Policy report: Network and Information Systems: improving implementation

Website: https://www.ucl.ac.uk/steapp/policy-report-network-and-information-systems-improving-implementation

The Government should focus on cross-sector dependencies and improve its approach to assessing compliance if the cyber security of critical national infrastructure is to be improved.

About this briefing

The Network and Information Systems (NIS) Regulations came into force in May 2018. They aim to improve the way that cyber risks are managed in Critical National Infrastructure (CNI) sectors.

This briefing is based on research carried out between March and August 2018 the purpose of which was to explore how cyber resilience risk management is implemented in the UK's CNI sectors that are subject to the Regulations. The objective was to study the effectiveness of the NIS regulations in bringing about a step-change in cyber security risk management across the UK's CNI sectors.

We recognise that since the research was conducted, the government has carried out a post-implementation review of the NIS regulations and will be making some amendments to the regulations as a result. The next review is due in 2022.

Key findings

Improving risk management capabilities

The Government does not have a way of measuring whether the overarching aim of boosting the level of security of network and information systems for critical national infrastructure has been met. We suggest that a set of Key Performance Indicators (KPIs) should be developed for this purpose.

The Cyber Assessment Framework (CAF) provides a good first step in helping organisations to understand how they can improve their resilience. We suggest that organisations now need a more tailored roadmap of steps for improvement, which should be based on a clear understanding of how critical that organisation is towards maintaining end-to-end services as well as how critical each outcome within the CAF is to maintaining that organisation's operations.

Cross-sector security and resilience

Different Competent Authorities (CAs) are responsible for oversight and enforcement in each of the six sectors covered by the NIS regulation. However, some services rely on more than one type of infrastructure. For example, a train service relies not only upon transport infrastructure, but also energy and digital infrastructure. There is currently no way to understand or measure the resilience of an end-to-end service, and cross-sector dependencies need to be better understood and incorporated into the implementation of the NIS.

There also needs to be a mechanism to share lessons learnt between sectors. We suggest developing a 'lessons learnt framework' that could be incorporated into all self-assessments.

Assessing compliance with the NIS

There is room for improvement in the way that compliance is assessed. First, a central audit methodology should be developed, that can then be applied by all the CAs.

Second, auditors must have the appropriate skills (including cyber security, risk management, business assurance and audit skills). Using cross-disciplinary teams may be one way to achieve this.

Glossary

CA	Competent Authority
CAF	Cyber Assessment Framework
CNI	Critical National Infrastructure
DSP	Digital Service Providers
DSPT	Data Security and Protection Toolkit
IGPs	Indicators of Good Practice
IT	Information Technology
NIS	Networks and Information Security
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
OT	Operational Technology
RDSP	Relevant Digital Service Provider

Introduction

Attacks on Critical National Infrastructure (CNI) are becoming increasingly common.In recognition of the growing threats of cyber-physical attacks, the EU launched the Networks and Information Security (NIS) Directive on 6 July 2016 to "improve the EU's preparedness for cyber-attacks".[i]

The objectives of the NIS Directive can be summarised as:

1. To raise the security levels and resilience of CNI Operators of Essential Services (OES) and Relevant Digital Service Providers (RDSP) by supervising and bringing a step change in how cyber risks are managed.
2. To create a forum between EU countries to establish communications specific to cyber security incidents to improve the level of protection, and to provide an overarching regulation covering all EU countries.
3. To ensure that the OES and the RDSP take "appropriate and proportionate security measures" across sectors using a national legal framework and notify the relevant national authorities of serious incidents.[ii]

Under the NIS Directive, the organisations identified as an OES or RDSP are required to take "appropriate and proportionate security measures to manage risks to their network and information systems".[iii] In addition, they must report any serious incidents to the relevant

authority. The NIS Directive also requires that member states nominate at least one Competent Authority (CA), who is responsible for assessing and enforcing compliance with the regulations. In the UK, different CAs have been appointed in each of the sectors covered by the legislation.

The NIS Directive was transposed to UK law as The Network and Information Systems (NIS) Regulations in 2018 and cover OES in health, transport, energy, water, digital infrastructure and digital services sectors.[iv]

Requirements on RDSPs (such as cloud service providers, online market places and search engines) are lighter touch: the Directive provides for *ex post* supervision of RDSPs as opposed to the much more proactive and involved approach to OES.

The CAs must assess whether OES/RDSPs are achieving the principles and determine what constitutes "appropriate and proportionate measures" in their sector. To achieve this, the National Cyber Security Centre (NCSC) has developed a Cyber Assessment Framework (CAF) which CAs, OESs and RDSPs can use for their assessments (this is a voluntary framework; it is not mandatory for the CAs to use it).[v] The CAF uses an "outcome-based" cybersecurity risk management approach. This means that rather than providing a prescriptive set of rules for OES/RDSPs to follow, the CAF provides a set of 14 top-level cyber security principles designed to collectively describe good cyber-security practice. Under each of the 14 principles there is a set of 39 lower-level outcomes, along with Indicators of Good Practice (IGPs) for each outcome, which can be used to assess whether outcomes are 'not achieved', 'partially achieved' or 'achieved'. Table 1 provides examples of principles and outcomes under each of four overarching objectives.

Since May 2018, the OESs and RDSPs have been carrying out self-assessment using guidance provided by their sector's CA. The CAs are working with the OESs to understand the gaps identified through their self-assessments and to determine compliance with the NIS regulations. They have put together action plans and strategies for regulating the sector in the first year.

Table 1: NIS objectives and principles with associated CAF outcomes

Objectives	**Example principles (top-level outcomes)**	**Example CAF outcomes (lower-level outcomes)**
A: Managing security risk Appropriate organisational structures, policies and processes are in place to understand, assess and systematically manage security risks to the network and information systems	A1: Governance The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems. A2: Risk management A3: Asset management A4: Supply chain	A1.a Board direction Effective organisational security management led at board level and articulated clearly in corresponding policies. A1.b Roles and responsibilities A1.c Decision-making

Objectives	Example principles (top-level outcomes)	Example CAF outcomes (lower-level outcomes)
supporting essential services.		
B: Protecting against cyber attack Proportionate security measures are in place to protect essential services and systems from cyber-attack.	B1. Service protection policies and processes The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services. B2. Identity and access control B3. Data security B4. System security B5. Resilient networks and systems B6. Staff awareness and training	B1.a Policy and process development You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service. B1.b Policy and process implementation
C: Detecting cyber security events Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.	C1. Security monitoring The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures C2. Proactive security event discovery	C1.a Monitoring coverage The data sources included in monitoring allow for timely identification of security events which might affect the delivery of essential service. C1.b Securing logs C1.c Generating alerts C1.d Identifying security incidents C1.e Monitoring tools and skills
D: Minimising the impact of cyber security	D1. Response and recovery planning	D1.a Response plan

Objectives	Example principles (top-level outcomes)	Example CAF outcomes (lower-level outcomes)
incidents Capabilities to minimise the impact of a cyber-security incident on the delivery of essential services including the restoration of those services where necessary.	Capabilities to minimise the impact of a cyber-security incident on the delivery of essential services including, the restoration of those services, where necessary. D2. Lessons learned	An up-to-date incident response plan grounded in a thorough risk assessment that takes account of essential service and covers a range of incident scenarios. D1.b Response and recovery capability D1.c testing and exercising

How effective are the NIS regulations?

The NIS regulations were intended to improve the security and resilience of the UK's health, transport, energy, water, digital infrastructure and digital services. However, the Government does not currently have a way of measuring whether this aim has been met or not.

Recommendation:

The government needs to provide a set of Key Performance Indicators (KPIs) to measure and analyse the extent to which the NIS regulatory compliance is improving service resilience within OES/RDSPs.

Roadmap for improvement

Under the current CAF, the Indicators of Good Practice (IGPs) can be used to determine whether an OES has 'achieved' or 'not achieved' each of the 39 outcomes (some outcomes also include a 'partially achieved' category). Initially, OES are required to complete a self-assessment and to develop and submit an improvement roadmap to the CA, which describes how and when any gaps will be closed. However, there is lack of sufficient guidance to translate the CAF results to capability improvements.

The NCSC and CAs are considering how to approach the interpretation of CAF results.[i]One option is to consider a CAF profile, which would mean identifying which of the 39 lower-level outcomes are most important for a particular OES depending on the essential service being supported by the OES and setting targets for compliance against these priority outcomes. This could mean that lower priority outcomes would only be required at 'partially achieved' level or could even be 'not applicable' for that OES.[ii] Some sectors have already developed CAF profiles, for example the DWI has produced one for the water sector.[iii]

A similar approach has worked in the US National Institute of Standards and Technology (NIST) framework, which provides four tiers of implementation based on the risk management practices of an organisation (see box). The organisation defines current as well as target risk profiles that map to the appropriate implementation tier relevant to the organisation's risk requirements.

The US's National Institute of Standards and Technology (NIST) has developed a voluntary cyber security framework to promote a cost-effective approach to reducing cybersecurity-related risk for critical infrastructure. The framework uses a more graduated system of "Framework Implementation Tiers", which describe organisations as "partial", "risk informed", "repeatable" or "adaptive", with respect to the degree of rigour and sophistication in cybersecurity risk management practices. Organisations are encouraged to work towards the tier that meets their requirements considering their "mission, regulatory requirements and risk appetite". Progression to higher tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.[i]

As we argued in section 2.1, above, the Government needs to be able to make an assessment of the security of end-to-end services, not just the individual OES that underpin them. Taking a service-level perspective would allow CAs to understand which organisations supporting the same service were not at the same level of compliance. This would then allow a roadmap to be developed that would bring all of the associated OES up to the standard necessary to ensure the security of that particular service.

Recommendations:

We support the idea of introducing a CAF profile, which is based on an assessment of the criticality of each outcome to maintaining the service. The NCSC should also consider introducing multiple levels into the CAF IGPs. CAs could then use these to determine required compliance levels (if they choose to use the CAF).

CAs should look at end-to-end services to build a picture of all of the OES that contribute towards its overall resilience. The different components should be assessed to understand how critical they are to delivering overall resilience. This knowledge can then be used to develop CAF profiles for individual OES/RDSPs along with a progressive roadmap of improvement for each organisation. There should be a clear understanding of how all of the OES/RDSPs that contribute to a particular service will work towards developing the capabilities to deliver the desired level of cyber security.

Cross-sector security and resilience

Critical National Infrastructure covered by the NIS regulations

- Health
- Transport
- Energy
- Water
- Digital infrastructure
- Digital services

Improving understanding of cross-sector interdependencies

The emergence of dependencies between different critical sectors is a growing concern in cross-sector cyber security. Cyber-attacks can have catastrophic consequences due to the ripple effect of the failure of a single system on other inter-connected systems and services. For

example, a failure in regular electricity supply can cause harm to critical transport or medical services.

The NIS regulations focus on the resilience of individual organisations within a sector and not on end-to-end services which might depend on multiple organisations and sectors. For example, a train service relies not only on the rail network, but also the electricity system and digital communication networks.

Under the UK's 'multiple CA' approach, each CA has responsibility for ensuring that security assessments within their sector are appropriate and proportionate. CAs focus on a single sector, they have an intimate knowledge of the sector and a deep knowledge and understanding of the risks posed to those essential services. They are therefore well placed to determine what is 'appropriate and proportionate' within their sector. However, a downside of this approach occurs where end-to-end *services* depend on more than one OES. If these OES are in different sectors – as in the case of a train service, which depends on transport, energy and digital infrastructure – then each of the contributing organisations will need to be at the same level in terms of their cyber risk management capabilities, if the service as a whole is to be resilient. Under the current multiple-CA approach, different CAs might take a different view on what is considered 'appropriate and proportionate', leading to inconsistencies in the levels of cyber risk management in OES across a particular service. There is currently no mechanism for testing or measuring the resilience of an end-to-end service and cross sector dependencies. The Post-Implementation Review, published in May 2020, highlighted the importance of improving cross-sector interdependencies for supply chains.[i]

More focus is required within the implementation of the NIS regulations on cross-sector dependencies to understand and strengthen cross-sector resilience. The members of cross-sector regulatory collaborative forums such as the UK Regulators Network (UKRN) are facilitators for this, but experts within the regulatory organisations are currently not actively participating in the forum.

Recommendation:

DCMS should develop a plan to explore and measure how end-to-end service resilience and cross-sector dependencies can be better understood, assured, governed and improved. DCMS should then consider how end-to-end service resilience can be incorporated into the NIS regulations in future.

Sharing lessons learnt

The NIS regulations require OES to share details of incidents with impacts above a defined threshold to the appropriate CA within 72 hours of being aware of them. The CA is subsequently expected to conduct post-incident analysis of such incidents.

In addition, NIS principle D2 states that:

"When an incident occurs, steps are taken to understand its root causes and ensure appropriate remediating action is taken to protect against future incidents."

While it is clearly important that OES are able to understand and learn from any incidents that may occur, additional benefit could be gained by ensuring that the lessons learnt are shared more widely within and between sectors. Yet lessons learnt from incidents are not currently incorporated in a formalised manner to improve service resilience upfront in a formalised way.

Recommendations:

The NCSC should develop a 'lessons learnt framework' that could be incorporated into all OES/RDSPs' self- assessments. This would provide a common basis on which CAs could share learnings between sectors. CAs could then share generalised (and therefore anonymised) lessons to the organisations within their sector. This will help to build up a knowledge base that can be used within an organisation, sector and at cross-sector level. Consideration would need to be given to the balance between information sharing, security, confidentiality and resilience.

Assessing compliance

While the NIS regulations have only relatively recently come in to force, early indications from our research suggest that they are not yet driving the kind of step-change in risk management practices that was one of the primary goals of the legislation. We believe that a lack of consistent effective compliance assessments across sectors is a one of the reasons for this.

Consistent and independent assessments for compliance

OES and RDSPs are not necessarily expected to achieve all 39 outcomes set out in the CAF and it is the responsibility of the relevant regulator in each sector to define what represents "appropriate and proportionate cyber security and resilience".[ii] This creates a possibility that there may be inconsistencies in the levels of cyber security that organisations in different sectors are being asked to achieve. Indeed, the sector specific security risk and emergency recovery processes are currently at different stages within different sectors. For example, the financial sector is well advanced, and Ofcom and the NHS have passed pilot phases, while other sectors are less advanced.

In addition, common components across critical services are operated by the same supply chain companies, which amplifies the issue of lack of consistent cyber security framework across sectors.

Challenges might arise where the same regulator is responsible for assessing compliance with cyber security legislation and for meeting other service delivery objectives, resulting in the need to take conflicting demands into account. For example, financial penalties imposed for non-compliance with cyber security could leave a reduced budget available for core services.

Recommendations:

A central audit oversight team should be established to develop a user-friendly tool that defines metrics of good practice and indicators to ensure cyber risk management measures for service resilience are implemented effectively and consistently across sectors.

Effective compliance assessments

The UK has adopted an outcome-based approach to the NIS, which means that the CA audit teams responsible for conducting audits should also take an outcome-based approach to their assessments.

The NCSC has developed the CAF, which CAs can use in their assessments. However, use of the CAF is voluntary and CAs can choose other approaches to assessment if they wish.

Our research uncovered examples of regulators that were not using the CAF (see health sector case study box). The risk is that the assessment exercise becomes a 'tickbox' activity that fails

to drive a deeper cultural change towards cyber risk management within the OES; exactly the situation the outcome-based approach was intended to avoid.

Case study: Health sector

The health sector currently uses a Data Security and Protection Toolkit (DSPT) for regulatory assessments, which is being updated to include NIS elements. To understand the gaps in the health sector against compliance with the NIS, the Department of Health and Social Care (DHSC) has provided an initial mapping of the 14 NIS Principles to the DSPT standards. However, the DPST follows a checklist audit approach that misses out a few qualitative aspects of the outcome-based CAF. What is more, the self-assessment checklist does not cleanly map onto the 14 NIS Principles. This strongly suggests that modifying the DSPT might not be enough to move away from a checklist-mentality. It might therefore fail to meet the NIS objective of outcome-based assessments to improve the cyber security risk management capabilities of the health sector.

Recommendations:

The Government should create a central audit methodology for conducting NIS self-assessment or CA audits (an approach that has worked well in the finance sector). An NIS audit methodology should be built to assess the design and operational effectiveness of key cyber risk management controls. The audit process must be able to check the expected outcomes from the NCSC CAF. A common audit methodology and guidance will ensure that audits assess the quality of cyber risk management controls, are consistent across sectors and meet the purpose of the outcome-based NCSC CAF. This will make the assessment of the NIS regulations consistent between sectors.

Skills and capability for auditing NIS

The shortage of cyber skills is not only a problem for those OES and RDSPs covered by the NIS regulations, it is also a problem for those who are responsible for auditing to assess compliance.

Section 4.2 described how not all of the CNI sectors had opted to use the CAF in their audits. But even if the CAF were adopted by auditors in all sectors, the lack of both technical capacity relating to cyber security and experience of using an outcome-based assessment process in audit teams might result in ineffective cyber risk management judgements. For example, it might be difficult for an auditor to determine how to measure whether an IGP has been achieved. Take the IGPs for outcome A1.b (table 2): under the statement 'key roles are missing, left vacant or fulfilled on an ad-hoc or informal basis', who decides which roles should be considered 'key'? There is no guidance on this and decisions may not be consistent across different auditors.

A further challenge to the delivery of effective audits is the lack of appropriate skills within the regulatory bodies responsible for assessing compliance. Table 3 sets out the CA and auditors for each sector under the NIS regulations in England (Scotland, Wales and Northern Ireland have different CAs in some sectors).

Table 2: Indicators of Good Practice for outcome A1.b (roles and responsibilities)

Not achieved	Achieved
At last one of the following statements is true	All the following statements are true
Key roles are missing, left vacant or fulfilled on an ad-hoc or informal basis. Staff are assigned security responsibilities but without adequate authority or resources to fulfil them. Staff are unsure what their responsibilities are for the security of the essential service.	Necessary roles and responsibilities for the security of networks and information systems supporting your essential service have been identified. These are reviewed periodically to ensure they remain fit for purpose. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.

Table 3: Sectors, CAs and auditors for NIS implementation in England

Sector	Designated CA (England)	Auditors (England)
Health	Secretary of State for Health	• Department of Health and Social Care • Care Quality Commission
Transport	Secretary of State for Transport and the Civil Aviation Authority (acting jointly)	• Civil Aviation Authority • Department for Transport
Energy	Secretary of State for Business, Energy and Industrial Strategy (BEIS)	• BEIS • Ofgem • Health and Safety Executive (HSE)
Water	Secretary of State for Environment, Food and Rural Affairs (Defra)	• Defra • Drinking Water Inspectorate

Sector	Designated CA (England)	Auditors (England)
Digital Infrastructure	Office of Communications (Ofcom)	• Ofcom
Digital Service Providers	Information Commissioner's Office (ICO)	• ICO

None of the auditors have previous experience of auditing cyber security and some auditors – such as the Health and Safety Executive (HSE) and the Drinking Water Inspectorate (DWI) - may be more familiar with checklist and tolerance-based auditing approaches and may therefore not have the experience necessary to deliver an outcome-based audit.

The national shortage in cyber security skills is well documented and we welcome the development of the National Cyber Security Skills Strategy. However, technical security skills are not the only skills needed to carry out effective audits; it also requires professionals who understand programme management, risk management and business/service assurance.

Developing multi-disciplinary teams for NIS audit will potentially address the issue of skills shortage as well as transform the checklist-based audit approach to an outcome-based one.

Recommendations:

DCMS should develop a competency framework for NIS audits. If individual auditors do not have all of the necessary skills (including cyber security, risk management, business assurance and audit skills) then cross-disciplinary teams should be used to conduct the audits. A cross-disciplinary team is more likely to be able to interpret and apply the CAF effectively.

Conclusion

Many aspects of the UK's implementation of the NIS Directive are fit for purpose, in particular the decision to take an outcomes-based approach to compliance, and the development of the CAF collection by the NCSC.

There are several areas where implementation could be improved to deliver the aim of improved security and resilience of NISfor the UK's CNI providers.

Firstly, greater consideration must be given to cross-sector dependencies, where critical services are reliant upon more than one type of critical infrastructure.

Second, improvements to the auditing process need to be made to ensure that the regulations do not merely lead to a box-ticking exercise, but are effective in driving discernible improvements in cyber security practices among regulated organisations.

Finally, a more nuanced assessment of compliance with the regulations would allow the development of realistic roadmaps for improvement for organisations covered by the legislation.

Summary of recommendations

How effective are the NIS regulations?

- The government, needs to provide a set of Key Performance Indicators (KPIs) to measure and analyse the extent to which the NIS regulatory compliance is improving service resilience within OES/RDSPs.
- We support the idea of introducing a CAF profile, which is based on an assessment of the criticality of each outcome to maintaining the service. The NCSC should also consider introducing multiple levels into the CAF IGPs. CAs could then use these to determine required compliance levels (if they choose to use the CAF).
- CAs should look at end-to-end services to build a picture of all of the OES that contribute towards its overall resilience. The different components should be assessed to understand how critical they are to delivering overall resilience. This knowledge can then be used to develop CAF profiles for individual OES/RDSPs along with a progressive roadmap of improvement for each organisation. There should be a clear understanding of how all of the OES/RDSPs that contribute to a particular service will work towards developing the capabilities to deliver the desired level of cyber security.

Ensuring cross-sector resilience

- DCMS should develop a plan to explore and measure how end-to-end service resilience and cross-sector dependencies can be better understood, governed and improved. DCMS should then consider how end-to-end service resilience can be incorporated into the NIS regulations in future.
- The NCSC should develop a 'lessons learnt framework' that could be incorporated into all OES/RDSPs' self- assessments. This would provide a common basis on which CAs could share learnings between sectors. CAs could then share generalised (and therefore anonymised) lessons to the organisations within their sector. This will help to build up a knowledge base that can be used within an organisation, sector and at cross-sector level. Consideration would need to be given to the balance between information sharing, security, confidentiality and resilience.

Assessing compliance

- A central audit oversight team should be established to develop a user-friendly tool that defines metrics of good practice and indicators to ensure cyber risk management measures for service resilience are implemented effectively and consistently across sectors.
- The Government should create a central audit methodology for conducting NIS self-assessment or CA audits (an approach that has worked well in the finance sector). An NIS audit methodology should be built to assess the design and operational effectiveness of key cyber risk management controls. The audit process must be able to check the expected outcomes from the NCSC CAF. A common audit methodology and guidance will ensure that audits assess the quality of cyber risk management controls, are consistent across sectors and meet the purpose of the outcome-based NCSC CAF. This will make the implementation of the NIS regulations consistent between sectors.
- DCMS should develop a competency framework for NIS audits. If individual auditors do not have all of the necessary skills (including cyber security, risk management, business assurance and audit skills) then cross-disciplinary teams should be used to conduct the

audits. A cross-disciplinary team is more likely to be able to interpret and apply the CAF effectively.

Our Research

This briefing was produced in partnership with UCL STEaPP's Policy Impact Unit as part of work carried out by the Jill Dando Institute of Security and Crime Science.

Contact us

Meha Shukla specialises in cyber and physical security risks of smart cities in the Department of Security and Crime Science. Meha can be contacted at Meha.shukla.17@ucl.ac.uk

Professor Shane D. Johnson is the Director of the Dawes Centre for Future Crime at UCL. Shane can be contacted at: Shane.johnson@ucl.ac.uk

Professor Peter Jones specialises in transport and sustainable development at the Department of Civil, Environment and Geomatic Engineering. Peter can be contacted at Peter.jones@ucl.ac.uk

www.ucl.ac.uk/security-crime-science

www.ucl.ac.uk/STEaPP/PIU

---

[i] HM Government, Post-Implementation Review of the Network and Information Systems Regulations 2018, May 2020

[ii] NCSC CAF guidance, accessed 17 November 2019

---

[i] NIST Cybersecurity Framework, accessed 17 November 2019

---

[i] NCSC CAF guidance, accessed 17 November 2019

[ii] NCSC CAF guidance, accessed 17 November 2019

[iii] Drinking Water Inspectorate (2019) 'Guidance on the implementation of the network and information systems (NIS) regulations 2018' , Version 1.1, March 2019

[i] *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*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, (accessed 17 November 2019)

[ii] ENISA (2017) NIS Directive. Retrieved July 11, 2018

[iii] DCMS, "Security of Network and Information Systems Guidance for Competent Authorities", 2018

[iv] *The Network and Information Systems Regulations 2018* (2018/506) Available at: http://www.legislation.gov.uk/uksi/2018/506/made (accessed 17 November 2019

[v] NCSC CAF guidance (accessed 17 November 2019)