Deloitte.

Developing cybersecurity
capabilities for the EU NIS Directive

Developing cybersecurity capabilities for the EU NIS Directive

Network and information systems support many of the essential services for the EU society and economy. It is therefore highly important to protect these networks and information systems from a continuously evolving threat landscape. The European Commission has taken various regulatory initiatives concerned with the security of network and information systems and the protection of data In particular. The EU Directive on the security of network and information systems (NIS Directive) is among the main legislative initiatives involving all EU Member States With the aim of enhancing the overall level of cybersecurity in the European Union.

This report provides an account of the needs of developing cybersecurity capabilities in alignment with the NIS Directive. In particular, the report highlights how NIS Directive stakeholders such as Operators of Essential Service (OES) across different sectors (e.g. Energy, Transport, Banking, etc.) and Digital Service Providers (DSPs) require and prioritise the developments of specific cybersecurity capabilities. Therefore, this report provides:

- ✓ An overview of the NIS Directive, with a particular focus on the security requirements and notification for OES and DSPs;
- ✓ An account of the NIS Directive developments based on the results of Deloitte's NIS Directive Compliance Survey;
- ✓ An outline of cybersecurity capabilities supporting OES and DSPs to comply with the NIS Directive.

Hence, this report provides a comprehensive account of the needs of OES and DSPs for building key cybersecurity capabilities in alignment with the NIS Directive. Therefore, it offers insights to organisations dealing with the NIS Directive in their operational environments.

1. Cybersecurity governance in the European Union

The European Commission has developed a comprehensive regulatory framework consisting of different EU regulations and directives, which define relevant obligations in order to enhance cybersecurity across the European Union. In particular, specific EU regulations and directives focus on data protection and security such as the General Data Protection Regulation (GDPR), the directive on the security of network and information systems (NIS Directive) and the EU Cybersecurity Act . Other, regulatory frameworks define further governance obligations for specific sectors (e.g. Banking, Medical Devices, Telecom, etc.). In this whitepaper we focus on the analysis of the NIS Directive in order to provide insights for complying with relevant obligations and building capabilities.

1.1 NIS Directive

The NIS Directive is the first EU-wide legislation concerned with achieving a high common security level of network and information systems. It provides legal instruments enhancing the security of network and information systems underlying essential services in the EU. In order to achieve its main objective, the NIS Directive provides the legal instruments for three strategic developments :

- ✓ Improved cybersecurity capabilities at a national level – Member States have to adopt a national Cyber Security Strategy (NCSS) and to designate a Single Point of Contact (SPOC), National Competent Authorities (NCAs) and Computer Security Incident Response Teams (CSIRTs) with different responsibilities for monitoring and supporting the implementation of the NIS Directive;
- ✓ Increased EU-level cooperation by establishing the CSIRTs Network and the Cooperation Group (composed of representatives of the Member States, the European Commission and the European Union Agency for Network and Information Security – ENISA);
- ✓ Defined security requirements and incident notification obligations for Operator of Essential Services (OES) and Digital Service Providers (DSPs).

These strategic developments of the NIS Directive across the Member States contribute towards building capabilities in order to enhance the security of network and information systems of OES and DSPs. Furthermore, they support establishing trust and cooperation among the Member States.
The NIS Directive was adopted and put into force by the European Parliament in 2016 (see the planned NIS Directive timeline in Figure 1). Member States were obliged to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018. Most EU Member States have already transposed the NIS Directive into their local legislations and regulations, which has an impact on OES, DSPs, NCAs and European institutions, and triggers an extensive set of actions.

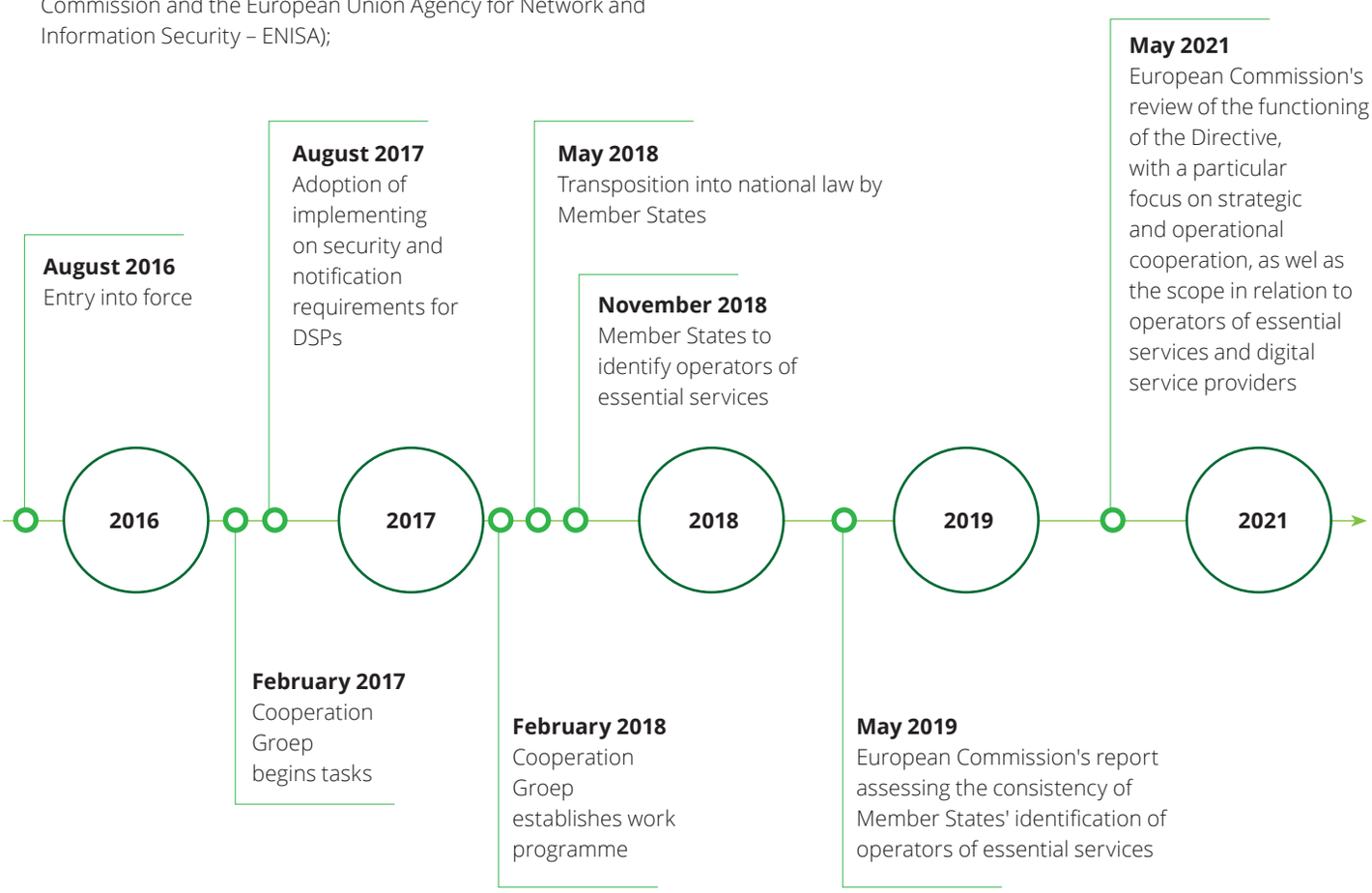


Figure 1 Planned NIS Directive timeline

As shown by the timeline, and based on the data from the European Commission's State-of-play of the transposition of the NIS Directive , the NIS Directive implementation is an ongoing effort. On 28 October 2019, the EU Commission published a report that provides an overview of how the Member States have identified OES. The report finds that the NIS Directive has played a key role in preparing operators of essential services for cyber-incidents throughout the Union and that some countries have identified essential services in sectors beyond those listed in the Directive. National authorities have developed a wide variety of identification practices leading to inconsistency when it comes to the identification of OESs across the internal market. The report concludes that some identification practices used by the Member States can have a negative impact on the level playing field in the internal market and potentially render entities more vulnerable to cross-border cyber-threats .

1.2 Operators of Essential Services and Digital Service Providers

The NIS Directive defines security requirements and notification for OES and DSPs. Member States have identified the OES operating in their nations. Therefore, OES and DSPs have major responsibilities and critical roles in enhancing the overall cybersecurity across the Union.

- ✓ Operators of Essential Services: An OES is a public or private entity, which provides an essential service for the maintenance of critical societal and/or economic activities. An OES depends on networks and information systems in order to deliver its services. A cyber incident affecting such systems may have an impact producing significant disruptive effects on its ability to provide its service. In line with these criteria, EU Member States have identified OES for each sector (and subsector) that are within the scope of the NIS Directive (Figure 2): Energy, Transport, Banking, Financial market infrastructure, Health sector, Drinking water supply and distribution, and Digital infrastructure.
- ✓ Digital Service Providers: A DSP means a service offered at a distance by electronic means at the request of a business organisation or of an individual recipient of services. The NIS Directive covers three different types of digital services (Figure 2): Online Marketplaces, Online Search Engines and 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, as long as they are at least equivalent in effect to the obligations in the NIS Directive.

Figure 2 Sectors of OES and types of digital services in the scope of the NIS Directive

In order to comply with the NIS Directive, OES and DSPs have to take appropriate security measures and notify the relevant National Competent Authorities (NCAs) or CSIRTs, on incidents that have significant disruptive effect. Therefore, in order to enhance the security of network and information systems the NIS Directive provides a comprehensive framework involving (Figure 3): Governance at Member State level and cooperation among them, Security Requirements for OES and DSPs, Impact Assessment based on specific criteria, and Incident Notification obligations for OES and DSPs to relevant NCAs or CSIRTs.

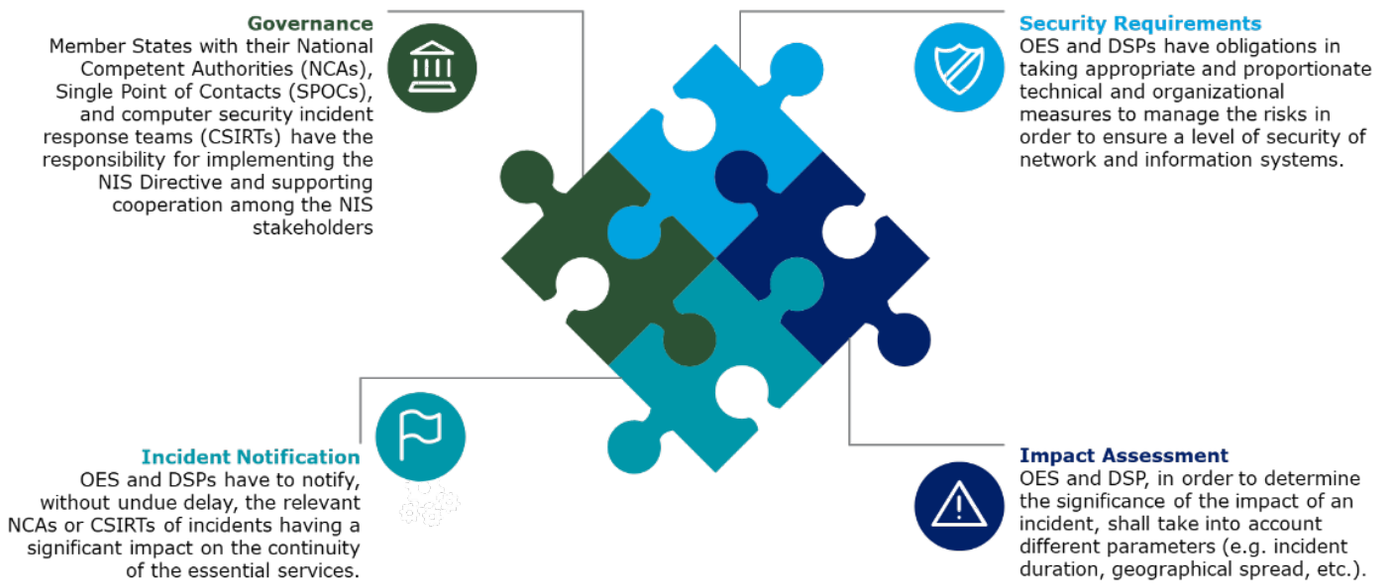


Figure 3 NIS Directive's perspectives on the security of network and information systems

In order to assess impact of an incidents, OES and DSPs have to take into account and assess different parameters: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident.

Additionally, DSPs shall take into account: (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities. The security measures may include technical and organisational measures that are appropriate and proportionate to the risks; ensuring the security of network and information. The adopted measures should prevent and minimise the impact of incidents on the IT systems that are used to provide the essential services. The NIS Directive emphasises that the adopted security measures support the protection against any action that could compromise potentially the availability, integrity and confidentiality of network and information systems.

2. NIS Directive developments across sectors and the Member States

Deloitte has engaged with relevant NIS Directive stakeholders in order to investigate their needs in building relevant capabilities and complying with the NIS Directive. This section presents the results and insights drawn from a NIS Directive compliance survey that Deloitte conducted during the summer of 2019. This section provides a characterisation of the NIS Directive stakeholders who responded to the survey and their current practices concerned with security requirements and incident notification. Finally, it highlights how NIS Directive stakeholders prioritise relevant cyber capabilities in order to comply with the Directive.

2.1 NIS Directive Stakeholders

Deloitte gathered responses from a sample population representing the NIS Directive stakeholders. OES, in particular, represents the majority (77%) of the consulted NIS Directive stakeholders (Figure 4). The remaining sample population (23%) involves the other key NIS Directive stakeholders (i.e. DSPs, NCAs, CSIRTs and SPOC). Hence, the Deloitte investigation focuses mainly on the merging needs of OES in building relevant capabilities in order to comply with the NIS Directive. The sample OES cover all seven sectors that the NIS Directive identifies (Figure 5).

NIS Directive Stakeholders

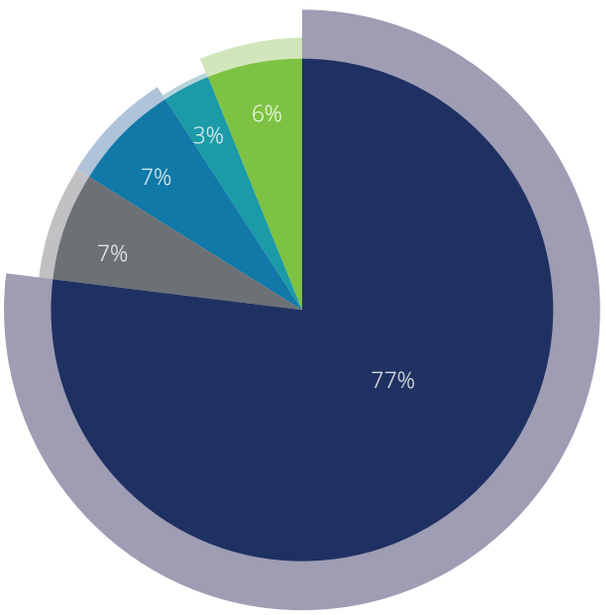


Figure 4 Sample population of NIS Directive stakeholders

NIS Directive Sectors

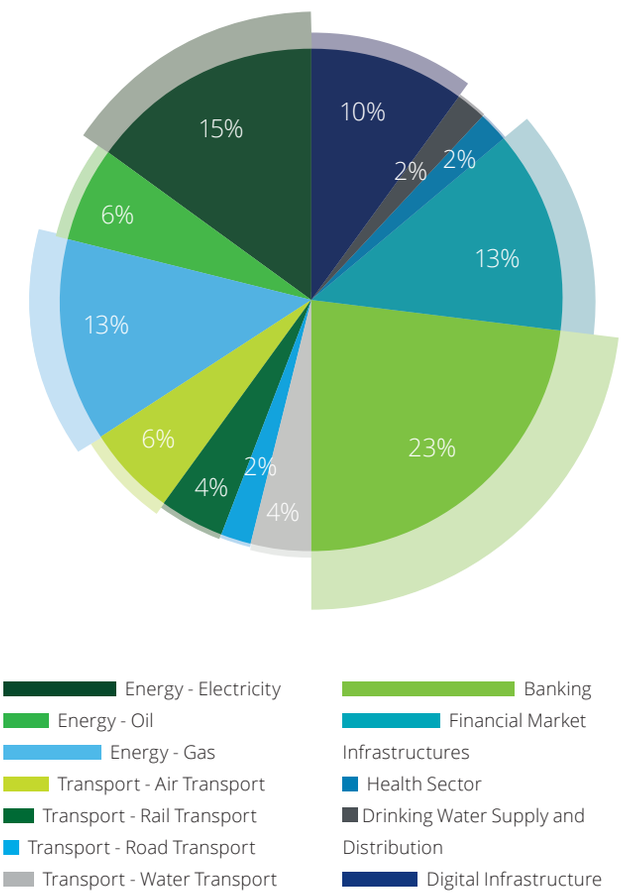
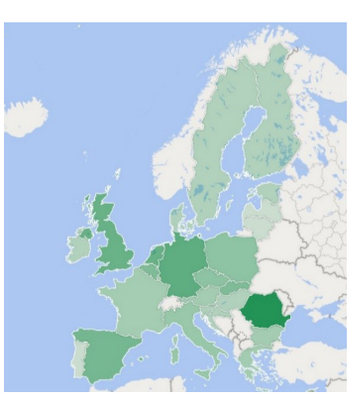


Figure 5 Covered NIS Directive sectors of OES



The sample NIS Directive stakeholders operate across the majority of all 28 Member States. This involves, in particular, OES operating and providing services cross-border in multiple Member States. This is an important element in order to understand what capabilities OES perceive important in order to comply with the NIS Directive, in particular with the incident notification. There are also emergent dependencies and interdependencies across the OES (and DSPs), which may affect the security of OES across sectors and cross-border[7].

Figure 6 Sample population of NIS Directive stakeholders that operate across the majority of all 28 Member States

2.2 Preparedness of NIS Directive Stakeholders

The NIS Directive requires OES and DSPs to take appropriate and proportionate technical security measures in order to minimise the risks of incidents affecting the security of network and information systems underlying their services. The survey investigates to what extent OES and DSPs perceive they are addressing security requirements and incident notification. In particular, the survey poses questions concerned with measures addressing risks and minimising the impact of potential incidents. The survey investigates whether OES and DSPs, in particular, 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 their operations;
- ✓ Appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems.

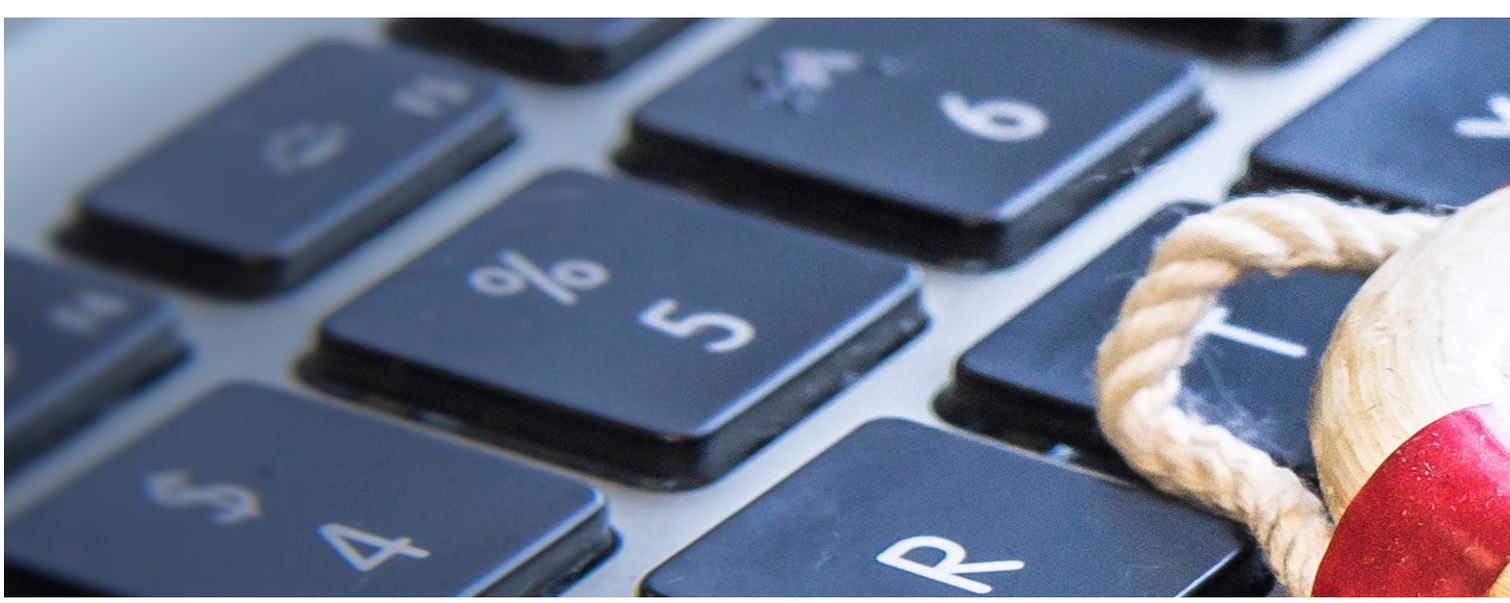
All respondents indicate that their organisations are taking appropriate and proportionate measures to manage risks and to minimise the impact of incidents. This indicates that the respondents have confidence in the overall security posture that their organisations have. Another obligation that OES and DSPs have is to notify relevant security incidents. The survey investigates whether OES and DSPs:

- ✓ Notify, without undue delay, the competent authority or the relevant CSIRT of incidents having a significant impact on the continuity of the essential services.

All respondents highlight that to a certain extent their organisations address incident notification. However, in order to investigate incident notification practices further, it is necessary to understand how OES and DSPs assess the severity of incidents and define incident notification thresholds. The NIS Directive identifies different parameters to determine the significance of the impact of an incident. In particular, the NIS Directive states that in order to determine the impact of a security incident, actors need to consider parameters such as:

- ✓ the number of users affected by the incident, in particular the users relying on the service for the provision of their own services;
- ✓ the duration of the incident;
- ✓ the geographical spread with regard to the area affected by the incident;
- ✓ the extent of the disruption of the functioning of the service;
- ✓ the extent of the impact on economic and societal activities.

Respondents highlight that organisations already consider these indicators when assessing cybersecurity incidents. In fact, these indicators are a subset of all the indicators used by organisations when assessing cybersecurity incidents (Figure 6).



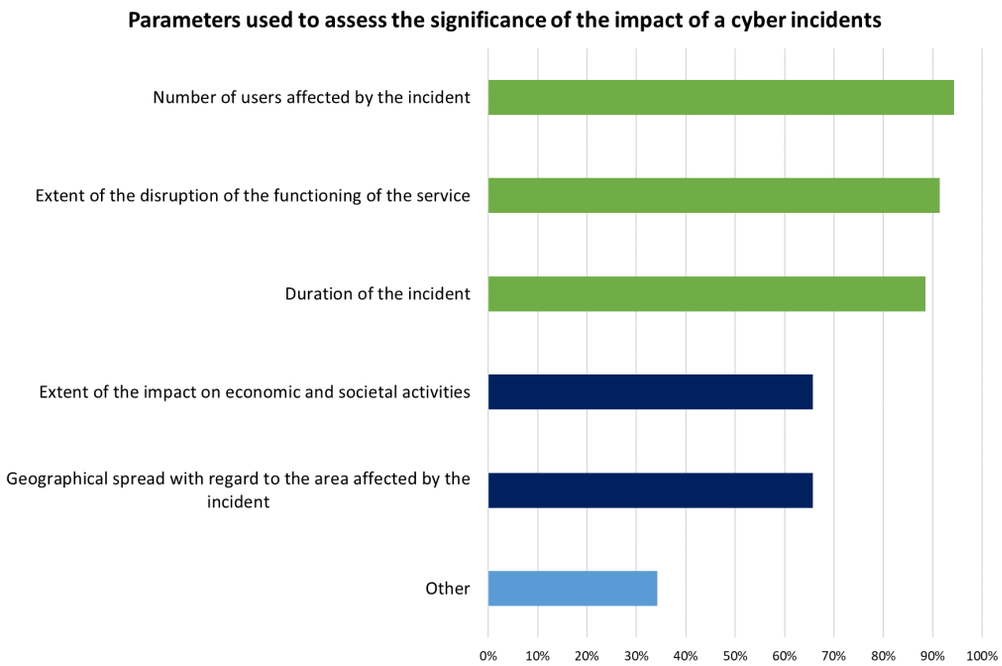


Figure 7 Parameters used to assess the significance of the impact of cyber incidents

The three main parameters that are considered by more than 80% of the organisations are the number of users affected by the incident, the duration of the incident and the extent of the disruption of the service. Close behind, more than 60% of organisations consider the geographical spread of the attack and the impact on other economic and societal activities, which could hint at an oversight to the dependencies and interdependencies of cyber incidents. Almost 40% of respondents stated that they consider other indicators when assessing cyber incidents.

2.3 Cyber capabilities for NIS Directive

The NIS Directive states that organisations need 'to take 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 the aim of ensuring the continuity of those services', not explaining specifically what those appropriate measures are. When the respondents were asked what cyber capabilities their organisation considered to be relevant to the implementation of security requirements and incident notifications, they indicated that multiple capabilities are considered. The most frequently considered capabilities according to the respondents highlights a roadmap for building cybersecurity capabilities and enhancing the maturity of OES and DSPs in alignment with the NIS Directive (Figure 7).

Technical measures are the top measures taken by the organisations, with 91.4% of the respondents saying that they consider Infrastructure Protection, Vulnerability Management and Cyber Incident Response to be relevant. Other capabilities that more than 80% of the respondents consider relevant were Cyber Risk Management and Compliance; Cyber Training, Education and Awareness; Information Privacy and Protection and Security Operations Centre. Capabilities considered by more than 70% of the respondents were Application Protection, Identity Services, Advanced Threat Readiness and Preparation, Cyber Risk Analytics and Cyber Threat Intelligence. While Cyber Strategy, Transformation and Assessment, were supported by 65.7% and cyber wargaming was supported by 37.1% of the respondents

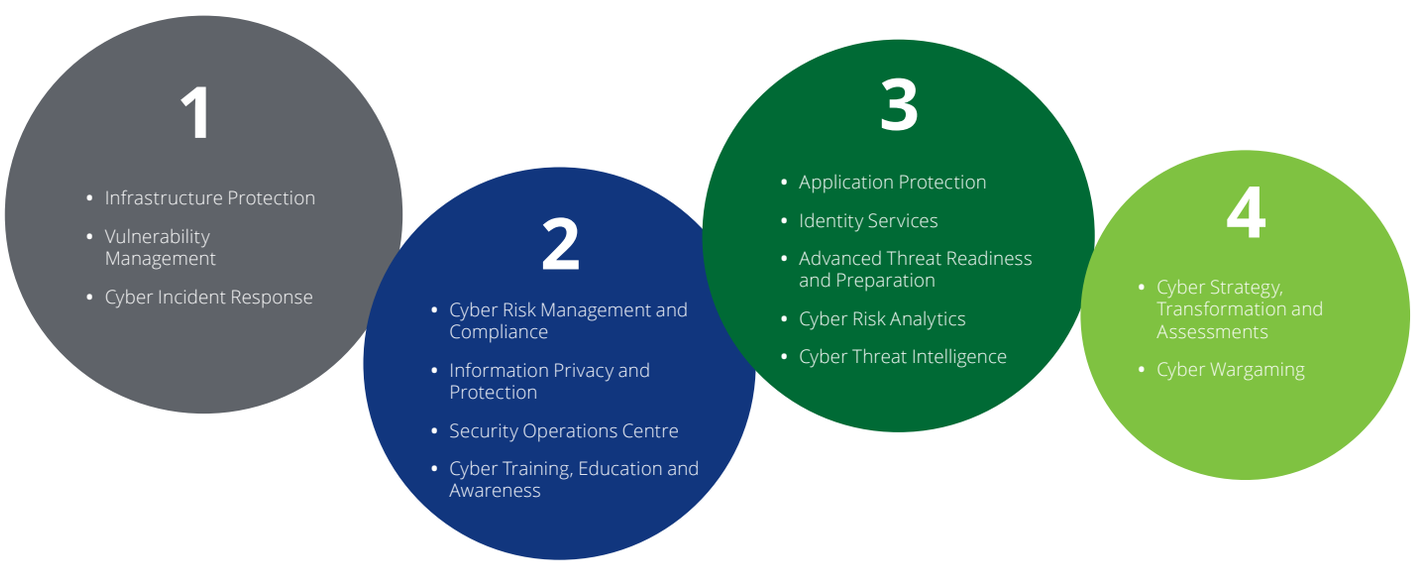


Figure 8 Cybersecurity capabilities enhancing the maturity of OES and DSPs in alignment with the NIS Directive

Belgium – ISO/IEC 27001 & 27701 - A Swiss knife for operationalising compliance in Belgium: In Belgium, the NIS Directive is implemented through the "Act establishing a framework for the security of network and information systems of general interest for public security." The law obliges the OES, amongst other things, to:

- ✓ provide a description of the network and information systems they depend on;
- ✓ 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 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 risks posed;
- ✓ take appropriate measures to prevent and minimise the impact of incidents ;
- ✓ designate a contact point; and
- ✓ conduct a yearly internal audit and a three-yearly external audit.

Article 22(1) of the law explicitly states that, until proven otherwise, the OES fulfilling the requirements of the information security management standard ISO/IEC 27001 shall be considered as complying with the security requirements embedded in Article 20 if its compliance is supported by a certification issued by an accredited certification body.

An NIS incident may be a GDPR data breach if personal data is involved. The GDPR and the NIS Directive (and their Belgian implementations) both require organisations to take appropriate

security measures and report incidents and breaches. Therefore, the Belgian authorities consider a holistic approach to tackle both information security and data protection risks as a best practice. This can be achieved by extending ISO/IEC 27001 with ISO/IEC 27701, which details the requirements and controls for a privacy information management system. Together, they form an integrated management system, which can be established in one specific project. Contact Deloitte to find out how we can help you.

3 Conclusion

The NIS Directive provides legal instruments enhancing the security of network and information systems underlying essential services in the EU. The Directive triggers the need for an extensive set of actions on behalf of organisations defined as Operators of Essential Services, Digital Service Providers, National Competence Authorities, and European institutions.
Member States were obliged to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9th November 2018. Most Member States have already transposed the Directive into their local legislation and regulations. A recent report published by the EU Commission highlights that there are inconsistencies with regards to the way the Member States identify OES across the internal market, and that some identification practices used by the Member States can potentially render entities more vulnerable to cross-border cyber-threats.

Deloitte has conducted a NIS Directive Compliance Survey that investigates to what extent OES and DSPs perceive that they are addressing security requirements and incident notification. The main findings of the survey are that the respondents indicate that their organisations are taking appropriate and proportionate measures to manage risks and to minimise the impact of incidents. Furthermore, their responses imply that to a certain extent, their organisations address incident notification.

4 About Deloitte Cyber Services

Deloitte is actively assisting a large number of stakeholders in the private and the public sector, to enhance their cybersecurity posture as well as to achieve compliance with relevant obligations as they are defined in the NIS Directive.

Deloitte is a worldwide leader in cyber risk management and has led the way through every era of cyber risk, from compliance to resilience to complexity. Our comprehensive suite of solutions cover every aspect of cyber risk management—from advisory and implementation to managed security services and incident management. We help clients perform better, solving complex problems so organizations can build confident futures.

Contacts

Thorvaldur Thor Henningsson
Director
thhenningsson@deloitte.com
+32 2 301 82 85

Massimo Felici
Manager
mfelici@deloitte.com
+32 2 302 25 81

Evert Koks
Manager
ekoks@deloitte.com
+32 2 800 23 84

Yoshi Parlevliet
Senior Consultant
yosparlevliet@deloitte.com
+32 2 600 60 00

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). ELI: http://data.europa.eu/eli/reg/2016/679/oj
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. ELI: http://data.europa.eu/eli/dir/2016/1148/oj
3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). ELI: http://data.europa.eu/eli/reg/2019/881/oj
4. European Commission (2016): Fact Sheet - Directive on Security of Network and Information Systems.
5. European Commission): State-of-play of the transposition of the NIS Directive. Last accessed 24/09/2019, Available at: https://ec.europa.eu/digital- single-market/en/state-play-transposition-nis-directive
6. European Commission (2019): Report assessing the consistency of the approaches in the identification of operators of essential services. Available at: https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services. Last accessed 04/11/2019.
7. ENISA (2018): Good practices on interdependencies between OES and DSPs.

Deloitte.