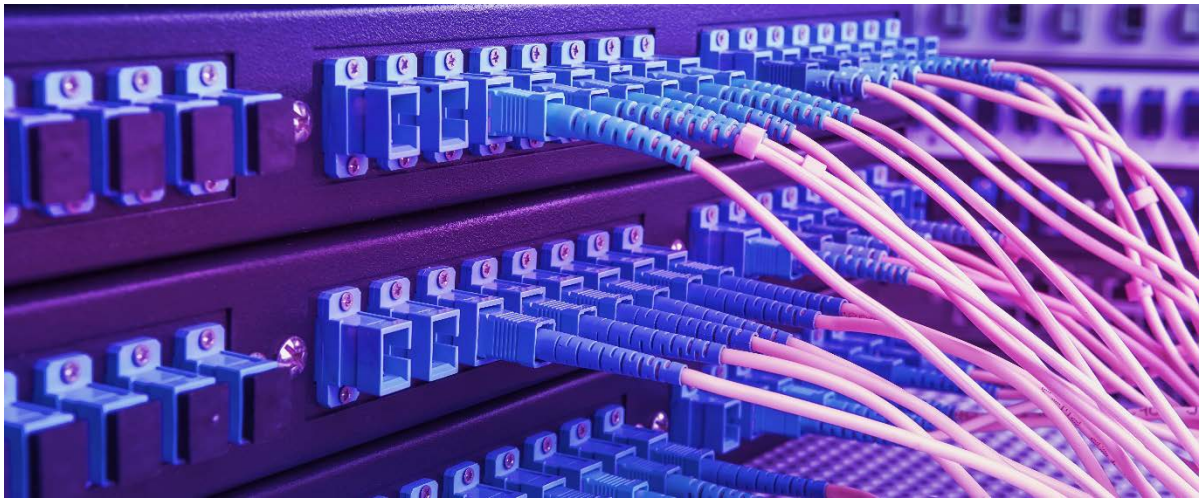
Deloitte.

Agreement reached on EU Network and Information Security (NIS) Directive

A first analysis of the security and incident notification requirements for Operators of Essential Services and Digital Service Providers



January 2016

The Network and Information Security (NIS) Directive aims to achieve a high common level of security of networks and information systems within the European Union. After more than two years of negotiation, the European Council reached an informal agreement with the Parliament on December 7th 2015, and the agreed **final compromise text** was approved by the Member States (MS) December 18th 2015.

About the NIS Directive

The NIS Directive establishes **security and notification requirements for Operators of Essential Services (OoES)** such as banking, energy, transport, financial market infrastructure, health, drinking water, digital infrastructure; and **Digital Service Providers (DSP),** including online marketplaces, online search engines and cloud services.

In addition, the NIS Directive lays down specific **obligations** for MSs of the EU to adopt a national NIS strategy, to designate **National Competent Authorities (NCA)**, **Single Points of Contact (SPoC)** and specific NIS tasks to **Computer Security Incident Response Teams (CSIRT)**.

Furthermore, it creates **a cooperation group** in order to develop trust amongst MSs and facilitate **strategic** cybersecurity information sharing. In parallel, it creates **a CSIRTs network** to build confidence amongst MSs to boost **operational** cybersecurity cooperation.

What are Operators of Essential Services and Digital Service Providers?

An **Operator of Essential Service** is a public or private entity, which provides an essential service for the maintenance of critical societal and/or economic activities, depends on networks and information systems, and for which an impact on these systems would produce "significant disruptive effects" on its ability to provide its service. In line with these criteria, MSs will have to identify such OoESs from the sectors and subsectors depicted below.

A **Digital Service** means a service offered at a distance by electronic means at the request of an individual recipient of services (Article 1b of **Directive 2015/1535**) or of a businesses at large, meaning Online Marketplaces, Online Search Engines or Cloud Computing Services.

Some sectors are already regulated or may be regulated in the future by sector-specific EU legal acts that include rules related to the security of networks and information systems. Whenever those acts impose requirements, their provisions will take precedence over the corresponding provisions of the NIS Directive, so long as they are at least equivalent in effect to the obligations in the NIS Directive.

Figure 1 - Sectors and subsectors in scope of the NIS Directive

What security and incident notification requirements will apply to Operators of Essential Services and Digital Service Providers?

Both OoES and DSPs will have to ensure the security of their networks and systems to promote a culture of risk management and ensure that serious incidents are reported to NCA or CSIRT. These would include primarily private networks, and systems for which security is managed either by internal IT staff or by outsourced staff.

The tables below summarise the requirements from the **final compromise text** of the NIS Directive.

Security requirements	Operators of Essential Services?	Digital Service Providers?
A. Take technical and organisational measures to manage the risks posed to the security of networks and information systems.	**Yes**	**Yes** (partially)
B. Provide information needed to assess the security of networks and information systems, including security policies.	**Yes**	**Yes**
C. Provide evidence of effective implementation of security policies, such as the results of security audits.	**Yes**	**No**
D. Execute binding instructions received by the NCA to remedy their operations.	**Yes**	**No**
E. Remedy any failure to fulfil the requirements set out in the NIS Directive.	**No**	**Yes**
F. Designate a representative in the EU when not established in the EU, but offering services within the EU.	**No**	**Yes**

In the case of DSPs the first 5 requirements listed above do not apply to micro- and small enterprises as defined in **the Commission Recommendation of 6 May 2003**. Therefore, DSPs with less than 50 employees and whose annual turnover and/or annual balance sheet total does not exceed 10 million EUR are exempt from taking security measures and notifying incidents.

Incident notification requirements	Operators of Essential Services?	Digital Service Providers?
A. Notify any incident having a “significant” or “substantial” impact to the NCA or to the CSIRT without undue delay.	**Yes**	**Yes**[1]
B. Notify impact of incident if OoESs relies on a third-party DSP.	**Yes**[2]	**No**
C. Inform the public about individual incidents if required by the notified competent authority or CSIRT.	**No**	**Yes**

Details of technical and organizational measures

Using a risk based approach, for DSPs only, security measures will have to take into account the following elements: the security of systems and facilities, incident management, compliance with international standards, business continuity management, monitoring, auditing and testing.

NCAs will have the power to require both OoES and DSPs to provide information needed to assess the security of their networks and information systems, including documented security policies. In addition, NCAs will require only OoES to provide evidence of effective implementation of security policies, such as the results of a security audit carried out by the NCA or a qualified auditor. These operators will also have to execute binding instructions received by the NCA to remedy less secure operations, while DSPs will simply be required by the NCA to remedy any failure to fulfil its requirements.

[1] Will only apply where the DSP has access to the information required to appreciate if the criteria are fulfilled.
[2] Where an OoES relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities any “significant” impact on the continuity of the essential services due to an incident affecting the digital service provider will still have to be notified.

DSPs that are not established in the EU, but offer services within the EU, will have to designate a representative, established in one of the MSs where the services are offered, and will be deemed to be under the jurisdiction of that MS.

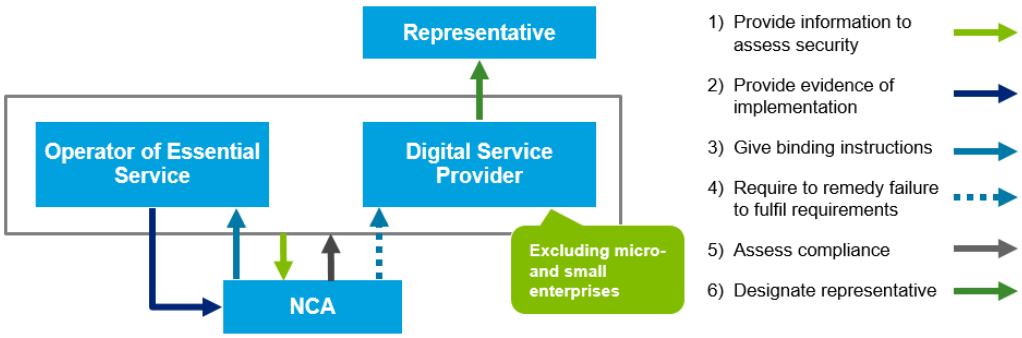


Figure 2 - Technical and organizational measures

Details of incident notification requirements

OoESs will have to notify NCAs or CSIRT whenever there is a “significant” impact on the provision of the operator’s service. The “significance” of an incident will be mainly determined by the **number of users affected** by the disruption, the **duration** of the incident, and the **geographical spread** with regard to the area affected by the incident.

DSPs will have to notify any incident having a “substantial” impact on the provision of a service. The “substantiality” of an incident will be determined by the same criteria as for OoESs, and in addition **the extent of the disruption** of the functioning of the service and **the extent of the impact** on economic and societal activities.

This incident notification requirement will be stronger for OoESs than for DSPs, as the obligation to notify an incident will only apply where the DSP has access to certain information.

Besides notification of incidents, the NIS Directive foresees, under specific conditions, the obligation to inform affected MSs and, to a certain extent, the public. Therefore, in the case of OoESs, the notified NCA or CSIRT will be required to inform affected Member State(s), in case of significant impact on the continuity of the essential services. The notified NCA or CSIRT has the option to choose whether or not to immediately disclose individual incidents to the public; it may be decided that public awareness is necessary to prevent an incident, or that they must first deal with ongoing incident, and only later disclose it to the public after consultation of the concerned OoES.

Regarding DSPs, the notified NCA or the CSIRT will be required to inform other affected MSs. The NIS Directive further details this requirement by stating that information is particularly deemed appropriate where the incident concerns two or more MSs. In any case, security and commercial interests of the DSP and the confidentiality of the information provided should be preserved. An obligation to inform the public is foreseen as well where public awareness is necessary to prevent an incident or to deal with an ongoing incident. What differs from requirements applicable to OoESs is that information may be decided where disclosure of the incident is otherwise in the public interest. Information can be done not only by the NCA or CSIRT but also, where appropriate, by the NCAs or CSIRTs of other MSs concerned and even by the DSP itself if so required. Like in the case of OoESs, DSPs will be consulted.

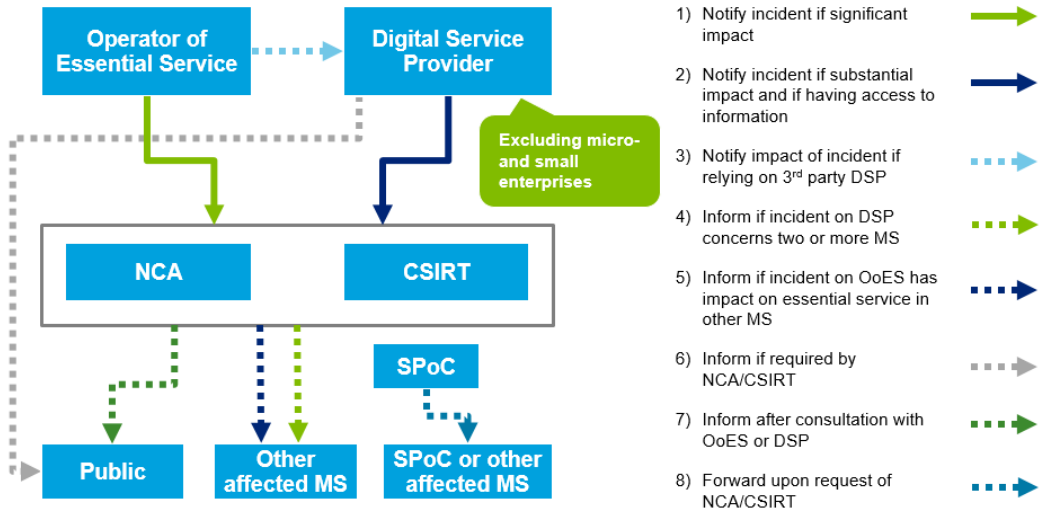


Figure 3 - Incident Notification

What obligations will be imposed on Member States?

MSs will be required to adopt a national NIS strategy, defining the **strategic objectives** and appropriate **policy and regulatory measures** in relation to cybersecurity and coverage of essential sectors. This will include setting up a governance framework including **roles and responsibilities** of the governmental bodies and relevant actors; the identification of **measures on preparedness, response and recovery**, including cooperation between the public and private sectors; **awareness raising and training programs**; and **research and development plans** relating to the NIS strategy.

MSs will also be required to designate a **National Competent Authority (NCA)** for the implementation and enforcement of the NIS Directive at national level. These NCAs will consult and cooperate with the **national Law Enforcement Authorities (LEA)** and **national Data Protection Authorities (DPA)**. In addition, each MS will have to designate a national **Single Point of Contact (SPoC)** with whom NIS will liaise to **ensure cross-border cooperation** of MS authorities, the cooperation group, and the CSIRTs network. Once a year, the SPOC will submit a summary report to the cooperation group on the incident notifications received.

Each MS will have to designate one or more CSIRTs responsible for handling incidents and risks covering at least the sectors in scope of the Directive. Tasks of the CSIRT shall include the **monitoring of incidents** at a national level; the **provision of early warning, alerts, and dissemination of information** to relevant stakeholders about cyber risks and incidents; **responding to incidents; providing risk and incident analysis** and **situational awareness**; and **participation in the CSIRT network**. In addition, the CSIRT will have to promote the adoption and use of **common or standardized practices** for incident and risk handling procedures including **information classification schemes**.

How will cooperation between Member States be fostered?

The NIS Directive will set up a **strategic** cooperation group to **draw up strategic guidelines for the activities of the CSIRT network** and **discuss capabilities and preparedness of MSs**, among other tasks. This group will be composed of **representatives from the MSs, the Commission** and the **European Union Agency for Network and Information Security (ENISA)** while **representatives from relevant stakeholders** will also be allowed to be invited for participation. The Commission will provide the secretariat for this group.

In addition, at an **operational** level a network of CSIRTs will be assigned multiple tasks, including **supporting MSs in addressing cross-border incidents, exchanging best practices** on the exchange of information related to incident notification, and **assisting MSs in building capacity in NIS**. This network will be composed of **representatives of the MSs' CSIRTs** and **CERT-EU,** while the Commission will participate as an observer. ENISA will provide the secretariat for the CSIRTs

Network and will be encouraged to maintain a website with general information on major NIS incidents occurring across the Union.

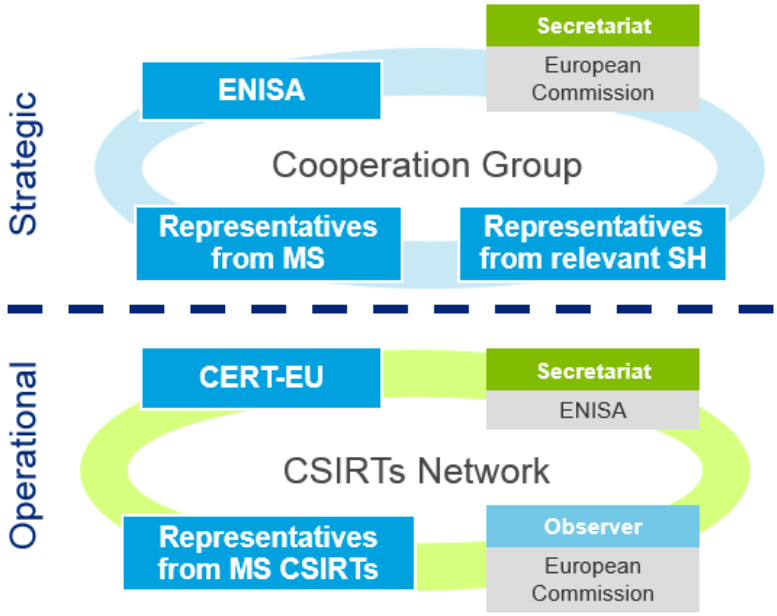


Figure 4 - Cooperation between Competent Authorities

What is next?

Once the agreed text has undergone technical finalization, it should be formally approved first by the Council and then by the Parliament. The procedure is expected to be concluded in spring 2016.

After the Directive has entered into force, MSs will have 21 months to transpose the Directive into national law. After this period, they will have another 6 months to identify the essential services operators established in their territory which are to be covered by the directive.

Date	Legislative Step
Spring 2016	Formal approval first by the Council and by the Parliament.
Q2 2016	Expected publication in the Official Journal of the European Communities.
Q4 2016	MSs to ensure representation in the Cooperation Group and the CSIRTs Network.
Q2 2018	Deadline for the transposition into national law.
Q4 2018	Deadline for MSs to identify the Operators of Essential Services with an establishment on their territory for each subsector.

Contact

Stéphane Hurtaud
Partner - Information & technology Risk
shurtaud@deloitte.lu

Roland Bastin
Partner - Information & technology Risk
rbastin@deloitte.lu

Laurent de la Vaissière
Director - Information & Technology Risk
ldelavaissiere@deloitte.lu

Alexander Cespedes Arkush
Manager – Information & Technology Risk
alcespedesarkush@deloitte.lu