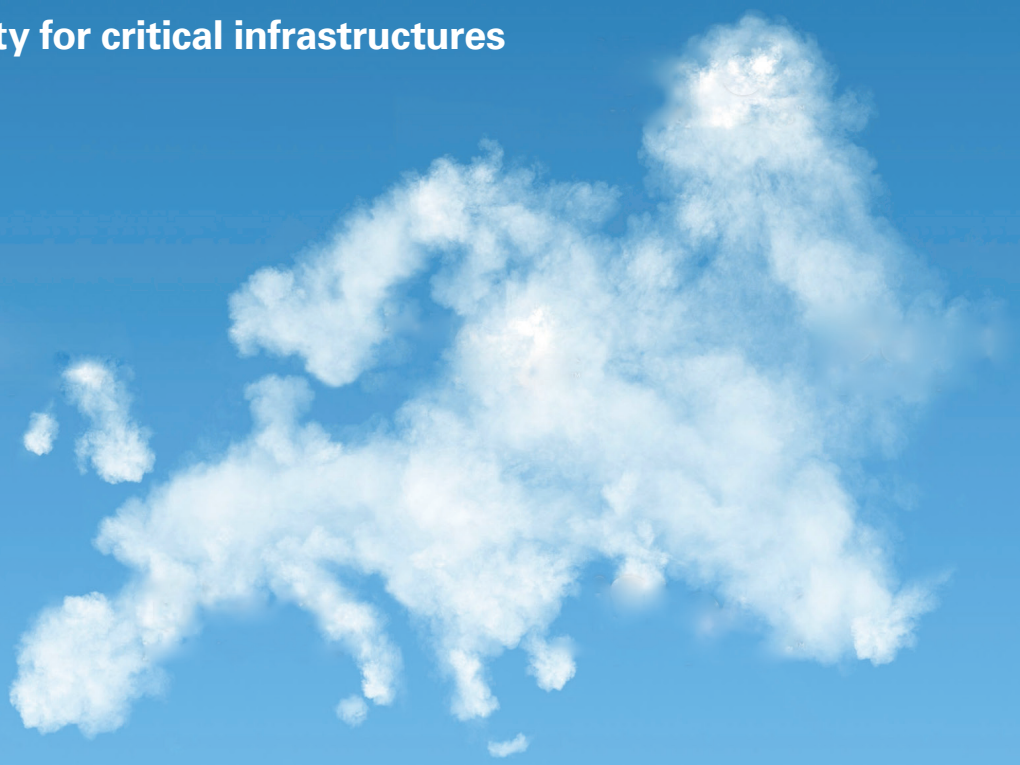
KPMG

Complying with the European NIS Directive

Cybersecurity for critical infrastructures



April 2019

kpmg.fr

Contents

Foreword

In the past decade, several cyber-attacks targeting critical infrastructures have been made public around the world. Some of these attacks on nuclear facilities, power grids, oil & gas facilities, or national Internet infrastructures have drawn considerable although ephemeral media attention. Other critical infrastructures of a nation, such as logistics and transportation infrastructures, water supplies, healthcare infrastructures, banking networks or telecommunication networks also constitute potential targets.

Although much rarer than mainstream cybercriminal activities, these incidents have naturally caused considerable concern among administrations and authorities worldwide about the cyber-risks to critical infrastructures. In response, authorities on all continents have started to lay down new cybersecurity regulatory obligations. The first of these regulations was the NERC CIP framework[1], which appeared in North America as early as 2006 for power grids and power generation facilities.

In the European Union, the different member states have historically had very different approaches to regulating the protection of their critical infrastructures, as well as very uneven levels of cyber-defence preparedness. This fragmentation in itself was recognised as a vulnerability. The NIS Directive strives to improve this situation, firstly, by increasing the cooperation between the member states on cybersecurity, and secondly, by compelling all member states to adopt more homogeneous cybersecurity regulations.

The present study provides an overview of the status of the transposition of the NIS Directive in the different member states of the EU. As this document shows, implementation the NIS Directive is facing numerous hurdles in the member states, and reaching a common level of cyber-defence across all Union remains a distant target.

For transnational operators of critical infrastructures, complying simultaneously with several distinct national cybersecurity frameworks can also prove challenging. This document identifies the common approaches that can be used by industry operators to help in these cases.

Nonetheless, in spite of these challenges, the NIS Directive is undoubtedly a step in the right direction, compelling member states that had little or no prior regulation to lay down one, or to strengthen it considerably, and introducing cybersecurity concerns.

About the Contributors

Thomas Stubbings (Austria),
Benoit Watteyne (Belgium),
Thomas Kristmar (Denmark),
Marian Corbe (Germany),
Danai Dimara (Greece),
Ahmed Amokrane (France),
Thierry Cornu (France),
Arno Sevinga (The Netherlands),
Matteo Galimberti (Italy),
Irene Sanchez Vaquero (Spain).

1 NERC CIP standard: the Critical Infrastructure Protection standard of the North American Electric Reliability Corporation (current version of standard is version 5)

Evolutions of the EU cybersecurity regulatory landscape

The EU NIS Directive

The Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) was put into effect in November 2018. The purpose of the directive is to increase cyber security across the EU.

The NIS Directive gives obligations to both member states and EU. Specifically, it lays down obligations for all member states to:

- Adopt a national strategy on the security of network and information systems;
- Establish security and notification requirements for operators and suppliers;
- Designate national competent authorities, single points of contact, and CSIRTs with tasks related to the security of network and information systems.

Additionally, it directs the EU to:

- Create a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among member states, and to develop trust and confidence among them.
- Create a computer security incident response team's network (CSIRTs network) in order to contribute to the development of trust and confidence between member states, and to promote swift and effective operational cooperation.

The NIS Directive is applicable to two types of organisations that offer services in the EU: Digital Service Providers (DSP) and Operators of Essential Services (OES). These organisations do not need to be EU based as long as they offer services in the EU.

New obligations for Operators of Essential Services

The Directive identifies seven sectors with essential services and outlines common regulatory requirements and national supervision to be applied to the Operators of Essential Services in these sectors.

The member states are required to identify their operators of essential services, that is, the entities who operate the services in the identified critical sectors. How a member state identifies an operator of essential services is decided by each member state based on national criteria.

The disruptive effect of the unavailability of a service on the member state must also be identified by member state(s) which it impacts. This will vary from member state to member state based on cross-sectorial and sector-specific factors (e.g. market shares, geographical reach).

For the identified Operators of Essential Services, member states shall ensure that the operators have taken "appropriate and proportionate technical and organisational measures" to manage the risks posed to the security of networks and information systems, which they use in their operations.

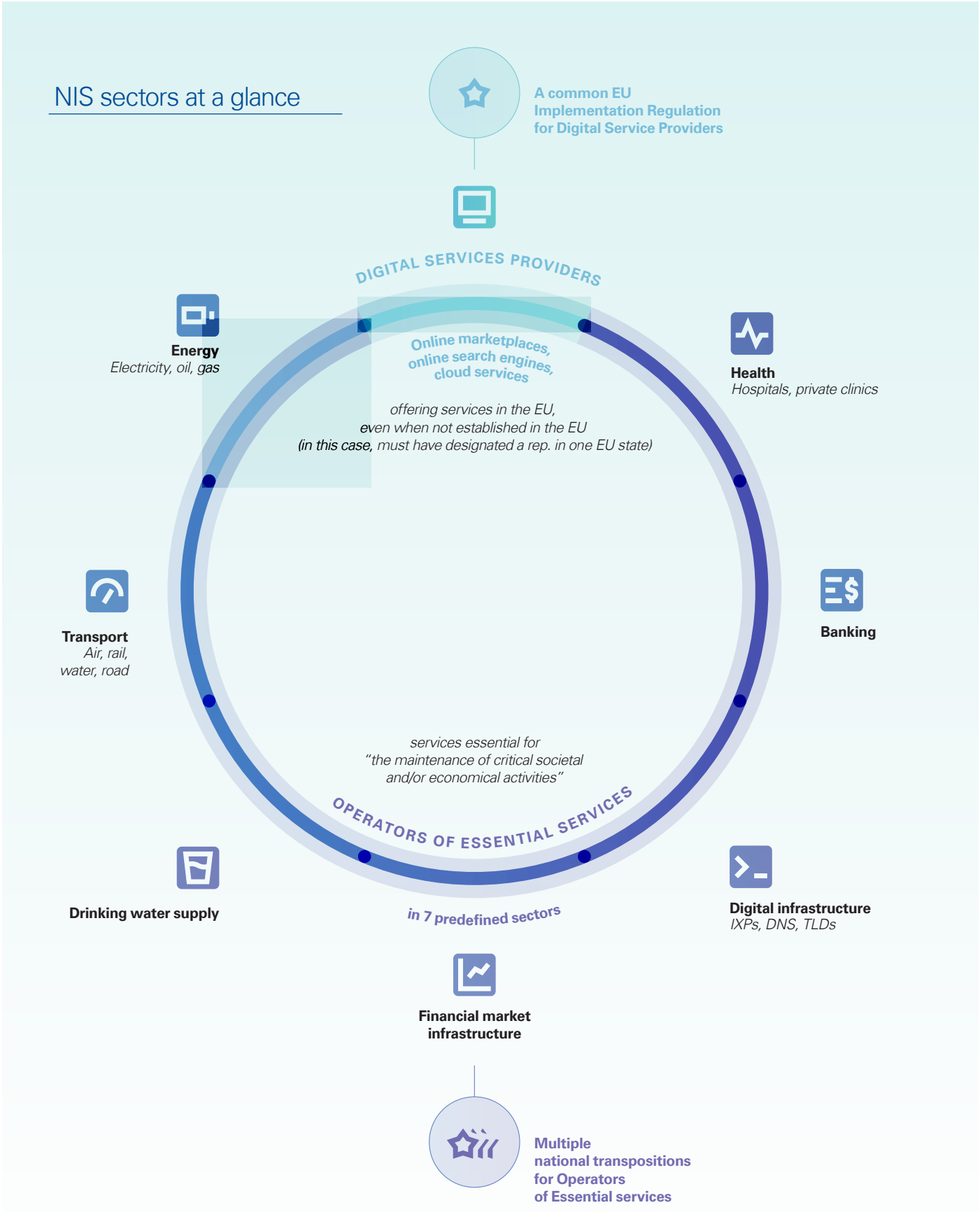
Member states shall also ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services.

What precisely constitutes "appropriate and proportionate technical and organisational measures" may vary from member state to member state. Operators' obligations are outlined in the national transpositions of the Directive, or in their supporting regulatory and procedural documents.

Digital Services Suppliers

The digital services that are addressed by the Directive include online marketplaces, online search engines, and cloud computing services. The new regulatory obligations for Digital Service Providers are delineated in an EU Implementation Regulation applicable since May 2018. Its most notable point is the introduction of the obligation for DSP to declare cyber incidents with significant impact to the competent authorities. Incidents causing unavailability of the service for more than 5 million user hours, loss of integrity, authenticity or confidentiality of data affecting more than 100,000 users, risk to public safety, public security or loss of life, and finally, damage in excess of 1 million Euro to a single user, are considered as having a significant impact.

DSP are also obliged to implement appropriate and proportionate technical and organisational security measures, but in contrast to OES, DSP are not under a regular supervisory control by the regulator. The competent authorities will act only if there is evidence that a DSP does not meet the requirements of the NIS Directive — especially after an incident.



Declaring the incidents

Member states shall ensure that OES and DSP notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. How the notification is delivered may vary from member state to member state, however, multinational entities are only required to notify the competent authority in the member state where it is headquartered. The National CSIRT will then inform other member states of the incident if the disruption affects or may affect other member states.

The diversity of national regulation frameworks

Legacy regulations, as well as the pre-existing governance frameworks of existing national cybersecurity authorities in the member states, naturally have a deep influence on how each state implements its new cybersecurity regulation framework.

These differences, as well as uneven prior levels of preparedness to cybersecurity incidents across EU member states, have led to highly diverse approaches to transposing the Directive throughout the EU. In addition, at the time of writing this document, not every EU member state has completed the transposition of the NIS Directive into its national law and regulations.

National Authorities

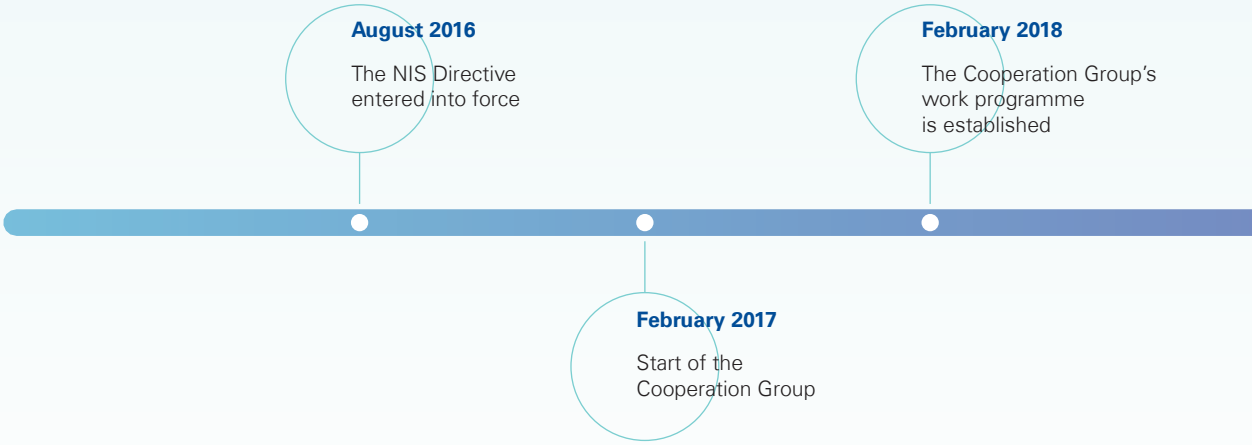
Member states are directed to designate one or more competent national authorities to monitor the application of the NIS Directive at a national level. This can be either a single authority or multiple authorities which are responsible for specific sectors.

Each member state must further delegate a single point of contact on the security of network and information system. The single point of contact (SPOC) shall liaise with other member state authorities and CSIRTs.

Most member states have delegated responsibility for the implementation of the NIS Directive to pre-existing information security agencies. Fewer countries have chosen to delegate responsibility to multiple (sector-specific) authorities.

- 16 member states have established a single competent national authority for all sectors
- 10 member states opted for multiple competent authorities (by appointing sector-specific authorities)
- 2 member states have not yet appointed any competent authorities at the time of writing this document.
- All EU member states have designated **Computer Security Incidents Response Teams** (CSIRTs) acting as point of contact for security incident reporting.

Timeline of the NIS Directive



Identification of Critical Sectors

National transpositions differ when it comes to the identification of critical sectors (Annex II of the NIS Directive). A common list of economic sectors is defined by the Directive, with the possible addition of member state-specific sectors. For instance, France and Germany added the insurance sector into their respective lists. At the time of writing, most member states have defined their critical sectors.

The definitions of essential services within each sector further differ in the degree of granularity. Some member states have chosen to include other essential services in addition to those mentioned by the Directive.

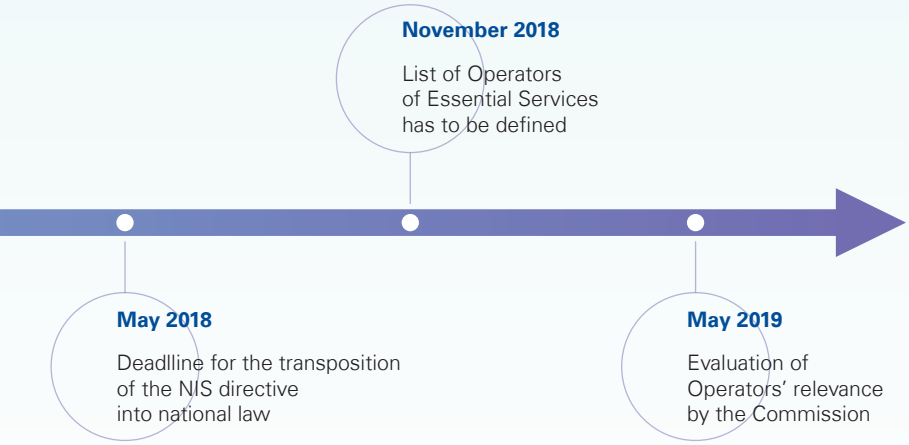
Identification of Operators of Essential Services

The identification of the Operators of Essentials Services by each member state generally follows one of two approaches:

- In a part of the member states, it is the responsibility of the operators to identify themselves as OES, based on criteria and thresholds made available publicly for each sector in the national law or regulation
- In other member states, OES are designated by the competent authorities, based on criteria that can be either public or confidential. In this case, there is usually a formal notification of OES by the competent authority (which can be opposed).

Both approaches present advantages and drawbacks. Self-assessment places less burden on the authorities, but some OES might simply not report themselves. In contrast, when the authority undertakes to designate the OES, it needs in-depth knowledge of the sector and of its business. In all cases, establishing the list of the OES remains a complex venture.

As an illustration of these challenges, approximately two thirds of the EU member states had not identified all OES yet by the reporting date to the European Commission on 09 November 2018.



Variety in the definition of Essential Service

The NIS Directive defines an operator of essential services as a public or private entity in one of the critical sectors identified in the Directive whose criteria for identification are:

(a) an entity provides a service which is essential for the maintenance of critical social and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

This terminology remains intentionally vague. As a result, some authorities struggle to interpret this and to decide when a service should be considered essential. As an example, how many users a water distribution service or a railway transportation service should have before being considered essential, may differ from one member state to another. The definition of the notion of Essential Service was also changed and/or amended by several member states while creating their national transposition. This has an adverse effect on the clarity for cross-border operators of essential services.

The weight of legacy in upcoming regulation

One of the main reasons for the creation of the NIS directive was the fact that not all of the EU member states had cybersecurity legislation in place. To be able to give some insight into the journey some countries have gone through and the diverse starting points they had, we have collected the pre-existing legislations and noted when there is no pre-existing legislation.

CAPTION

Authority & CSIRT

- Single authority
- Multiple authorities
- Single CSIRT
- Multiple CSIRT

Information

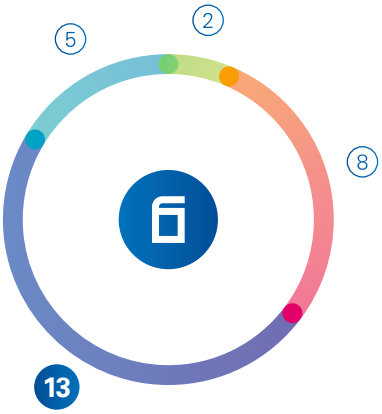
- Incomplete information
- Not defined yet

Country	Pre-existing Legislation	Year of Implementation	Specific Sector Acts	Authority	CSIRT
Austria	–	–	✓	Multiple authorities	Single CSIRT
Belgium	✓	2011/2016	–	Multiple authorities	Single CSIRT
Bulgaria	✓	2016	–	Incomplete information	Not defined yet
Croatia	Incomplete information	Incomplete information	Incomplete information	Multiple authorities	Multiple CSIRT
Cyprus	Incomplete information	Incomplete information	Incomplete information	Single authority	Single CSIRT
Czech Republic	✓	2014	–	Single authority	Single CSIRT
Denmark	–	–	✓	Multiple authorities	Single CSIRT
Estonia	✓	2017	–	Single authority	Multiple CSIRT
Finland	–	–	✓	Multiple authorities	Multiple CSIRT
France	✓	2016	–	Single authority	Single CSIRT
Germany	✓	2009	–	Single authority	Single CSIRT
Greece	–	–	–	Single authority	Not defined yet
Hungary	✓	2017	–	Single authority	Single CSIRT
Ireland	Incomplete information	Incomplete information	Incomplete information	Single authority	Not defined yet
Italy	✓	2012	–	Single authority	Single CSIRT
Latvia	Incomplete information	Incomplete information	Incomplete information	Multiple authorities	Single CSIRT
Lithuania	✓	2016	–	Single authority	Single CSIRT
Luxembourg	Incomplete information	Incomplete information	Incomplete information	Incomplete information	Incomplete information
Malta	✓	2011	–	Single authority	Single CSIRT
Netherlands	–	–	✓	Multiple authorities	Single CSIRT
Poland	✓	2017	–	Multiple authorities	Multiple CSIRT
Portugal	Incomplete information	Incomplete information	Incomplete information	Single authority	Single CSIRT
Romania	Incomplete information	Incomplete information	Incomplete information	Single authority	Single CSIRT
Slovakia	✓	2015	–	Single authority	Single CSIRT
Slovenia	–	–	–	Single authority	Single CSIRT
Spain	✓	2010	–	Single authority	Multiple CSIRT
Sweden	Incomplete information	Incomplete information	Incomplete information	Multiple authorities	Single CSIRT
United Kingdom	–	–	✓	Multiple authorities	Single CSIRT

Regulation

Pre-existing Legislation

- Sectorial only
- Full CIP legislation
- Partial
- None

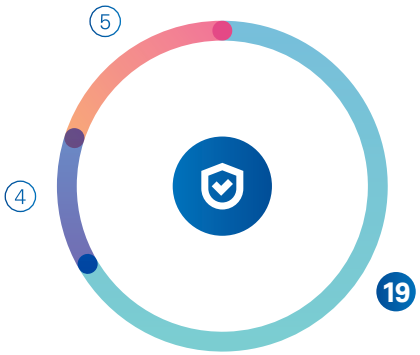


Nearly half of the EU member states did have some pre-existing legislation or regulation regarding Critical Infrastructure Protection, prior to the implementation of the NIS Directive.

Even though these pre-existing frameworks did present a very uneven level of maturity from one country to another, the weight of legacy in the transposition of the NIS Directive is present in many member states.

CSIRT

- Single CSIRT
- Multiple CSIRT
- Not defined yet

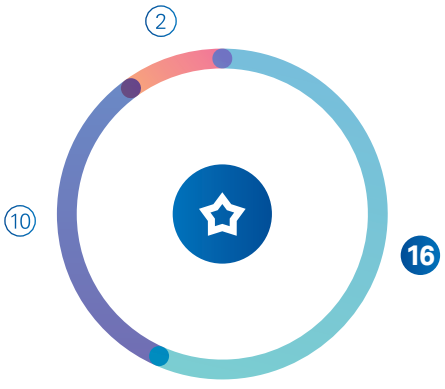


A majority of EU member states have selected an organisation with a single Computer Security Incident Response Team (CSIRT) at nation state level. For instance, member states that already have regulations similar to the NIS directive, have identified CSIRTs

Those retaining a more complex scheme with multiple CSIRTs often do it due to a pre-existing legacy organisation (usually, pre-existing national CSIRTs competent by sector). The NIS Directive will compel these states to improve the cooperation between their various national CSIRTs, thus improving their capability to deal with a cross-sector or nation-wide cybersecurity incidents.

Authority

- Central authority
- Multiple authorities
- Not defined yet



Slightly more than half of the EU Member States have designated a single central regulatory authority. However, about a third of the Member States retain several regulatory authorities, on a sectorial basis. For these states, one of the authorities had to be designated as the single point of contact for the member state at European level. Once again, in these cases, the implementation of the NIS Directive also results in a better coordination at national level.

Top challenges for operators

Operators required to implement the NIS Directive and its local transposition face a number of challenges, both technical and organisational.

Identifying and delineating critical digital assets and networks

The first step for every operator is to identity critical assets and networks that are in scope. This can be a subset of systems or business processes, an entity/department within the organisation, or the whole organisation, depending on the organisation's size and activity as well as the country's regulation in place within the member state where it is headquartered / conducts its activities.

Orchestrating the risk identification, risk analysis and the risk acceptance process across the organisation

Most compliance frameworks rely on an initial high-level risk analysis, on the building of the corresponding risk mitigation plan, and finally on the formal acceptance of the residual risks by the organisation's management.

Orchestrating this analysis across the organisation, and involving all entities, departments and activities in developing a common vision of the risks, can be a complex undertaking, especially for organisations unfamiliar with this kind of formal process.

Complying with diverse national frameworks for multinational organisations

For operators of essential services who provide essential services in multiple member states, compliance with the local transposition of the directive needs to be achieved in every country. Compliance frameworks may vary widely, and a common baseline must be defined first. In addition, in some countries the compliance processes require the use of local language and templates.

Managing suppliers and contractors

Part of the critical systems supporting essential services may be maintained, or even operated, by external suppliers or contractors. This is especially frequent in the case of industrial systems and control systems.

The compliance requirements have to be cascaded to the various contractors, headquartered in the EU or not, and pre-existing contracts may need to be revised. Some core activities may even have to be internalised by the operator when closely linked to security.

Declaring incidents and reporting to authorities

With the NIS Directive in place, operators of essential services are required to report serious cyber security incidents, including data breaches, to the national competent authorities within a specified time. For some operators this is an additional reporting line (depending on sector regulations). The reporting requires new processes (means of communications, templates for declaration, content of the declaration, etc.) and responsibilities within the organisation, also considering the penalties applicable for late reporting.

Implementing effective security incident detection and response processes

Incident detection and incident response are two of the key capabilities that operators need to develop. These processes will be composed of procedures for reaction, escalation, and contingency plans, as well as technical solutions for detection and response such as Security Information and Event Management (SIEM) solutions and Security Operational Centres (SOC).

Some industry sectors, such as banking or telecommunications, are significantly mature in this area, while others may have to reinforce their detection and incident response capabilities considerably, or even build them from scratch.

Managing the regulatory complexity in four steps

In spite of the diversity of regulatory obligations between EU member states, there are common steps that Operators of Essential Services in all countries can undertake to secure their essential systems, and that will be applicable to all regulatory approaches.

For multinational operators, these steps also lay down the foundation for a common in-house framework and policy, allowing compliance simultaneously with several distinct national regulations.

KPMG's security compliance approach comprises four steps:

- Identifying your critical digital assets
- Defining your security maturity target state
- Reaching compliance
- Maintaining compliance over time

Identifying your critical digital assets

Identifying your critical digital assets and the boundary separating critical from non-critical assets is a key initial step, as it will help in defining those assets to which the regulatory controls will actually apply.

The electronic communications crossing the boundary between zones with critical and non-critical assets need to be identified. Once identified, the security of this communication needs to be reviewed in great detail.

A key challenge when identifying the critical assets is to inventory the technical interdependencies between systems, especially when these interdependent systems are owned and operated by different asset owners within a business. For instance, if a mission critical industrial system server depends on the availability of an Active Directory Domain Controller for its operation. Then this Domain Controller should be considered a part of the critical digital assets too, and should be protected accordingly.

Defining your security maturity target state

Before starting any security improvement project, it is good practice to define the desired target state for the security posture. This target state usually comprises a number of in house rules to be complied with, both organisational and technical, together with overall technical architectures, security solutions to be implemented, and security controls to be instituted.

Compliance in 4 steps: the KPMG method

1

Identifying your critical digital assets

High level risk analysis

Identify the critical business processes for providing your Essential Services

Analysis of dependencies

List the digital assets supporting these processes, as well as the assets they depend upon to operate

Identification of the boundaries

Delineate the digital security perimeter separating your critical assets from the other assets

2

Defining your security target

Regulatory requirements inventory

List the mandatory security controls for the national regulation(s) with which you need to comply

Detailed risk analysis

Conduct a detailed risk analysis for each critical system, taking into account the identified boundaries

Definition of security target & strategy

Define the security target & strategy incl. policies, company rules and technical architecture to reach compliance

KPMG

Most national cybersecurity regulations impose a combination of a compliance-based approach (mandatory controls) and a risk-based approach (conduct a specific analysis). Therefore, the security target will include a combination of the mandatory controls for the various regulations needed to achieve compliance, as well as additional controls based on the results of the mandated risk analysis conducted on the critical systems.

When defining the strategy to reach the target state, it is essential to pursue an integrated approach considering the plethora of regulations, standards and requirements the specific industry is obliged to follow. Only with an integrated approach, it is possible to assure coverage of all requirements while avoiding duplication of efforts.

Reaching compliance

Being able to measure the gap between the current state and the desired end-state is a powerful indicator and enabler for the organisation, not only to design the action plan required, but also to measure its progress.

This is especially the case when multiple sites or systems have to become compliant simultaneously: in this case, the gap assessment by site becomes the primary tool to drive the entire compliance program.

Developing a road map of prioritised implementation steps is usually helpful to achieve compliance in a phased approach, especially when there are multiple sites involved.

Maintaining compliance

Once compliance is reached, being able to maintain the attained level of security and compliance in the long term requires planning ahead. Dashboards and key performance indicators should be used to monitor the application of the defined controls, internal audits (and in some regulatory frameworks also third-party audits) should be conducted periodically; and finally the risk analyses themselves should be reassessed at regular intervals.

Some member state regulations recommend the use of international standards such as ISO 27001 as a way to establish a sustainable Information Security Management System (ISMS), while others lay down their own specific management frameworks and obligations.

Building close contacts with relevant authorities and peer groups helps developing a balanced and adequate approach for reaching and maintaining compliance and enabling a continuous improvement process.

Reaching compliance

Gap analysis

For each critical system or site, assess the current state and list the gaps with the target state

Roadmap definition

Develop an action plan to remediate the gaps and reach security target

Roadmap implementation

Implement the actions and monitor progress

Maintaining compliance

Control and monitor

Implement controls and KPIs to ensure that security controls continue to be implemented correctly over time

Audit

Commission third-party audits regularly

Reassess risks and update as needed

Periodically reassess your risks, and update target and controls accordingly

Beyond check-the-box compliance

The temptation of minimal compliance

Introduction of new regulations frequently prompts the same initial question from the companies which are to be regulated: how to reach compliance with minimal effort and cost.

Since many operators have to conduct business in a highly competitive economic environment, with stringent cost reduction objectives and compliance with multiple regulations at the same time, this baseline compliance attitude is not, after all, unreasonable.

However, following a regulation to the letter but ignoring its larger meaning may expose operators to risks.

The most obvious of them is that a minimal compliance approach simply misses the intended objective: in this case, improved cybersecurity. Money invested in maintaining a façade of compliance but with little or no actual security benefit is not money well spent. Therefore, the question that upper management should ask themselves is: how will we reap the maximum benefit from these new, mandated expenses? To answer this question, organisations need to change their point of view and regard regulation not only as a burden but also as an opportunity.

Another potential pitfall is that, in the event of a major cybersecurity incident, demonstration of minimal compliance efforts will not, in most cases, exonerate the organisation. Authorities are more and more inclining to seek operators' liability beyond apparent compliance.

Finally, a pure check-the-box approach may not be sufficient to comply with the national and sectorial regulatory frameworks derived from the NIS Directive. Regulatory authorities being more aware today of the drawbacks of compliance-only approaches, many have designed their national NIS Directive transpositions to include a risk-based approach: operators are required to conduct a risk analysis, and to tailor their security baseline according to its results.

As a consequence, operators are left with the task of interpreting the regulatory criteria, adapting them to their own situation, weighting their risks, and finally making decisions and engaging their responsibility on which security controls they decide to implement and which they do not.

Towards risk-based compliance

Although more complex than a checklist process, the risk analysis process, if conducted correctly, is a unique opportunity for operators to become compliant in a smart way. Especially, it should allow them to:

- Restrict the scope of critical regulated systems to what is strictly necessary, but without omitting any component critical to the essential services
- Justify derogations to mandatory requirements if the analysis shows that they bring no added security benefit for the essential services
- Go beyond check-the-box compliance and focus on the actions that count to improve security for the systems for which it really matters

Company reputation and societal impact

The essential services impacted by the NIS Directive are the major services that affect the daily life of the citizens of Europe. Therefore the NIS Directive is not just the opportunity to reevaluate your level of protection for the systems that matter the most, but the opportunity to:

- Be responsible for the interests of the public in the countries where your company has an impact.
- Reduce the risk of negatively impacting on your company's reputation, and create added value by improving the confidence of business partners, clients, and the public.

Our NIS Directive and Critical Infrastructure experts

The KPMG NIS Directive Working group is composed of cybersecurity experts from all EU member states. As the Directive and its transpositions come to play across the EU, the working group is committed to regularly updating the present synthesis, taking account of the regulatory changes occurring in the different member states of the EU.

KPMG

Your contacts in France…

Vincent Maret
Partner
Tél. +33 6 17 12 22 13
vmaret@kpmg.fr

Thierry Cornu
Director
Tél. +33 6 77 64 88 77
tcornu@kpmg.fr

Ahmed Amokrane
Manager
Tél. +33 6 10 24 51 71
aamokrane@kpmg.fr

… and in the European Union

Austria
Andreas Tomek
atomek@kpmg.at

Belgium
Benny Bogaerts
bbogaerts@kpmg.com

Bulgaria
Krasimir Ivanov
kkivanov@kpmg.com

Croatia
Daniel Lenardic
dlenardic@kpmg.com

Cyprus
Christos Yiacoumis
christos.yiacoumis@kpmg.com.cy

Czech Republic
Martin Hladík
martinhladik@kpmg.cz

Denmark
Morten Klitgaard Friis
mortenkfriis@kpmg.com

Estonia
Teet Raidma
traidma@Kpmg.com

Finland
Mika Laaksonen
Mika.Laaksonen@kpmg.fi

France
Vincent Maret
vmaret@kpmg.fr

Germany
Uwe Bernd-Striebeck
uberndstriebeck@kpmg.com

Greece
Efi Katsouli
ekatsouli@kpmg.gr

Hungary
Tamas Korasz
Tamas.Korasz@kpmg.hu

Ireland
Michael Daughton
michael.daughton@kpmg.ie

Italy
Luca Boselli
lboselli@kpmg.it

Latvia
Kaspars Iesalnieks
kiesalnieks@kpmg.com

Luxembourg
Laurent de la Vaissiere
laurent.delavaissiere@kpmg.lu

Netherlands
John Hermans
Hermans.John@kpmg.nl

Poland
Michal Kurek
michalkurek@kpmg.pl

Portugal
João Madeira
jmadeira@kpmg.com

Romania
Mihai Gabriel Tanase
mtanase@kpmg.com

Slovak Republic
Pavol Adamec
padamec@kpmg.sk

Slovenia
Matjaz Pusnik
marcmartinez@kpmg.es

Spain
Marc Martinez Marce
email@kpmg.fr

Sweden
Peter Lind
peter.lind@kpmg.se

United Kingdom
Martin Tyley
martin.tyley@kpmg.co.uk

Conception: Marketing — OLIVER — April 2019.

Photo Credits: ArtJazz / iStock, Samuel Zeller / Unsplash