 Cloud interface security

SO 25 Cloud software security

SO 26 Cloud interoperability and portability

SO 27 Cloud monitoring and log access

Additional Security Measures

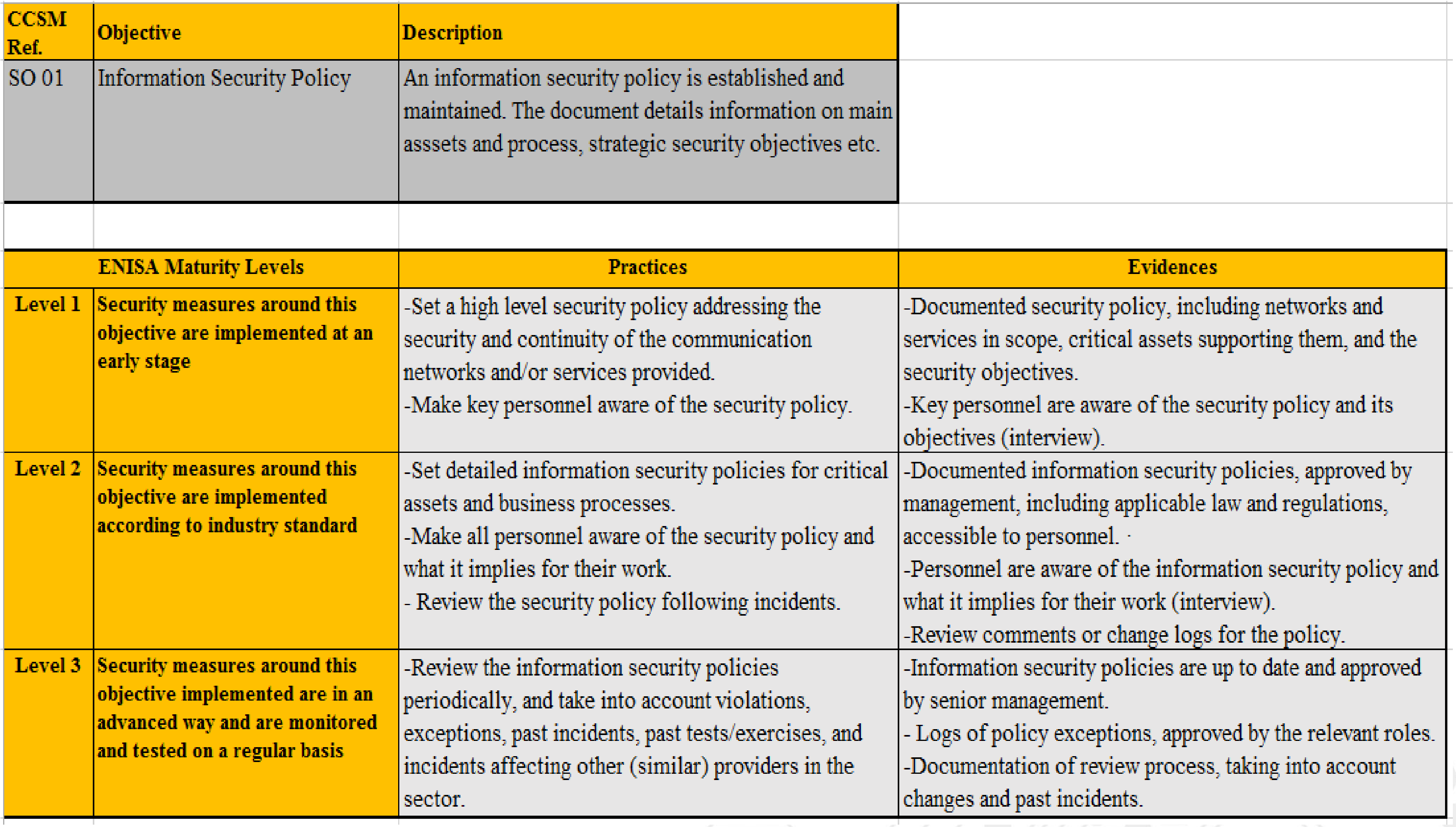
SO28 Encryption and key management

SO29 Infrastructures and virtualisation security

SO30 Interoperability and Portability (APIs)

Based on CSA OCF, and BSI C5

Security Measures sophistication levels - example



CCSM Ref.	Objective	Description
SO 01	Information Security Policy	An information security policy is established and maintained. The document details information on main asssets and process, strategic security objectives etc.

ENISA Maturity Levels		Practices	Evidences
Level 1	**Security measures around this objective are implemented at an early stage**	-Set a high level security policy addressing the security and continuity of the communication networks and/or services provided. -Make key personnel aware of the security policy.	-Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. -Key personnel are aware of the security policy and its objectives (interview).
Level 2	**Security measures around this objective are implemented according to industry standard**	-Set detailed information security policies for critical assets and business processes. -Make all personnel aware of the security policy and what it implies for their work. - Review the security policy following incidents.	-Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. -Personnel are aware of the information security policy and what it implies for their work (interview). -Review comments or change logs for the policy.
Level 3	**Security measures around this objective implemented are in an advanced way and are monitored and tested on a regular basis**	-Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	-Information security policies are up to date and approved by senior management. - Logs of policy exceptions, approved by the relevant roles. -Documentation of review process, taking into account changes and past incidents.

Summary

01 NIS directive

02 ENISA projects related to the NIS directive

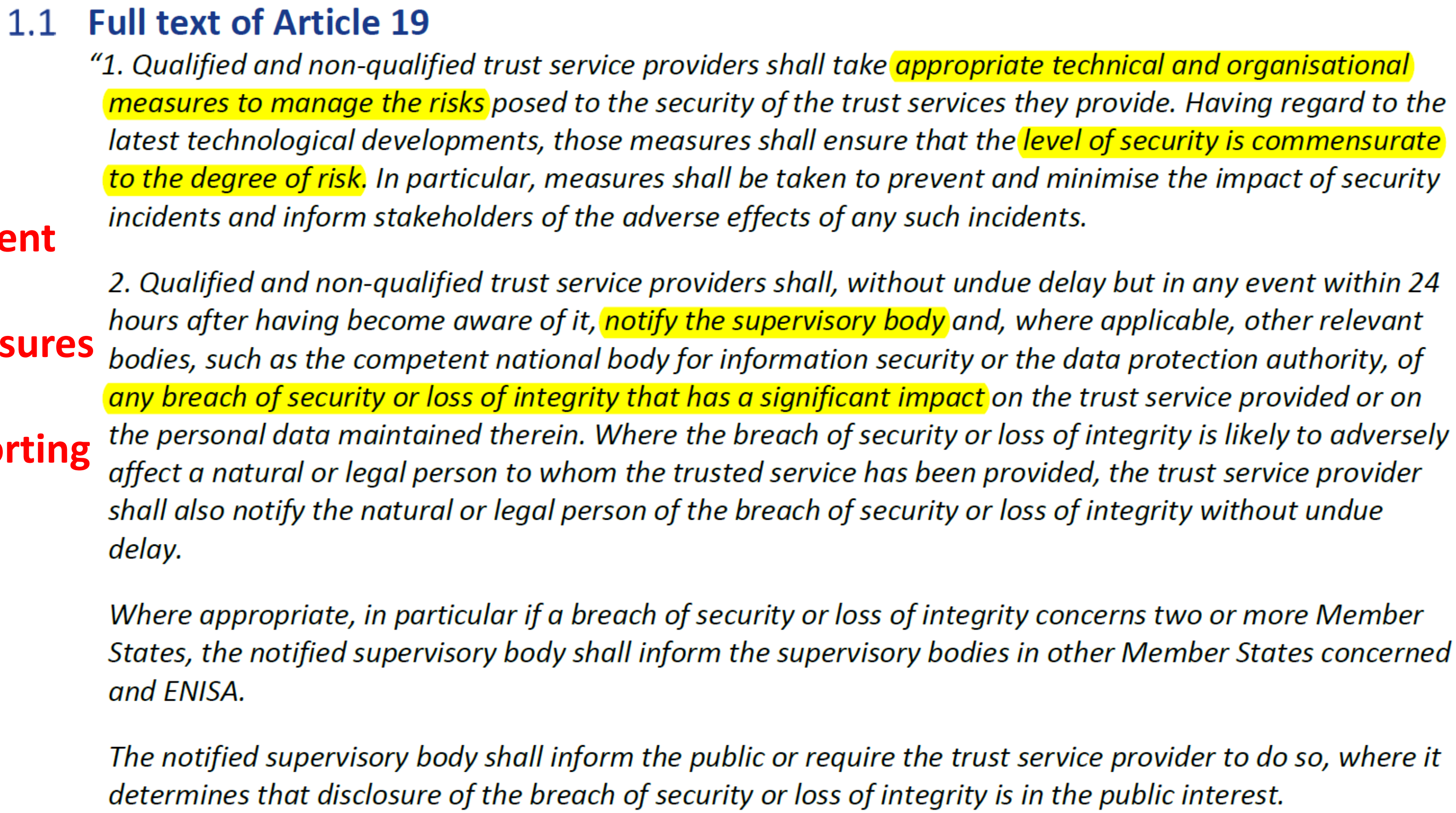
03 **Art. 19 – incident reporting for trust service providers**

General provisions of eIDAS article 19

Risk assessment

Security measures

Incident reporting



1.1 Full text of Article 19

"1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

ENISA in article 19 of eIDAS

ENISA runs an expert group: Scope of this group

- Scope is Article 19 – eTrust services providers
- Group is run by ENISA, ENISA will liaise with relevant industry groups
- EC supports this group and will liaise with other/existing groups or legislation (such as NIS directive).
- Simple, streamlined, harmonized, fitting existing national structures/authorities

Goal is to develop non-binding technical guidelines for supervisory bodies on article 19 (to support their work).

Working with experts from these bodies

The role of ENISA

Roadmap for Incident reporting framework

End of 2015

- Proposal for an Incident reporting framework - published

Spring 2016

- Decide on thresholds
- Input from CIRAS-T implementation- test

Summer 2016 – Incident reporting framework final

1/1/2017: Authorities are capable of submitting their national reports using the CIRAS-T

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu