Cetome
Securing a Better Future

White Paper

INTRODUCTION TO THE NIS DIRECTIVE

April 2019

Author: Dr. Cédric LEVY-BENCHETON, CEO

Table of Content

INTRODUCTION

WHY THE NIS DIRECTIVE?

THE CONSEQUENCES OF A CYBER ATTACK

THE NIS DIRECTIVE OR THE "GDPR OF CRITICAL INFRASTRUCTURE"

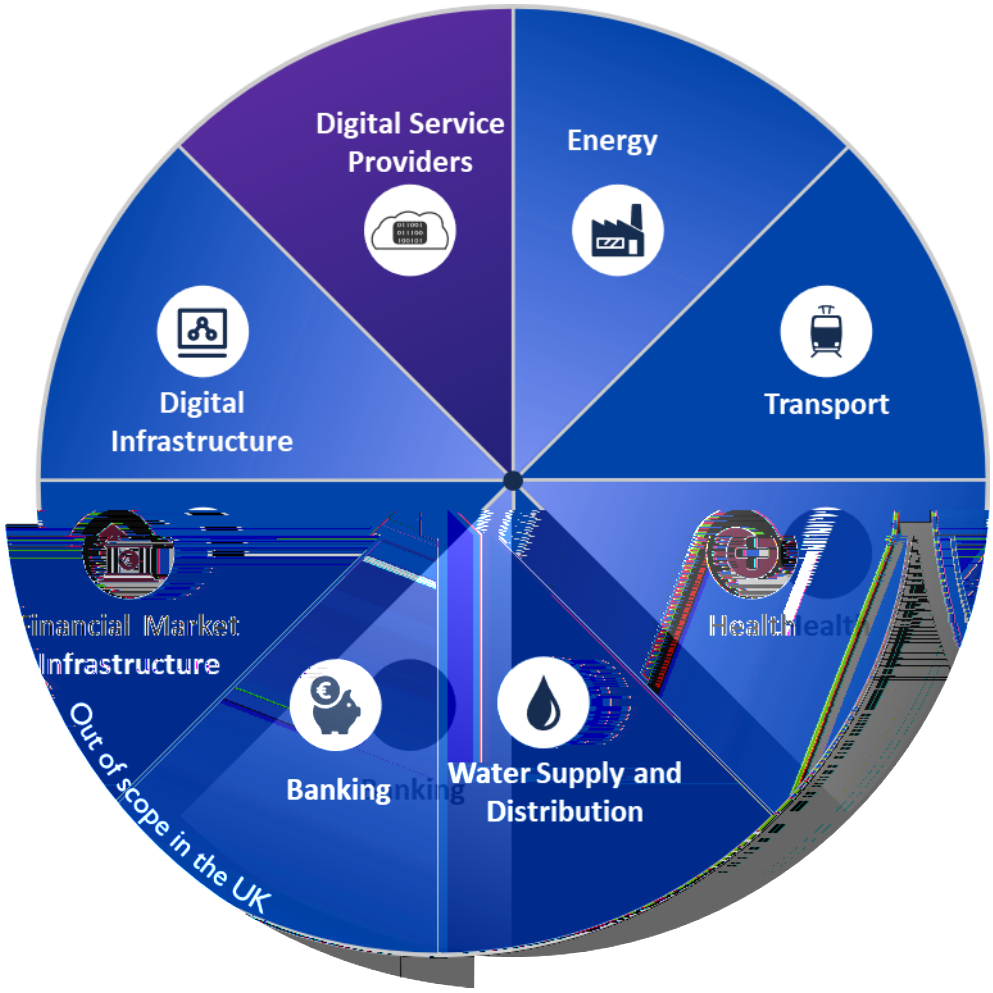


Figure 1. Sectors in Scope of the NIS Directive

- **Operators of Essential Services**

- **Digital Service Providers (DSP) that are**

For more information, please refer to the "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".

SECURITY REQUIREMENTS IN THE NIS DIRECTIVE

Security Measures for Operators of Essential Services

Operators of essential services 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 risk posed.

appropriate and proportionate

Security Measures for Digital Service Providers

"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."

INCIDENT NOTIFICATION

significant impact on the continuity of service

-
-
-

substantial impact on the provision of service

-
-
-
-
-

ENFORCEMENT AND PENALTY

WHY TAKE A LEGAL APPROACH?

CONCLUSIONS

ABOUT CETOME

Cetome
Securing a Better Future

The NIS Directive – The GDPR of Critical Infrastructure

Several recent cyber attacks have disrupted critical national infrastructure with an impact on our economy and our safety. For this reason, the European Union and its Member States (including the UK) have voted the NIS Directive to better protect our society from cyber risks.

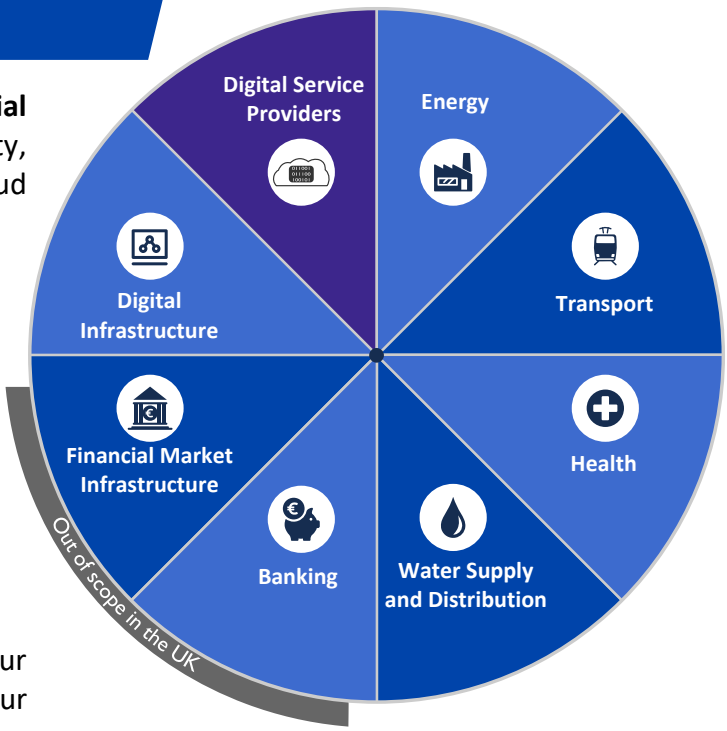
Where does it apply?

The NIS Directive applies to **Operators of Essential Services** who provide a service vital to the society, and to **Digital Service Providers** who operate Cloud services, search engines or online marketplaces.

The sectors in scope must:

- Implement appropriate and proportionate organisational and technical security measures.
- Notify significant cyber incidents to their Competent Authority without delay.

or face an important penalty!



You must comply with the NIS Directive if your organisation meets the criteria established by your Competent Authority.

Objectives of the Directive

- Understand and prevent **cyber risks** by securing network and information systems
- Augment the preparedness and **trust in critical infrastructure** across Europe and the UK
- Ensure the thorough implementation of **good security practices and cyber resilience**
- Handle incidents to **minimise impact on service** and develop lessons-learned

Compliance Timeline

NIS Directive adopted by the European Parliament
Summer 2016

May 2018
Governments published their transposition into local regulation

Governments have identified Operators of Essential Service
November 2018

Starting April 2019
Operators of Essential Services must:

- Ensure they have a security governance
- Map their gaps and risks
- Identify appropriate and proportionate security measures
- Communicate an improvement roadmap to their regulator

Operators of Essential Services must:

- Complete the deployment of appropriate and proportionate security measures
- Measure their security performance
- Demonstrate improvements in compliance

Before November 2020

Cetome is an **independent security csD 1Sun** wcopec essdenial( )-[ssD Ser)-Vicest

ifrastrucsD Pu rraondsot vndors(Po esD Sure thme)