Cetome
Securing a Better Future

White Paper

THE NIS DIRECTIVE IN THE UK

April 2019

Author: Dr. Cédric LEVY-BENCHETON, CEO

Table of Content

INTRODUCTION

THE NIS REGULATIONS

-
- **OES**
  RDSP
-

Note: the NIS Regulation does not apply to Banking and Financial Market Infrastructures as equivalent EU legislation applies.

ROLES AND RESPONSIBILITIES

OPERATORS OF ESSENTIAL SERVICES

Competent Authorities

i.e.

Note: The list of competent authorities is available in Schedule 1 of the NIS Regulations.

Computer Security Incident Response Team (CSIRT)

Single point of contact (SPOC)

Technical Authority

-
-

Note: The technical authority is not defined legally in the NIS Regulation. This role and its responsibilities appear in the DCMS "NIS Guidance for Competent Authorities", which explains how the NIS Regulations should apply in the UK.

The NIS Cooperation Group

Note: All UK interactions with the NIS cooperation group shall pass through the DCMS.

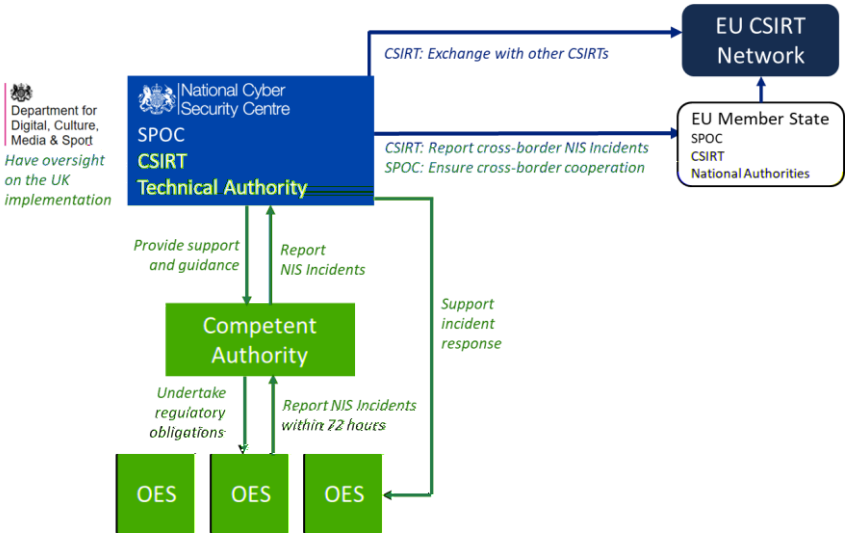


Figure 1. Summary of interactions in the UK (non-exhaustive)

THE NIS REGULATIONS FOR OESs AND RDSPs

OBLIGATIONS OF OESs AND RDSPs

-
-
-
-
-

SELF-ASSESSMENT [OES ONLY]

Note: At the time of this writing, this approach is not formalised for RDSPs. CAs are currently reviewing the first self-assessments for OESs.

Improvement plan [OES Only]

Note: To support this phase, the NCSC and CAs can develop "profiles" that emphasize specific areas of improvement. Again, this approach is not formalised for RDSPs at the time of this writing.

Collaboration with their Competent Authority

Note: If an OES is reliant on a RDSP, the OES must notify its Competent Authority (and not the ICO) as soon as the NIS Incident occurs.

Implementation Roadmap [Focus on OES]

THE NIS REGULATIONS FOR CAs

FORMAL NOTICES

- **Information notices**

- **Enforcement notices**

- **Penalty notices**

e.g.

POWER OF INSPECTION

-
-
-

Note: At the time of this writing, there is no approved list of third-party inspectors.

ENFORCEMENT AND PENALTIES

ENFORCEMENT

Note: For the first year, it is recommended that CAs take a cautious approach to enforcement

PENALTIES

e.g.

-
-
-
-

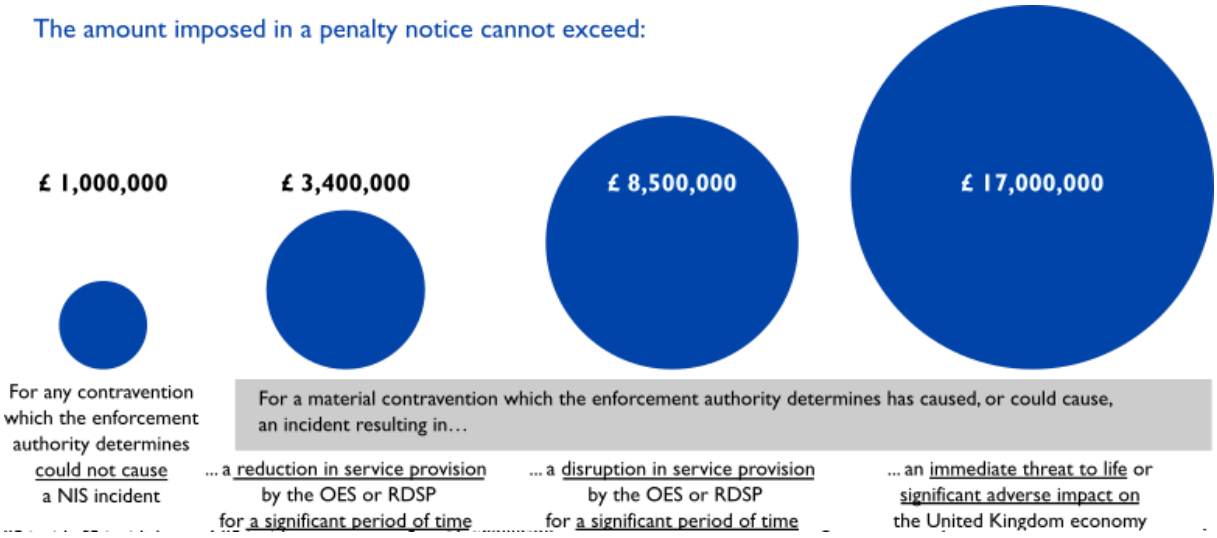


Figure 2. Penalties in the UK

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.

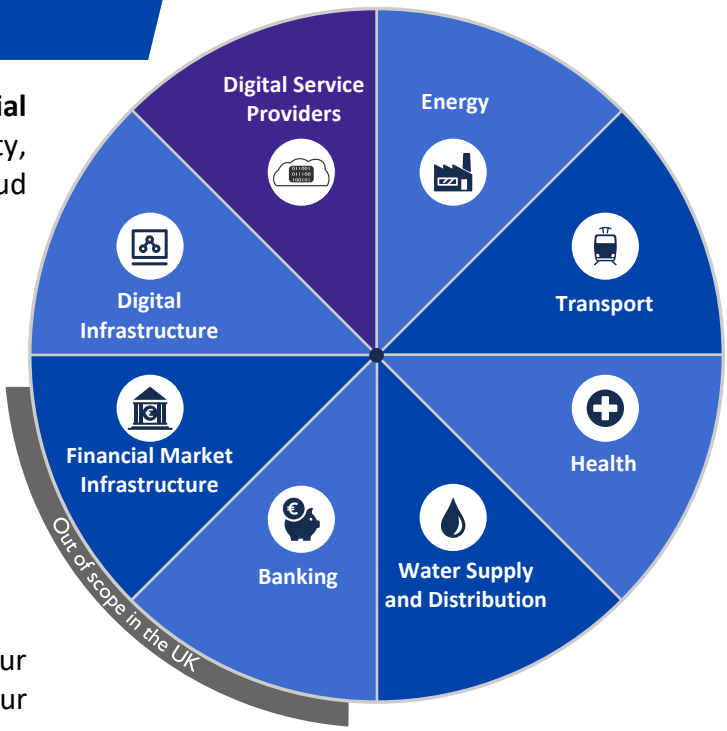
Where does it apply?

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)