



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

CONSIDERATI
PARTNERS FOR THE DIGITAL WORLD

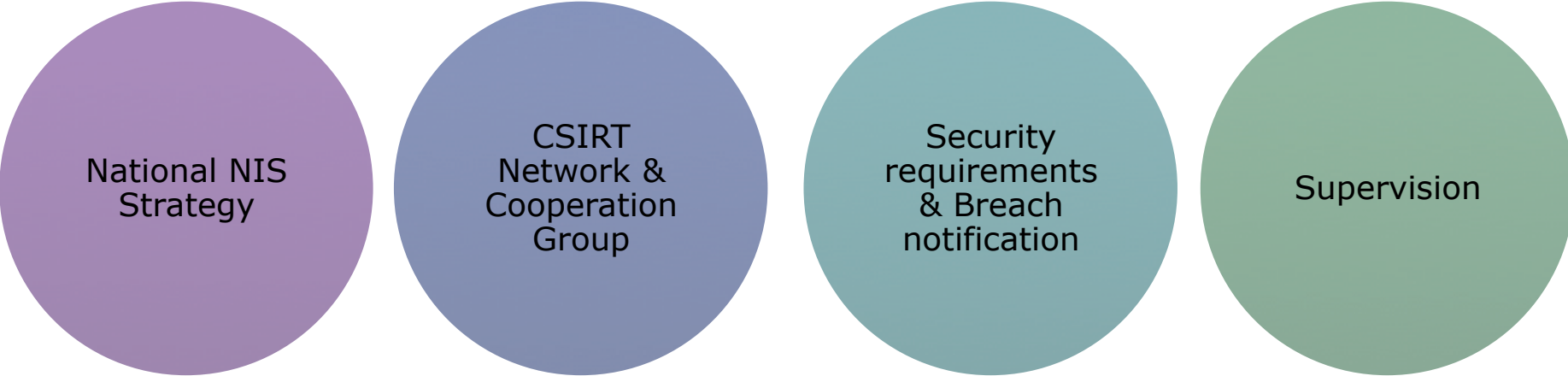
EU Directive on Network- and Information Security (NIS-Directive)

RIPE47

May 11, 2017

Quick facts

“measures for a high common level of security of network and information systems across the Union”



National NIS
Strategy

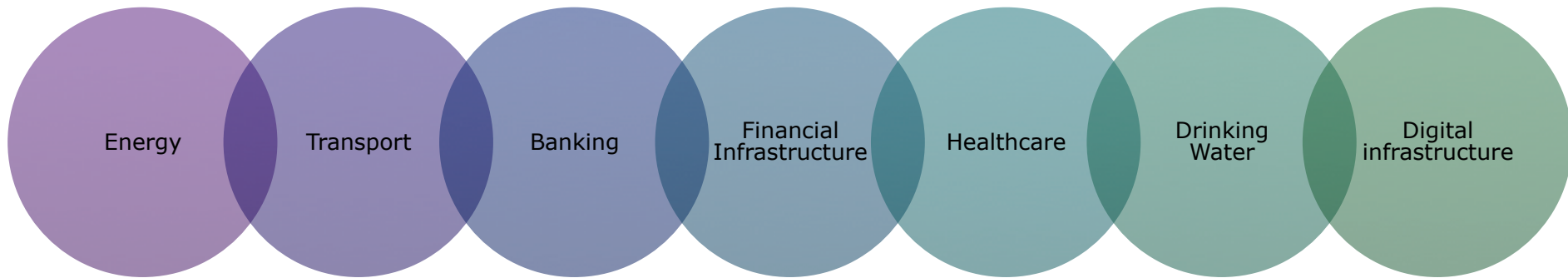
CSIRT
Network &
Cooperation
Group

Security
requirements
& Breach
notification

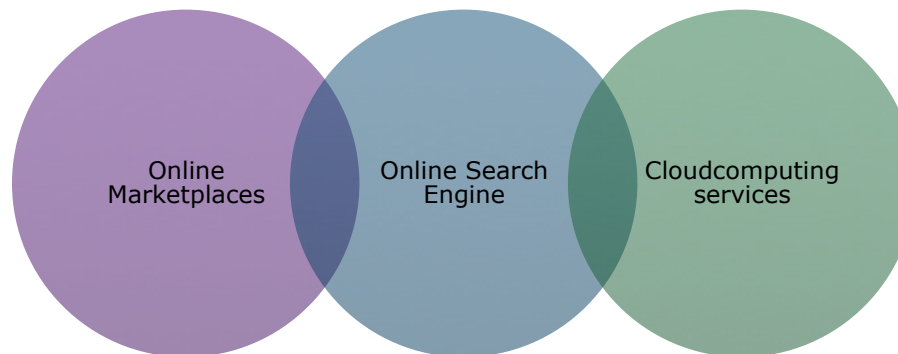
Supervision

May 2018

Operators of Essential Services



Digital Service Providers



Security requirement (OES)

*[...] **appropriate and proportional technical and organisational measures** to manage the risks posed to the security of networks and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.*

[...] appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

Security requirement (DSP)

*"[...] identify and take **appropriate and proportionate technical and organisational measures to manage the risks** posed to the security of network and information systems which they use in the context of offering [their] services[...]. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:*

- (a) the security of systems and facilities;*
- (b) incident handling;*
- (c) business continuity management;*
- (d) monitoring, auditing and testing;*
- (e) compliance with international standards.*

[...] measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on [their] services [...] that are offered within the Union, with a view to ensuring the continuity of those services.

Notification requirement (OES)

- the competent authority or the CSIRT
- of incidents having a significant impact on the continuity of the essential services they provide.
- Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident.
- Notification shall not make the notifying party subject to increased liability.

Notification requirement (DSP)

- the competent authority or the CSIRT
- any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union.
- Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact.
- Notification shall not make the notifying party subject to increased liability.

Note

- Parameters on security requirements, data breaches and fines will be established by each Member State separately;
- EC works on guidelines for OES and implementing acts for DSPs;
- Member States have to collaborate in cross-border security incidents;

Dutch implementation

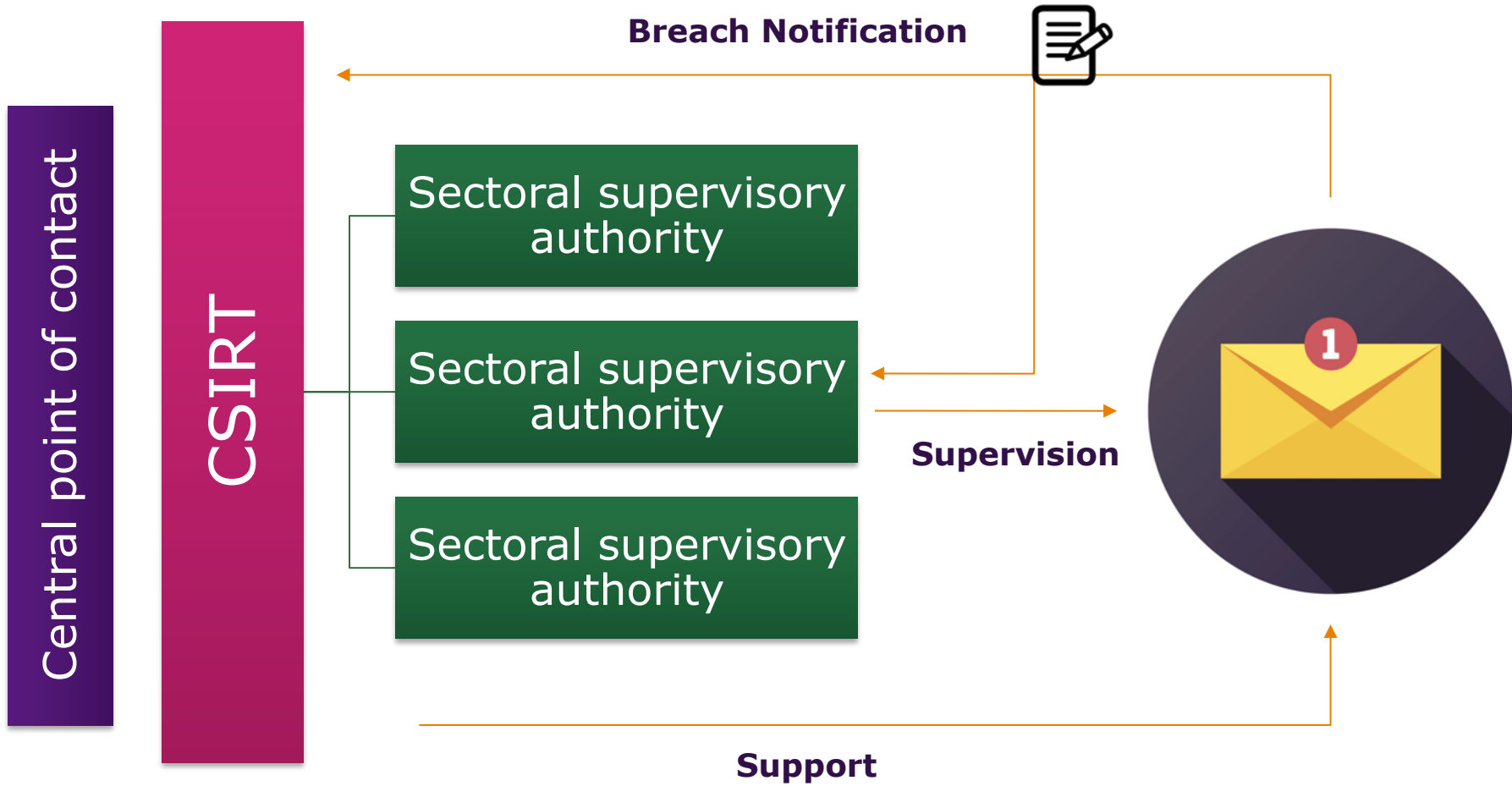
Still in progress

- Already has CSIRT and NIS strategy;
- "Sectoral or decentralised approach" for supervision;
- "Fitting NIS into existing framework";
- Parameters to establish impact are confidential.

Other options

- Centralised approach;
- Creating new cybersecurity framework.







Questions?