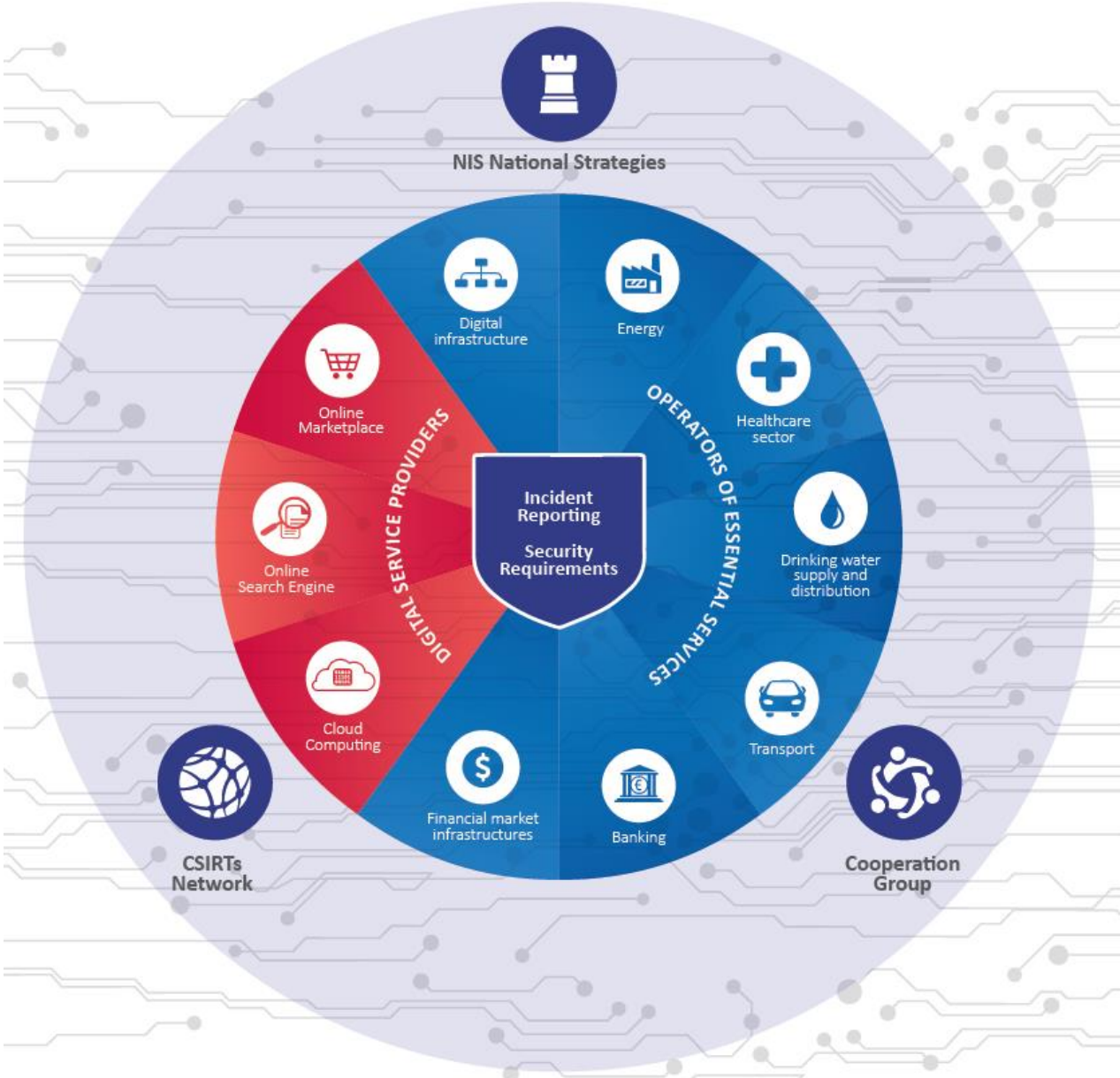
ENISA's efforts related to the NIS Directive

Konstantinos Moulinos| NIS expert – Secure Services and Infrastructures

NLO Meeting |Athens, GR| 26th April 2017


NIS National Strategies
Digital infrastructure
Energy
Healthcare sector
Drinking water supply and distribution
Transport
Banking
Financial market infrastructures
Cloud Computing
Online Search Engine
Online Marketplace
DIGITAL SERVICE PROVIDERS
OPERATORS OF ESSENTIAL SERVICES
Incident Reporting
Security Requirements
CSIRTs Network
Cooperation Group

ENISA's overall role and contribution

- Assist MS and EU COM by providing expertise/advice and by developing/facilitating exchange of good practices, e.g.
  - assist MSs in developing national NIS Strategies (NCSS)
  - assist EU COM and MSs in developing min security requirements for OESs and DSPs
  - assist EU COM and MSs in developing incident reporting frameworks for OESs and DSPs
  - assist MSs in the defining criteria for the designation of OESs
- Participate/contribute to the work of the Cooperation Group (CG)
- Be the secretariat of the CSIRT network and develop with members the network
- Elaborate advices and guidelines regarding standardization in NIS security, together with MS

National Cyber Security Strategies

- The MSs to adopt a national NIS strategy to include (art. 7) :
  - …
  - cooperation methods between the public and private sectors
- ENISA study on cooperative models for PPPs and ISACs
  - overview of current PPPs and ISACs related to cyber security in the EU Member States and EFTA.
  - identification of the common characteristics of PPPs and of ISACs.
  - identification of common challenges that highlight the need for future investment in PPPs and ISACs.
  - development of good practices and recommendations to improve the status of effective collaboration between public and private stakeholders.

ENISA's work for the Cooperation Group

Cooperation Group: current state

- 2 informal meetings in 2016
  - set-up, role, an indicative work plan, working methods and priority of tasks of the Group
- First formal meeting: 9-10 Feb. 2017, Brussels
  - the MSs to share experiences on the NISD transposition
  - adopt the rules of procedure of the CG
  - discuss and agree the work plan
  - agree on the different subgroups which will manage the workload for each work plan deliverable and agree on the working methods of each subgroup
  - ENISA update on the ongoing work of the CSIRT Network
- Next meeting: 4-5 May, Brussels
  - Reports on the progress of different CG activities

Obligations for MS on DSPs

- Minimum security measures: Technical and organizational measures proportionate to the risk (Implementing act by the COM, August 2017)
- Incident notification: prevent and minimize the impact of incidents on the IT systems which provide the services (Implementing act by the COM, August 2017)

Notes:

- Light touch approach to be applied for DSPs
- NIS directive applicable only to large and medium enterprises

ENISA's role in supporting MSs on DSPs

ENISA supported COM and the MSs with the following activities in 2016

1) guidelines for implementing incident notification – DSPs

   - Assist COM(by providing input for the implementing acts) and MS (by providing guidelines) in incident notification requirements for DSPs

2) guidelines for implementing security measures – DSPs

   - Assist COM (by providing input for the implementing acts) and MS (by providing guidelines) in implementing minimum security measures for DSPs

MSs discussed the provisions on DSPs in an informal group created by COM

- 3 meetings of the informal group took place in 2016 and 2017
- art. 22 Committee procedure kick off, 6 April, Brussels: discussion on the draft implementing acts

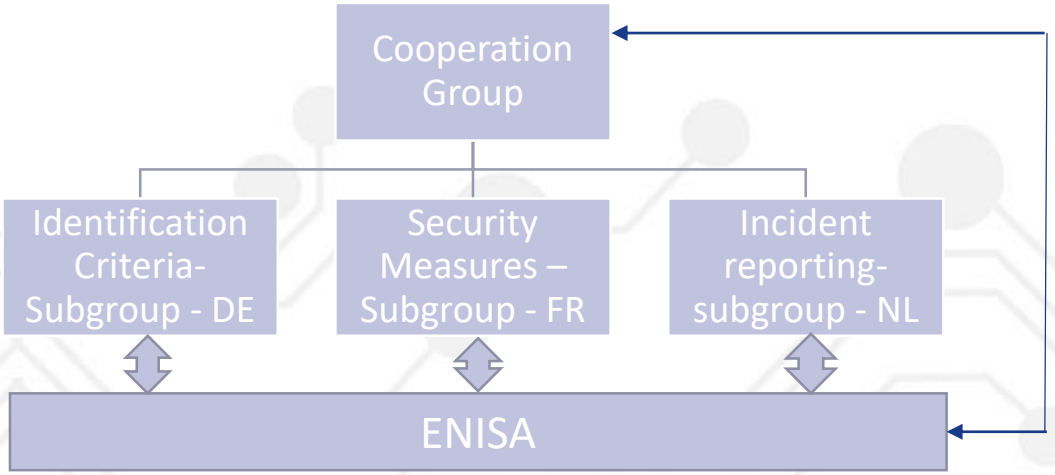
Challenges with the implementing acts

- To agree on how deep the description will be
  - Too many details: leaves no room for flexibility
  - Too few details: leaves room for misinterpretations
- Vague definitions of DSPs
- References to standards: to be or not to be?
- Definition of the ‘state of the art’ concept

Obligations for MSs on OESs

- Identification of operators of essential services
- Minimum security measures to ensure a level of security appropriate to the risks
- Incident notification to prevent and minimize the impact of incidents on the IT systems that provide services
- Make sure authorities have the powers and means to assess security and check evidence of compliance for OES

ENISA's role in supporting MS with OESs

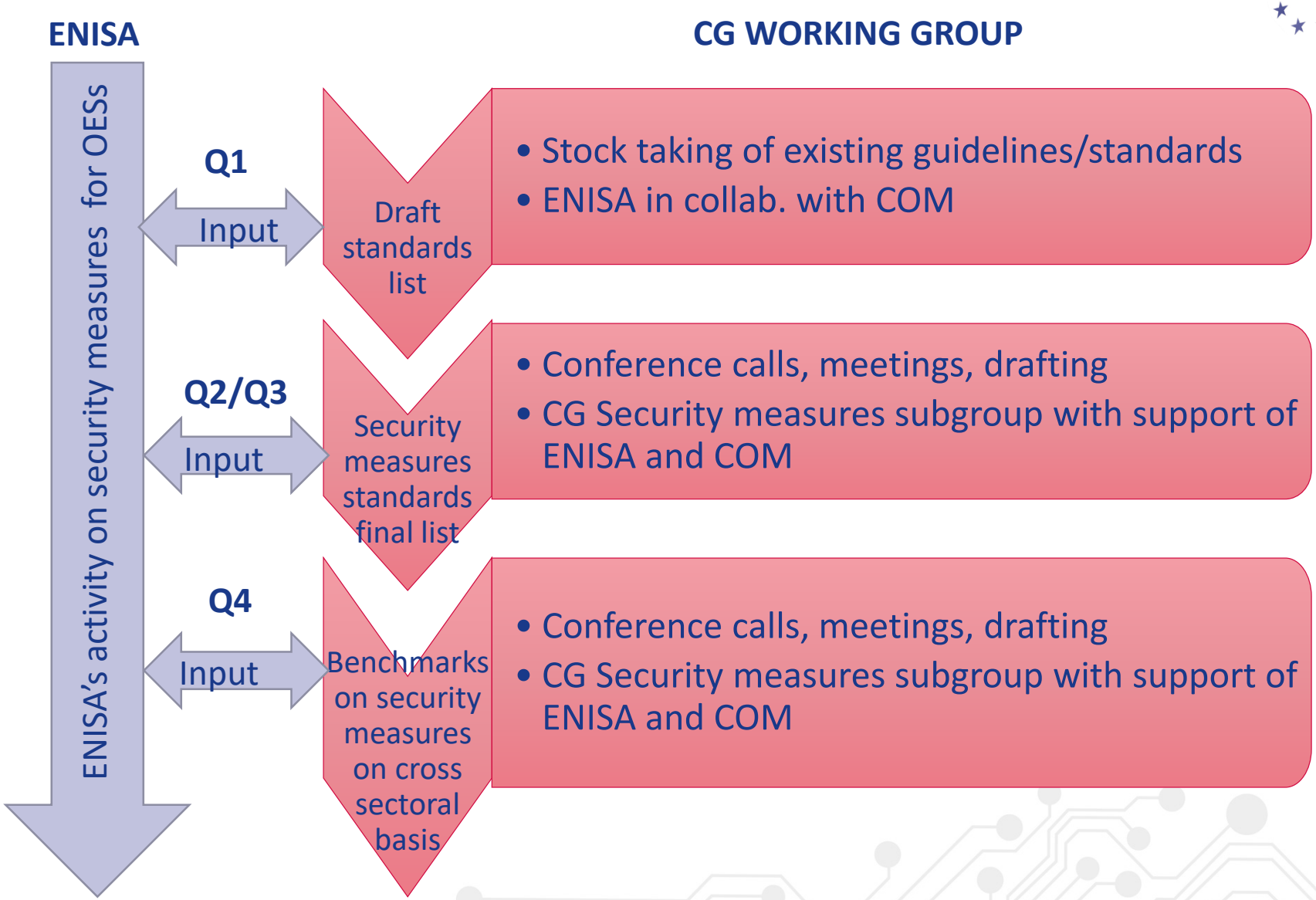


ENISA WP2017 activities	CG WP2017 activities
O.1.1.1 - Baseline Security Recommendations for the OES Sectors	1. Stock taking of existing schemes
	2. Non binding reference document
O.2.2.2 - Develop guidelines for the implementation of mandatory incident reporting	3. Stock taking of existing schemes
	4. Non binding guidelines concerning circumstances for notifications
	5. Non binding guidelines concerning format and procedures for notifications
	6. Guidelines on the procedure of sharing
O.3.3.2 - Restricted. Upon request, support the assessment of existing policies/procedures/practices on NIS within EU institutions	7. Mapping of relevant sectorial initiatives at EU and international level
O.2.2.6 - Supporting the Implementation of the NIS directive	8. Sharing of best practice related to the criteria defining the criticality of an OES
	9. Non-binding document on modalities
	10. Non binding guidelines on the interpretation of selected definitions of OESs

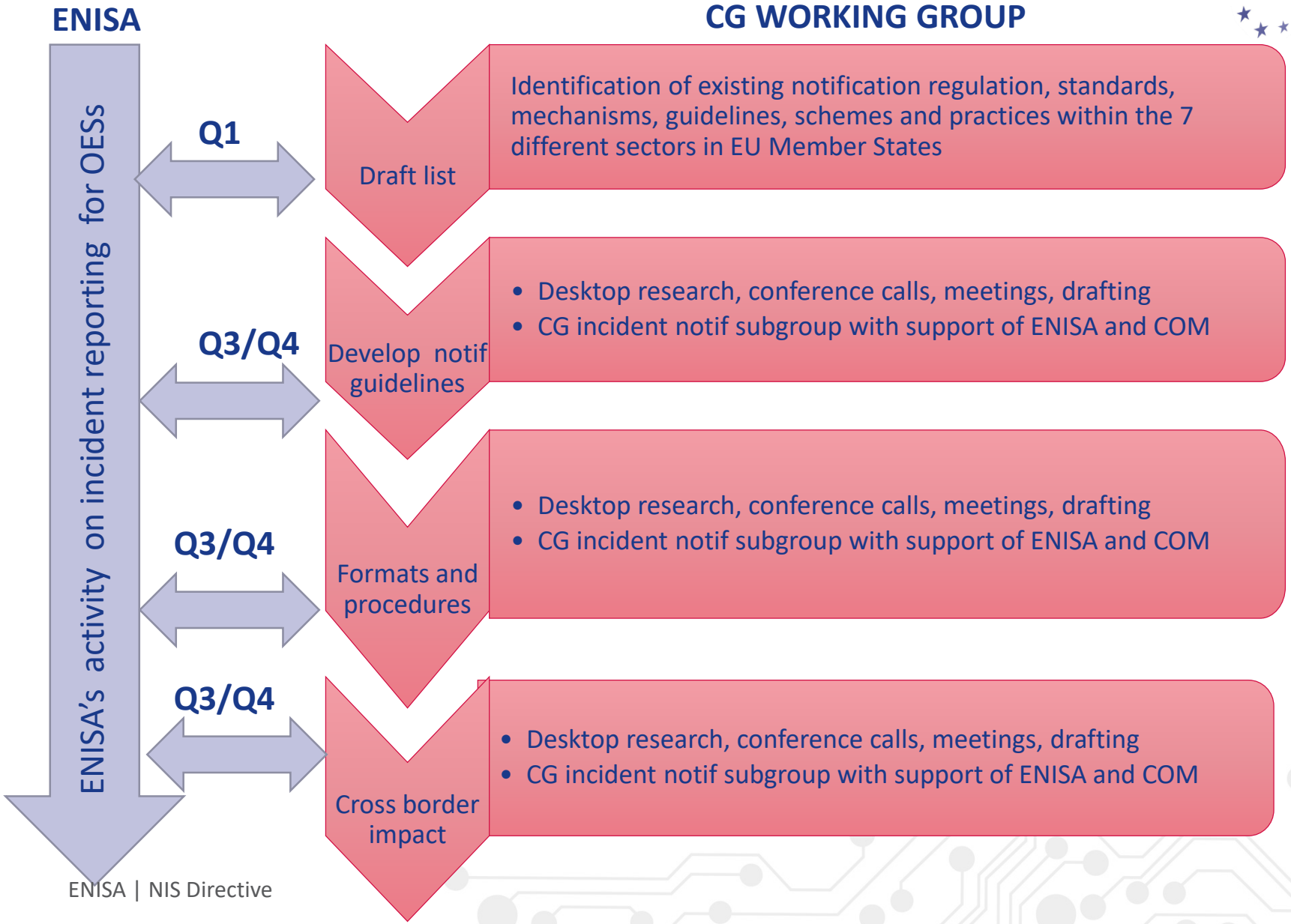
ENISA activities for the CG

- ENISA will transfer the knowledge gained from telcos/article 13a and eIDAS article 19 expert groups to the process
  - Incident reporting
  - Minimum security measures
- Several actions of Work Plan of the Co-operation Group (CG) relate with actions of ENISA's WP 2017
  - it is important to avoid overlaps and strengthen synergies by keeping the work of the CG in sync with ENISA’s WP 2017 of ENISA.
- ENISA, at the request of MSs/CG, will participate in all 3 Working Groups to
  - facilitate the process and engage the stakeholders
  - take stock of particular items inline with its WP 2017 studies (e.g. on incident reporting methods used by MS)
  - analyse and/or assess possible approaches (e.g. in criteria for OES)

ENISA's view on collaboration with CG working groups: Security measures for the OESs - example



Incident reporting for OESs



CG Working Groups: status update

- Security measures
  - Last meeting: 7 April, Brussels
  - Status:
    - Survey ongoing (11 participants so far)
    - ENISA prepared the TOC which sent to the task leader team (FR, BE, COM, ENISA)
  - Next step: The TLT to send the TOC to the MSs for comments
- Identification criteria
  - Last meeting: 28 February, Berlin
  - Status: DE to draft the guidelines
  - Next step: The TLT (DE, COM, ENISA) to send the draft guidelines to the MSs for comments
- Incident reporting
  - Last meeting: -
  - Status: ENISA survey ongoing (**https://ec.europa.eu/eusurvey/runner/IncidentReporting_OES**)
  - Next step: working group meeting, 26 April, Brussels

NIS directive - TIMELINE

August 2016	-	Entry into force
February 2017	6 months	Cooperation Group starts its tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
9 May 2018	21 months	Transposition into national law
November 2018	27 months	Member States to identify operators of essential services
May 2019	33 months (i.e. 1 year after transposition)	Commission report - consistency of Member States' identification of OES
May 2021	57 months (i.e. 3 years after transposition)	Commission review

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu