Study of cyber security risk management in UK's critical infrastructure sectors (With Smarter London Together Roadmap as case study)

Meha Shukla

Dissertation submitted in partial fulfilment of the requirements for the degree of [MRes in Security and Crime Science (UCL) of the University of London in 2018.

UNIVERSITY COLLEGE LONDON

UCL DEPARTMENT OF SECURITY AND CRIME SCIENCE

University College London
Department of Security and Crime Science

MSc and MRes Dissertations

University College London
Department of Security and Crime Science

MSc and MRes Dissertations

SUPERVISOR'S DECLARATION

Name of student: Meha Shukla

Name of (primary) supervisor: Prof Shane Johnson

I confirm that the student named above has undertaken this dissertation under my supervision, attended meetings with me as requested and provided me with adequate information about the progress of the research.

Supervisor's signature: …

Date: 2/09/2018

University College London
Department of Security and Crime Science

MSc and MRes Dissertations

STUDENT'S DECLARATION

I, Meha Shukla, hereby declare that this dissertation is my own original work and that I have clearly identified and acknowledged all source material used. No part of this dissertation contains material previously submitted to the examiners of this or any other university, or any material previously submitted for any other examination.

This dissertation is 13,000 words in length (including abstract but excluding reference list and reasonable use of tables and figures).

Student's signature:

Date: 31/08/2018

Acknowledgement

I would like to express my gratitude to my primary and secondary supervisors Professor Shane Jonson and Professor Peter Jones for providing the necessary direction, helping with the contacts for the research and supporting me all the way through this dissertation.

I would also like to thank all the 35 stakeholders (Refer Appendix D) for participating in this research, collating the required data for this research, being open about the current issues and validating the final contents of the dissertation. I acknowledge that the ongoing engagement with the Chief Digital officer (CDO) of London provided the much-required encouragement to conclude this research. DCMS was instrumental in providing the facts specific to NIS implementation. I sincerely thank the DCMS stakeholder for the cooperation and support all the way through this research. I would like to express sincere thanks to the key stakeholder from Department of Health and Social care for being forthcoming, investing time in explaining the health sector's cyber security approach, providing prompt information for analysis and valuable feedback on the terms used in the dissertation.

I would like to acknowledge the help provided in locating relevant contacts to Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, Prof Brian Collins, University College London, Barry Emerson and CIO NHSE London Region and Chris Hurran, Principal of the Register of Security Engineers and Specialists (RSES). Dr. Saira Ghafur, Centre for Health Policy, Institute of Global Health Innovation and Martin Guy, Clinical Research Fellow, Imperial College London provided me some insights into the ongoing cyber security issues in the Health sector for which, I would like to thank them as well. I would like to acknowledge that Michael Burton, Durham Chief Constable provided me with a brief background of the cyber security framework within the police forces in the UK, which was helpful for my research. I would also like to thank Mariya Rowland for accommodating my requests at city hall multiple times.

Many thanks to Marco Franken, Product and Service Innovation Consultant, for proofreading my initial versions of the dissertation and providing the required motivation for creating a quality output. It was nice of Alexandra Luck to volunteer and proofread the final version of the dissertation. I would like to express my sincere gratitude to her. Bhairavi Pandya provided voluntary assistance with the title picture in the non-technical short document, for which, I am very thankful. Finally, I would like to acknowledge my husband and my daughters in providing me the necessary moral support in conducting this research.

Abstract

The smart city components such as smart grids, smart transport and smart medical devices connected by physical sensors through Internet-of-Things (IoT) have heightened the threats to national security. The disruption to essential services such as water, transport, electricity and primary health care from a cyber-attack can cause significant damage to the national economy and harm to individuals. This research explored the cyber security risk management across the Critical National Infrastructure (CNI) sectors under Networks and Information Security (NIS) legislation implemented in the UK on 9 May 2018 and its impact on the Smarter London Together plan. In particular, the research examined how the NIS approach will bring a step-change in the cyber-security risk management capabilities of the CNI sectors. While previous work has assessed cyber capability maturity of CNI sectors and the NIS strategy, there has been limited study into the effectiveness of the national framework for cyber risk management. NIS being in its infancy, data was collected through interviews with the regulatory authorities, sampled Operators of Essential Services (OES) and primary organizations impacted by the Smarter London Together planning. Qualitative analysis of the data gathered against the NIS objectives pointed out gaps in the NIS framework specific to the holistic security measures, cross-sector security measures, outcome-based assessments, smart technology risks and NIS performance measures. The gaps highlighted the danger of not meeting the NIS key strategic objective of transforming the cyber security capabilities of CNI sectors in a progressive manner. This research served to be a discovery process for the design of the Smart London Together approach to cyber security. The researcher provided ten key recommendations to improve the effectiveness of the NIS framework. Implementation of these recommendations will strengthen the combined cyber, physical and personnel security of the CNI services prior to extending the NIS principles to non-CNI organizations of the future smart city of London.

Keywords: Cyber security risk management, Network and Information security Directive, Critical National Infrastructure, smart London, Operators of Essential Services, Smarter London Together, Operators of Essential services, NIS

Table of Contents

1. Introduction

The advent of smart cities will increase our dependency on the smart energy grid, smart medical devices, self-driving connected automated transport systems and smart street infrastructure (Cerrudo et al., 2016). The hardware and software used to monitor and control the smart systems, also known as the Operational Technology (OT), connect the physical infrastructure to Information Technology (IT) systems and networks. The cyber-physical attacks, where a hostile actor gains access to an IT system to interact with the OT control environment and disrupt the operations of Critical National Infrastructure(CNI) services, has become a global issue for a nation's economy and secure operations (Baig et al., 2017). The insecure Internet of Things (IoT) that connects multiple mobile physical devices adds to this threat as proven in many countries including Australia (Chapman, 2018). The cyber-physical threats of today are not just from lone cyber hackers and global cyber terrorists, but also from state sponsored attacks as well as insiders (Martin, 2013). Cyber-attacks on CNI such as those directed against the Ukraine power infrastructure in 2016, German rail attack in 2017, Atlanta water supply ransomware in 2018 and 2017 Wanna cry attack, that left many National Health trusts crippled in UK, has resulted in CNI sectors working harder to strengthen their approaches to cyber risk management (James Black, 2018).

The European Union(EU) recognized that cyber-incidents can disrupt the essential services of CNI across borders and the existing capabilities across the EU countries are in-sufficient individually and collectively for NIS security (European Parliament, 2016). The EU, as a result, proposed to improve the European cyber crisis through coordinated activity across member states (European Commission, 2015). Consequently, the EU launched the Networks and Information Security (NIS) Directive on 6 July, 2016 to "improve the EU's preparedness for cyber-attacks"(DCMS, 2018c). The UK is one of six EU nations, the others being Germany, Estonia, Slovakia, Slovenia, Czech Republic (European Commission, 2018) that transposed this legislation into the national law on 9 May, 2018 (UK Legislation, 2018). The NIS legislation plays a key part in delivering the UK's National Cyber Security Strategy 2016-2021 (H.M.Government, 2016) and informs the regulatory framework intended to protect the UK's CNI(DCMS, 2018b).

The objectives of the NIS directive (ENISA, 2017) can be summarized as:

1. To raise the security levels and resilience of NIS of CNI Operators of Essential Services(OES) and Digital Service Providers (DSP) 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 DSP take "appropriate and proportionate security measures" across sectors using a national legal framework and notify the relevant national authorities of serious incidents.

The personnel from EU countries, EU Commission, and the European Union Agency for Network and Information Security (ENISA) have come together to form the Cooperation Group. This group facilitates cooperation and communication within EU member states. It also intends to assess the implementation of the NIS regulation in EU member states, every one and a half years (ENISA, 2017).

1.1 The focus of this research

This research explores the question: "How are cyber security risks currently managed under the NIS Directive across UK's CNI sectors?" The research is exploratory and aims to study:

1. What are the current gaps in the cyber security risk management framework under NIS legislation?
2. Is the NIS directive's approach, aimed at bringing step change in the cyber security risk management across UK's CNI sectors, effective?
3. How do points in a) and b) fit into the Smart London cyber security planning.

As per the European Commission report, NIS is the first legislation within EU member states to regulate cyber risk management within CNI sectors (EECSP, 2017). The NIS legislation is in its infancy, appropriate and proportionate security measures are expected to be assessed, planned and matured by OES and DSP in the first year (DCMS, 2018b). As such, a timely question – which is the focus of this research – is how effective is the NIS approach? The research will assess the current implementation approach of the NIS framework across the CNI sectors to achieve its primary objectives mentioned in points 1 and 2 above. In absence of any prior research and data availability across organizations, this research will focus on collecting data through interviews of professionals within the OES and regulatory bodies. As a first case study, a sampled CNI sector's current cyber security framework will be compared with the self-assessment framework under NIS legislation. This will help analyze the gap between the existing and expected risk management capabilities and the roadmap to achieve the same.

To assess how NIS regulation can be applied to a smart city, the second case study will focus on the cyber security challenges for the Smarter London Together Roadmap published in June 2018(GLA,

2018). The Smarter London Together Roadmap has five focus areas:–

1. Secure world class connectivity;
2. City wide collaboration;
3. Enhancement of digital skills;
4. Data sharing; and
5. Digital inclusion.

The secondary objective of this research is to draw on the lessons learned from an analysis of NIS implementation to help the Smart London team to design customized practices aligned to the NIS legislation for London's cyber security strategy.

As per the National Risk register, the UK currently faces serious potential cyber-physical threats within the drinking water supply, health sector support systems, transport and energy control systems(Cabinet Office, 2017). The analysis of the data gathered from across professionals working currently in the NIS sectors will provide information on the challenges and gaps in cyber security risk management of the CNI. The standards and best practices of the NIS framework will also provide inputs to the cyber security framework of the sectors that are not covered by the NIS and in-turn, benefit the UK industry.

The dissertation is structured as follows:

Section 2 reviews the literature on cyber security risk management for CNI and the NIS legislation
Section 3 describes the research methodology, sampling and approach to data collection and data analysis.
Section 4 provides an analysis of the data gathered to describe the current state of the NIS regulatory framework
Section 5 analyses data for the case studies for this research
Section 6 covers the discussion of strengths, gaps and recommendations
Section 7 concludes with limitations of this research, further research suggestions and key messages.

2. Context and Literature review

UK Government has previously conducted an international review of methods tested to incentivize businesses to manage their cyber risk effectively, but concluded that there is very little impact of these methods(DCMS, 2016). The global cyber security breaches so far also make it clear that over and above the technology, an effective approach to deal with cyber security threats is to manage risk-based security of people and processes as is the case in a business transformation model (Microsoft, 2018). Cyber security risk management involves understanding the critical business processes supporting the critical services and the underlying components, systems, networks, physical assets and personnel(Quigley & Roy, 2012).

The study of cyber security strategies of EU and NATO countries has revealed that the service resilience, meaning quick recovery from a security incident, is the main goal of the EU and NATO cyber security strategies which is achieved through public-private partnerships (Štitilis, Pakutinskas, & Malinauskait\.e, 2017). The cooperation and collaboration across public-private sectors is the common thread in cyber security strategies in multiple countries such as Brazil (Trinkunas and Wallace 2015), Australia (Smith & Ingram, 2017), Israel (Štitilis et al., 2017), USA (NIST, 2018) and China (Maglaras, Drivas, Noou, & Rallis, 2018). However, these strategies differ in the legislative and implementation approaches. The Australian cyber security strategy has a state level ownership but focuses on voluntary governance and self-regulation (Smith & Ingram, 2017). Israel has a hybrid model between "liberalism and statism (Smith & Ingram, 2017). The Chinese Cyber security Law (CSLaw) implemented in Nov 2016 has similarities with NIS directive, for example the requirement to report important incidents (Maglaras et al., 2018), however, to make China safer, it is also oriented towards Chinese sovereignty. The Cybersecurity Act in the USA mandates the National Institute of Standards and Technology(NIST) framework (NIST, 2018) to manage cyber risks. However, the approach is voluntary and decentralized, shifting liability away from commercial companies in order to encourage information sharing, rather than the state-governed approach of the NIS directive in the EU (Department of Homeland Security, 2015). Enough research is not available to analyze the cyber security legislations across the world to understand "what works".

Research, in the past four years, has studied the design of the NIS legislation. The assessment of cyber security in UK raised an issue that the NIS legislation is seen as a compliance problem rather than an opportunity to improve cyber security (Walker-Osborn & Patel, 2014). The cyber capability maturity of sampled UK sectors to support National Cyber Security Strategy was analyzed in 2016 and organizations were found to have varying levels of capability maturity (Bada et al., 2016). The

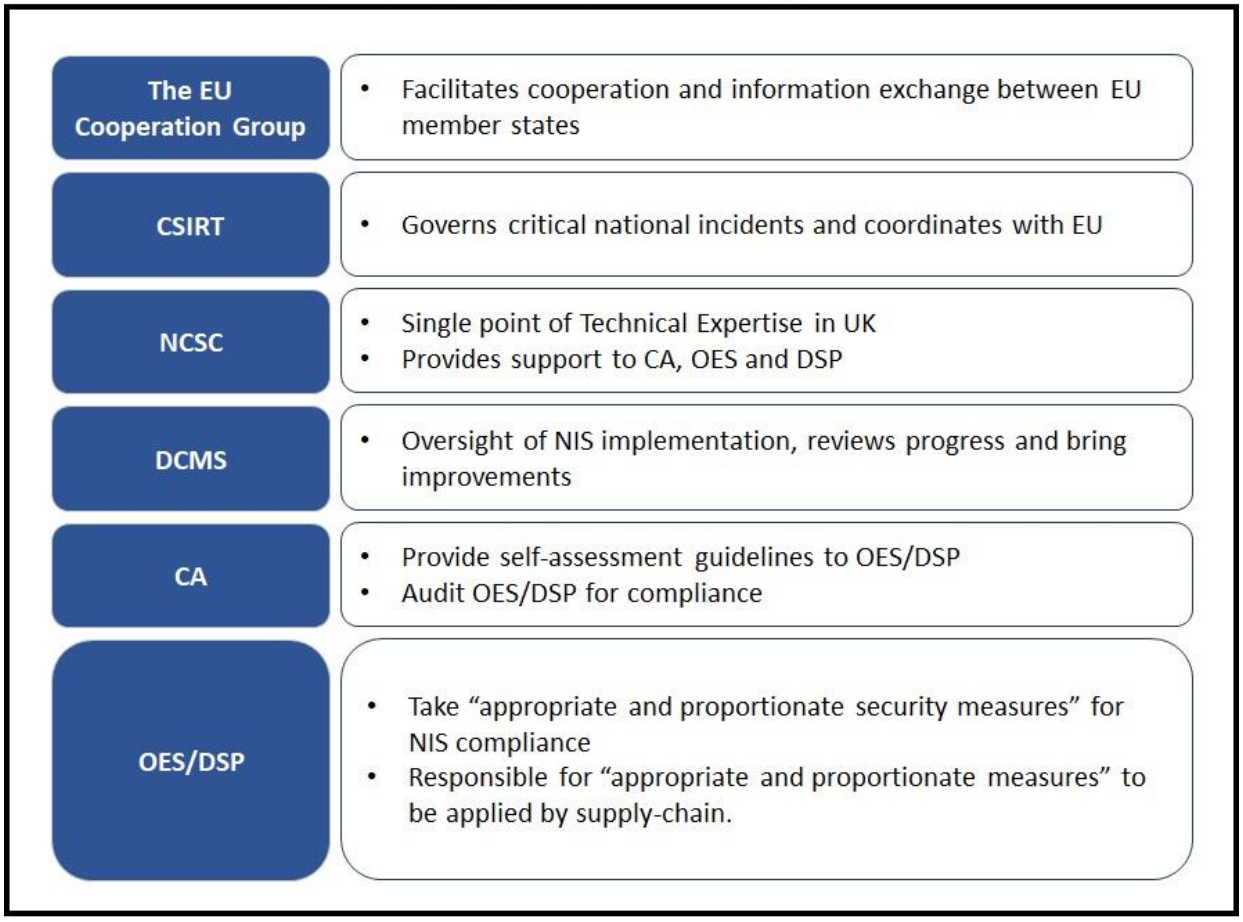
cross-organizational incident management model for NIS directive was found, based on the findings of a case study, to be very effective (Rao, Carreon, Lysecky, & Rozenblit, 2018). The study of security concerns in the energy sector, using a case study of the smart energy supply chain, highlighted challenges for NIS compliance such as optimal management of legacy systems, reporting incidents within the expected timeframe and insufficient resilience of the IoT products (Urquhart & McAuley, 2018). The need to focus on the interdependence of critical services within the NIS legislation has been identified in the analysis of how to protect CNI (VIIRA, 2018).

Although there has been research into elements of NIS framework design prior to its implementation, there has been no research on the actual effectiveness of the NIS framework since the implementation of NIS directive in May 2018. As NIS is the first piece of legislation in this area, there is no benchmark available to assess whether the NIS regime will be effective in managing the cyber security challenges within EU. Due to the limited availability of academic literature on cyber security risk management practices of CNI and NIS regulation, this research makes references to the available documents from Government or other organizational websites.

NIS Governance: As per the NIS strategy, in the UK, the Minister of the Crown publishes priorities and goals for the security of the networks and information systems (UK Legislation, 2018). The structure of NIS governance bodies in this section has been explained by the Digital Culture, Media and Support (DCMS) report (DCMS, 2018b). The DCMS is one of the lead UK government departments on cyber security policy that provides the oversight of NIS implementation, reviews progress and brings improvements. The NIS directive is implemented by the OES and DSP from six economic sectors. Each of the sectors under NIS has a lead Department termed as Competent Authority (CA) that identifies which infrastructure qualifies as a CNI asset in their sector and who are the OES. The CAs assess and enforce compliance of OES and DSP cyber risk management in each sector based on the business context and the needs of their sector or region, as per the DCMS report. Under NIS legislation, the Computer Security Incident Response Team (CSIRT) governs critical the incidents in the UK ("Introduction to the NIS Directive," 2018). The DCMS is the UK representative at the EU NIS Cooperation Group (DCMS, 2018b) and within UK, provides the oversight of NIS implementation, reviews progress and recommends improvements (DCMS, 2018b). The National Cyber security Centre (NCSC) is a part of the Government Communications Headquarters (GCHQ), which aims to protect critical services ("Welcome to GCHQ," 2017) and is the single point of technical expertise under NIS legislation. The Centre for Protection of National Infrastructure (CPNI), is the national technical authority for physical security and personnel/people security ("Critical National Infrastructure | CPNI | Public Website," 2018) and coordinates with NCSC for

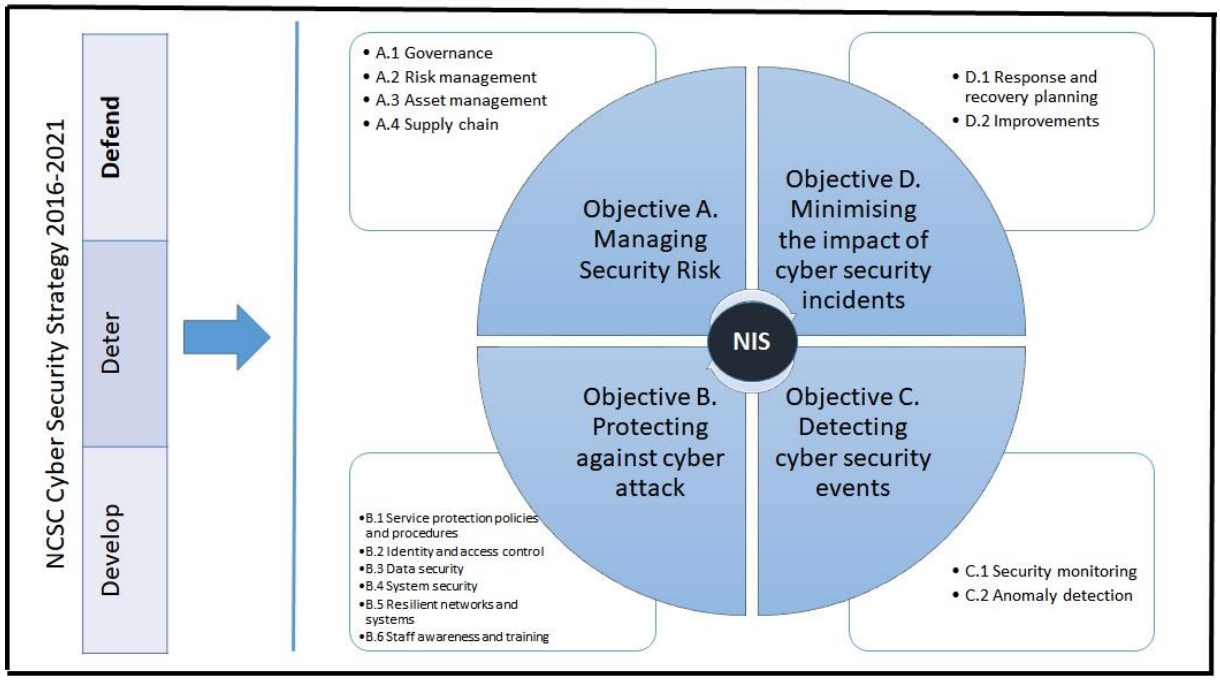
cross-cutting security, but is not covered by the NIS legislation. The organizations in the NIS framework are summarized in Figure 1 below:

Figure 1: Key Organizations in NIS Legislation



Cyber security risk management: The implementation of cyber risk management of CNI across the OES and the DSP is described through the four NIS objectives mapped to the three NCSC cyber security strategy goals-Defend, Deter and Develop (H.M.Government, 2016). The NCSC, has collaborated with the Government and the CAs to develop an initial generic version of a Capability Assessment Framework (CAF) that maps the four key objectives to each of the 14 principles for NIS compliance assessment ("Table view of principles and related guidance," 2018a). (See Figure 2 below). Against each NIS principle, the CAF lists the standards followed and a set of Indicators of Good Practice (IGPs).

Figure 2: NIS Objectives and Principles



Cyber security Incident Management: Under NIS regulation in the UK, it is mandatory for the OES/DSP to report any major service disruption to the CA within 72 hours of becoming aware of the incident (DCMS, 2018d). DCMS report also states that if a cyber and/or physical incident has an impact on the European service, the CSIRT needs to inform the Cooperation group within EU. DCMS has recommended, in the report, that the CAs should establish some form of triage system to classify incidents in terms of importance and make decisions on their investigation. The UK Government proposes to issue penalties similar to General Data Protection Regulation (GDPR) for the NIS compliance breaches ("Regulating Cyber: the UK's plans for the NIS Directive," 2017).

NIS Implementation in EU: The implementation of the NIS regulation follows different approaches in the countries within the EU. Germany follows a single CA approach compared to the multiple CA approach followed by the UK ("Implementation of the NIS Directive in Germany | Digital Single Market," 2018). During a discussion to understand NIS implementation in EU, a stakeholder from Germany's Federal Office for Information Security mentioned that in Germany the OES define the standards also known as B3S ("state of art"), that each sector intends to follow for cyber risk management and NIS compliance. UK, on the other hand, prescribes CAF IGP for NIS compliance to ensure that the regulatory assessments do not become a tick-box exercise and instead work as a means of achieving improved cyber risk management practices. There is lack of clarity as to how NIS legislation will be impacted by Brexit (DCMS, 2017).

3. Methodology

3.1 Sampling

A sampling approach was used to identify key areas for the research. As the study included Smart London, the sampling frame consisted of key organizations impacted upon by the NIS legislation in England from the DCMS report (DCMS, 2018c). These were the NCSC, the DCMS and the CA for each sector in England (see Appendix-F for a list). The rail transport, the road transport and the health sectors were selected for detailed discussions with the CA and the OES. The rationale for their selection was that they covered sectors that are important to the Smarter London Together Roadmap. Within the transport sector, the OES selected in the sample included key rail and road operators - Network Rail, Highways England and Transport for London (TfL). Within the health sector, two leading NHS trusts in London represented the OES sample. The finance and banking sector regulators were included in the sample to understand the available tools and practices from these sectors exempt from NIS (DCMS, 2017).

As mentioned in Section 1.1, two case studies were included in this research to assess the cyber security risk management capabilities in the organizations. The first case study compared the current cyber security framework against the NIS regulatory framework. The health sector was selected for this case study because the stakeholders within this sector volunteered to provide detailed information to support the analysis. The second case study was to understand the cyber security needs of the Smarter London Together Roadmap. The Chief Digital officer (CDO), in charge of the Smarter London Together Roadmap was selected as a key stakeholder for this research. London's CDO readily engaged, and provided contacts within government and public sector organizations. The stakeholders from these contacts who agreed to participate in the research came from the London Resilience Group, NHS England, London Fire Brigade and Metropolitan Police Service. To get a view of the smart city standards for the second case study, the British Standards Institute was included in the sampled organizations.

This approach led to the 35 stakeholders from 30 organisations identified as samples for the research (refer to Appendix D for the full list).

Numerous approaches were taken to identify the stakeholders responsible for the CNI cyber risk management in UK. These were:

- A small pool of stakeholders identified by contacting the identified organizations directly using the email provided on their website;
- The EU website ("Implementation of the NIS Directive in the UK | Digital Single Market,"

2018) and the NCSC website ("The NIS Guidance Collection," 2018) were reviewed for available contacts within various organizations involved in the implementation of the NIS legislation;

- Authors of academic articles identified during the literature review, professors from University College of London (UCL) working in relevant domains, and the author's professional contacts were contacted to help identify stakeholders; and
- Snow-ball sampling approach was followed to identify further stakeholders for interview.

3.2 Data Collection and Analysis

The researcher collected data between 1 March 2018 and 30 June 2018. The data gathering involved the completion of semi-structured interviews, Freedom of Information (FOI) requests and a review of information available online. The interviews were conducted with the identified stakeholders who participated voluntarily. Initial questions were general in nature to understand the role of the stakeholder and to help customize subsequent questions to the stakeholder's role. Questions then focused on the process of cyber risk management, implementation of the NIS legislation, NIS enforcement and the resolution of key cyber security risks. Stakeholders were also asked for their opinion of the key challenges and issues faced by the sector for cyber security of their CNI. The questions mapped to the objectives of the research, but were open ended to ensure that the interview did not restrict the information stakeholders could provide (see Appendices A, B and C). If the stakeholders were not available for an interview, specific questions were sent by email to the stakeholder address provided on the organization's website, under FOI, to collect data against specific questions per sector.

Secondary data was collected using reports, standards, guidelines and information published online on ENISA, UK Government, NCSC, CPNI and Greater London Authority (GLA) websites. UK websites were searched using the keywords:

- "NIS guidelines"
- "Network and Information Security directive"
- "cyber security risk management"
- "resilience for CNI"
- "NIS enforcement"
- "cyber security regulations"
- "national risk"
- "emergency response and recovery"

- "London cyber security strategy"
- "Smart London Plan"

Data was also collected from the Select committee reports for CNI cyber risk management(Parliament Select Committee-June, 2018).

The information gathering depended on the willingness of stakeholders to engage with this research and share relevant data. Anonymity, wherever requested, was maintained in the research outputs. The quotes from stakeholders are included only where the stakeholder granted permission. The gathered data illustrated the various activities and practices associated with the enforcement of the NIS directive, which were compared to analyze common themes across sectors using a qualitative approach. As a part of the first case study, the comparative assessment of the current framework with the NCSC CAF requirements provided the current gaps within the NIS framework, thus meeting the first objective of the research. The current risk management activities and gaps in the NIS sectors were compared with NIS objectives and a few best practices in Finance sector. This provided the effectiveness of the framework, thus meeting the second objective of the research. Key challenges for Smart London cyber security were assimilated through interviews for the second case study. The requirements for cyber security of Smart London were compared against the NIS framework to provide recommendations for the management of Smart London cyber risks, thus meeting the final objective of the research. The inputs provided by each stakeholder in this dissertation were sent for validation and the feedback was incorporated prior to the dissertation's submission.

4. Results - Cyber risk management under NIS Framework in UK

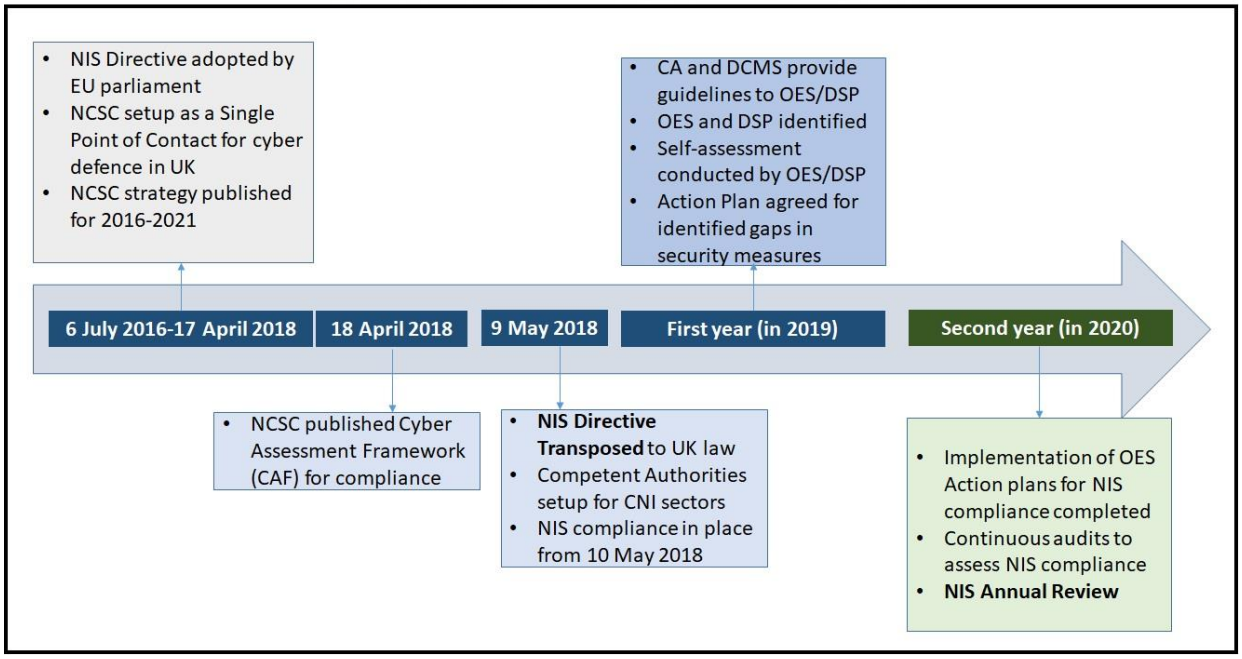
An assessment of the status of the NIS framework and its current implementation in the UK in this section was derived from interviews with the DCMS stakeholder (hereafter DCMS-S1) and the CPNI stakeholder (hereafter CPNI-S1). As explained by the DCMS-S1, under NIS legislation, the OES/DSP need to take appropriate and proportionate risk management measures for security risk management, the security of the network and information systems on which their essential service relies. It is the responsibility of CA to review the application of the NIS regulation within their respective sectors. Information published by NCSC (including the CAF) is intended to support the CAs in their role. The DCMS has published guidance for CA to implement the NIS risk management framework. It includes direction on how to create sector-specific guidance for OES/DSP (DCMS, 2018d) and the criteria to identify the OES in their sectors (DCMS, 2018c). DCMS-S1 explained that the list of OES per sector is expected to change dynamically based on the changing service criticalities and ownership for its operations. The OES also needs to identify and share the list of systems (operated by them and their supply chain) which could cause disruption to an essential service, when compromised.

DCMS-S1 was of the opinion that the implementation of the NIS is following a collaborative approach. Prior to the implementation of the NIS legislation, a collaborative assessment of how the NIS directive impacts the OES was conducted by the DCMS with the UK industry representatives in 2017 (DCMS, 2018a). DCMS-S1 confirmed that some CAs are not experienced and some were reluctant to accept regulatory responsibilities in this area. So even after NIS implementation, the efforts are on-going to ensure the buy-in of the CA, the OES and the DSPs for improvement of the cyber risk management practices. In order to coordinate, support, and to help develop methods to assess compliance with the NIS, the DCMS has been chairing a regular meeting of the CAs, OES, DSP and suppliers. This provides a forum to discuss issues and share best practices.

DCMS-S1 also stressed that the NIS needs to be enforced using an outcome-focused approach provided by the CAF to achieve a stepped change in good risk management practices. The CAs can use the CAF or an equivalent framework to assess OES in their sector. It is ultimately for the CA to determine what IGP from the CAF constitutes appropriate and proportionate measures for OES in their sector.

DCMS-S1 provided insight into the NIS implementation journey, which is illustrated in Figure 3. In the first year of NIS implementation, the CAs of each sector under NIS are in the process of understanding the requirements and the CAF compliance measures that define appropriate and proportionate security for their sector. OES/DSPs are participating in a pilot with the CA to assess themselves against the CAF and report the gaps. Cyber security experts and sector subject-matter experts within the CA will review the gaps to make a judgement on the acceptable levels of cyber security based on the possible impact and business context. An action plan to address any identified gaps from self-assessment will be created. The CAs will expect some OESs not to be fully compliant yet as the CAF was only published in April 2018 (DCMS, 2018b). DCMS-S1 expects that in a year's time, there should be a clear understanding of how different sectors manage cyber security under the NIS legislation. DCMS-S1 expressed an opinion that all OES/DSP are taking adequate measures, and therefore comply with NIS, hence, it is unlikely that any OES/DSP will incur any penalty for NIS non-compliance in the near future.

Figure 3: Business Transformation for UK CNI under NIS Legislation



CPNI-S1 added that, the CAF may not be a complete list, and currently, it does not include the non-cyber elements required for the cyber risk management. DCMS-S1 confirmed that the NIS framework performance measurement KPIs are yet to be defined. The intention is to develop the CAF based on the industry feedback and further research by the NCSC. In response to queries, CPNI-S1 and DCMS-S1 confirmed that for NIS, there is an on-going discussion on the governance for non-cyber elements to be included in the CAF. There is also lack of clarity as to how NIS standards are aligned with National Information Infrastructure (NII) standards. DCMS-S1 confirmed, the cyber infrastructure such as the data centres, servers, and transmission lines are a known gap for

ownership between CPNI and NCSC. It was not clear whether there is any impact assessment or mitigation for this gap.

The sector regulators engage in dry runs for emergency response and recovery termed as resilience tests for the sector's services. The CAs are also encouraged to work with other regulators outside of the NIS regulations, to manage cumulative requirements across multiple legislations. The EU Cooperation group, the DCMS, the CAs, the NCSC and the UK Regulators Network (UKRN) work collaboratively across sectors and borders to share best practices and to drive up maturity and capability. However, resilience tests for end-to-end service that spans across sectors is a current gap (UKRN, 2015). The gaps discussed in this section are summarized in Table1 below.

Table 1 Summary of the NIS implementation gaps – DCMS and CPNI inputs

Category	Description
CAF and IGP	Known Gaps: • The cyber, physical and personnel security are an integral part of holistic security. NCSC CAF currently does not include non-cyber elements • The CAF does not include cross-sector resilience
NIS Governance	• CAs take the decisions for appropriate and proportionate security assessment provided by OES/DSP. There is no governance to ensure that these decisions made by CAs are consistent across sectors especially for cross-sector services.

4.1 Finance and Banking Sector

This section summarizes the inputs provided by the stakeholders mentioned in Table a.

Table a – Stakeholders for Finance Sector

Organization	No of Stakeholders	Stakeholder Reference	Data Collection method
Financial Conduct Authority (FCA)	1	FCA-S1	Interview
Payment System Regulator (PSR)	1	PSR-S1	Interview
Bank of England(BoE)	1	BoE	FOI request

As discussed with FCA-S1, the Finance sector, historically, is heavily regulated at a local and global scale. As a result, it has already made considerable efforts to mature and evaluate the cyber security framework for continuous learning. FCA-S1 emphasized that "Finance and Banking sector's business model focuses on IT resilience" and "the finance sector is already working towards international standardization through a G7 cyber expert group." (BoE, 2016). FCA-S1 and BoE confirmed that the CBEST framework implemented by the finance sector (BoE, 2016), an intelligence-led ethical hacking tool, is widely considered to be a world-leading framework ("Oral evidence - Cyber Security: Critical National Infrastructure," 2018).

PSR-S1 focused on supply chain issues, "Although the payment industry is regulated for key actors such as Visa and Master card, the supply chain such as merchants are unregulated". PSR-S1pointed out that the Bankers' Automated Clearing Services (BACS) payment system had recently undertaken an enhanced cyber security program. BACS has a three-day clearing and settlement process, which provides greater opportunity to spot fraud and to reverse such payments, compared to payments that clear immediately. PSR-S1 emphasized, "The Treasury and authorities consider operational resilience a serious policy issue. Every bank has fraud prevention and detection monitoring systems in place. Similar systems need to be developed within other industries where they do not currently exist". Under the NIS directive, the challenge is that it is the OES and DSPs who are liable for appropriate and proportionate measures to manage the risk of their service disruption via their supply chain (DCMS, 2018b). FCA-S1 mentioned, "Currently, there is no stable, scalable framework for supply chain cyber security". FCA-S1 also added that for supply chain, frameworks such as "Know your third party" (KY3P) seek to develop a one-to-many federated type of model for supply chain assurance.

FCA-S1 also pointed out that "the Finance sector has three regulators, the FCA, Bank of England

(BoE) and HM Treasury (HMT) requiring a coherent joined up effort for regulating the sector. The Authorities' Response Framework (ARF) covers the coordinated response required by any incident that results in major disruption to the financial sector." Sectors with multiple CA can possibly follow this approach.

4.2 Transport Sector

This section summarizes the inputs provided by the stakeholders mentioned in Table b.

Table b – Stakeholders for Transport Sector

Organization	No of Stakeholders	Stakeholder Reference	Data Collection method
DCMS	1	DCMS-S1	Interviews
DfT	2	DFT-S1, DFT-S2	Interview for DFST2, Email for DFST1
ORR	3	ORR-S1, ORR-S2, ORR-S3	Interviews
TfL	1	TfL-S1	Interviews
CPNI	1	CPNI-S1	Interviews
Highways England	1	Highways England	FOI request
Network Rail	1	Network Rail	FOI request

Competent Authorities

The DfT-S1 explained that in England, on behalf of the Secretary of State for Transport, the Cyber Compliance Team (CCT) in the DfT carry out the roles and responsibilities of the CA for rail, maritime and road sub-sectors. For the aviation sub-sector, "the DfT and the CAA share the roles and responsibilities of the CA" (Refer Appendix F). As pointed out by DCMS-S1, it is important to note that the CAA is an experienced regulator whereas the DfT does not have any regulatory experience. Currently, the DfT and CAA are collaborating with DCMS, other regulators across sectors, industry partners and the supply chain to implement security measures in the transport network in proportion to the threat posed.

DFT-S1 mentioned that the criteria for OES and sector-specific thresholds for the incident reporting have been published in the initial sector-specific guidelines (DfT, 2018). DfT-S2 confirmed that DfT will engage in the post-incident analysis, however, the defect triaging process for the incident root-cause analysis to build a lessons learnt framework has not been published yet. The process to assess compliance using the NCSC published NIS CAF is currently a work-in-progress. DCMS-S1 confirmed that by December 2018, the pilots of their self-assessment tools with the OES are expected to be completed. The OES will provide the reports from self-assessments with red, amber and green

compliance gaps to the CAs. The DfT and the CAA will assess the impact and if the gap is found to be relevant, an action plan will be provided by the OES. DfT will review the on-going self-assessment on a pre-determined frequency. DfT, if it deems it necessary, will conduct audits after the action plans are agreed. As confirmed by DCMS-S1, the transport sector also plans to pilot sector-specific tests for recovery from severe disruption specific to cyber-attacks on IT and infrastructure. DfT-S2 and CAA-S1 raised a framework for cyber security of the supply chain as a common issue across sectors. To understand the details of the impacts of the NIS regulation on three subsectors within the transport sector with different operating models, further analysis was conducted.

1. **Rail Sub-Sector:** The information in this section was assimilated from the interviews conducted with the ORR stakeholders – ORR-S1, ORR-S2 and ORR-S3. The ORR is an independent economic and safety regulator for Britain's railways. It has a pivotal role in securing sustained improvement in the health, safety and performance of the rail industry. The European Train Control System (ETCS), the signaling and control component of the European Rail Traffic Management System (ERTMS) plans to replace the safety systems currently used by the European railways, making the cyber-physical systems vulnerable to security threats. ORR-S1 stated, "The threat increases with the upcoming infrastructure specific to automated signaling and elements of digitization in cross rail and High speed2 railway in London". However, NCSC CAF includes only cyber threats. ORR-S1 stated, "There are significant overlaps between the NIS regulatory requirements and the current rail safety and security regulations". Therefore, some amount of NIS compliance is expected to be in place in areas such as governance, risk assessment, asset management, supply chain, staff awareness and training, response and recovery planning and improvement. However, existing rail security regulation is designed to protect the rail network from acts of violence and does not include cyber-physical resilience hazards and stringent incident reporting.

   The rail cyber security strategy was published in Jan 2017 (DfT, 2016) to explain how railway stakeholders will work together to protect our cyberspace and provide inputs for policy makers. ORR-S1 further explained that ORR uses a Risk management maturity model RM^3 to determine capability maturity levels within the rail sector using a PDCA (Plan, Do, Check, Act) approach and evaluates twenty six criteria to assess safety management systems. ORR-S2 confirmed that, the ORR safety inspectors currently do not inspect cyber security aspects, which can be paramount to the safety of the cyber-physical infrastructure, as they are not a part of RM^3 model. However, there is awareness that cyber risks will need to be better managed under NIS legislation. As mentioned by the CPNI-S1, a cyber-security awareness program was conducted for safety engineers in the transport sector. The feedback was positive but there is a need to

follow-up and help the operators implement the solutions.

The issue of legacy Industrial Control Systems (ICS) not being patched due to fear of losing functionality was highlighted by ORR-S3. CPNI-S1 also confirmed that some Virtual Memory Systems (VMS), not designed for security, but which, run critical processes for the CNI, have not been patched since 1986 because there is limited understanding of how they operate and that this might have already made the systems insecure.

2. **Maritime Sub-Sector:** The information in this section was provided by DFT-S2. The Cyber Security codes of practice for Ports and Port Systems were published in in August 2016 and in September 2017 for Ships (DfT, 2018). As explained by DFT-S2, the NIS principles go further than the Codes of practice and hence a self-assessment for NIS compliance is currently under-way. The researcher observed that the DfT has not published guidelines for cyber-physical systems, such as the upcoming sophisticated and autonomous cargo ships within their NIS guidelines.

3. **Road Sub-Sector:** The information in this section was provided by DFT-S1, DFT-S2 and the FOI response from Highways England. The road sub-sector's cyber risks are mainly driven by future Connected Automated Vehicles (CAV). DFT-S1 provided the regulatory guidelines for the manufacturing of CAV by the DfT (The Key Principles of Cyber Security for CAV, 2017). As confirmed by DfT-S2 and Highways England, unlike aviation, maritime and rail, "there are no existing regulations for cyber security or requirements that cross over with the NIS regulations. As a result, the current guidance from DfT to the road service operators is to work within their existing licensing agreements for NIS compliance".

4. **Air Transport sub-sector:** CAA-S1 explained in the interview that the Civil Aviation Publication, CAP 1574 framework was published in Dec 2017. The controls in this framework are used as a guideline by the industry to manage the cyber security risks and achieve safety. The framework is also used to support the CAA's regulatory cyber oversight as well as resilience to cyber-attacks. The CAA has assessed the CAP 1574 controls against the NIS principles and concluded that the controls that are already operational appropriately supported the delivery of NIS (CAA, 2017). However, CAA-S1 confirmed that self-assessment is under way to comply with the legally binding aspects of NIS legislation and European safety regulation.

Operators of Essential Services

To understand the views of the OES within the transport sector, the researcher contacted Network Rail and TfL.

1. **Network Rail**: Network Rail stakeholders provided their inputs in an email against an FOI request. The email stated, "Network Rail's assessment for compliance with the NIS requirements is currently under review based on the guidance from the DfT. Network Rail has developed and published its own guidance for the security framework for managing cyber risks against a number of regulations and industry standards including ISO27001 and IEC62443. The management of third party risks is a part of the framework process". In response to the query whether the third party product approval process for safety critical systems includes cyber security checks , the email mentioned, "the industry is aware that there could be overlaps between regulations and standards in security including the NIS Directive and is considering the mapping these regulations and standards to the rail operators".

2. **Transport for London (TfL):** TfL-S1 provided detailed information across multiple interviews, which are summarized here. TfL's overall responsibility includes operation of London's public transport network, including London Underground trains, London Buses, Docklands Light Railway, London Overground trains, London Trams, London River Services, London Dial-a-Ride taxis, Victoria Coach Station, Santander Cycles, the Emirates Air Line, the management of the city's main roads as well as the traffic lights in London. It also has the largest contactless payment system ticketing system in the UK and 550 kms of strategic road network and CCTV systems (pervasive and old) where data is transferred using 4G.

   TfL-S1 explained that TfL follows structured processes for cyber risk management and governance. TfL studies the risks identified in the National risk register and manages cyber risks at multiple levels: 1) Corporate risk register for overall risks; 2) Directorate-specific risk register for strategic risks within the directorate; and 3) Specific cyber security risks for system/component level vulnerabilities. TfL publishes the high-level risks including cyber risks, which are discussed at the Board of Directors quarterly. TfL-S1 stressed, "the target hardening of protected bespoke systems is a part of its cyber security development process". TfL-S1's perception was that currently there are IT cyber risks but not many infrastructure cyber risks in the TfL risk registers due to the current low exposure to cyber-physical threats. Due to limited legacy systems and ongoing refurbishments of the infrastructure within TfL, there are comparatively fewer issues for cyber risk specific to the legacy systems. However, within TfL multiple safety critical OT are moving to the digital arena (e.g. digitization of signaling), which will change the cyber risk landscape. Self-driving vehicles technology is already driving the risks of the cyber-physical systems. TFL also has a Director of Innovation who looks at the technologies that are downstream and the resultant risks.

Managing a list of regulatory demands is challenging, however, as confirmed by DCMS-S1, DFT-S2 and TFL-S1, the work is progressing to embed the required processes for compliance to NIS. TfL is currently conducting a self-assessment to understand and create an audit trail for NIS regulatory compliance. The GDPR has a crossover with the NIS and it is a challenge to prepare a checklist for mapping multiple regulatory requirements. TFL-S1 also confirmed that there is an awareness in TfL about managing overlaps between safety and security on cyber and physical fronts. The supply chain guidance needs to be applied to the organization's outcome-based approach to NIS compliance. The key points from the above analysis are summarized in Table2 below.

Table 2 Summary of the NIS implementation within the Transport subsectors in England

NIS Implementation	Transport Sector			
	Rail Transport Sub-sector	Road Transport Sub-sector	Maritime Transport sub-sector	Air Transport sub-sector
CA	DfT, no regulatory experience	DfT, no regulatory experience	DfT, no regulatory experience	CAA has regulatory experience
Guidelines	OES identification and incident thresholds included in the guidelines, defect triaging guidelines are a work-in-progress (published by DfT)			
Existing frameworks prior to NIS	RM[3] capability maturity and rail safety regulations	No prior framework	Existing Codes of Practice for Ports and Port Systems	Existing 26 controls in CAP 1574 framework
Regulatory overlaps	Rail safety regulatory overlaps with cyber security	No prior framework	Overlaps with safety and cyber security	Cyber security controls overlap with European safety regulations
NIS Assessment framework	NCSC CAF	NCSC CAF	NCSC CAF	CAP 1574
Key Transport technology threats	Digitization in rail and signaling (e.g. ETCS, ERTMS)	CAV	Digitization in ports and ships including automated ships	Not discussed
Researcher's analysis	The implementation of the NIS legislation within the transport sector is heavily dependent on a collaborative approach between the DfT, CAA and OES. The sub-sectors are at varying degrees of maturity. Air Transport has the cyber security controls in place whereas road sector is still in formative stage. Current gaps: 1) Although organization in transport sector are at varying degrees of cyber security risk management maturity, all organizations are expected to demonstrate NIS compliance. There is no support for stepped maturity based on criticality of the components within the sector. 2) Holistic security threats need to be assessed in context of potential cyber-physical attacks. 3) NCSC CAF and CA guidelines for NIS do not include IoT, smart transport solutions such as CAV, automated ships and digitization in the rail sector. Hence, the audit framework will currently not assess the risks from these technology threats.			

	4) There is an overlap with safety and security on cyber and physical fronts, which is a known gap. However, there is no mapping done to assess these regulatory and audit overlaps. 5) Legacy Industrial Control Systems (ICS) are not patched due to fear of losing functionality. This risk is not evaluated within the CAF. 6) Robust supply chain framework is not available for cyber security 7) DfT does not have auditors experienced in conducting outcome-based risk assessments for cyber security.

4.3 Health Sector

After the Wannacry attack in 2017, the health organizations in England are rigorously managing the key infrastructure vulnerabilities, the supply chain cyber security and personnel security based on the national and local risk assessments (Parliament Select Committee-June, 2018). NHS Digital has provided a national information and technology governance to the health and social care system since 2013 ("Cyber and data security good practice guides - NHS Digital," 2018). The Department of Health and Social Care (DHSC), the CA for the health sector (Refer Appendix F), has published sector-specific NIS implementation guidance (DoH, 2018). NHSE-S1 confirmed that as per the guidelines from DHSC, all NHS Trusts and Foundation Trusts in England are designated as OES. The data in this section was collected from the following stakeholders:

Table c – Stakeholders for Health Sector

Organization	No of Stakeholders	Stakeholder Reference	Data Collection method
DCMS	1	DCMS-S1	Interviews
Department of Health and Social Care (DHSC)	2	DHSC-S1, DHSC-S2	Interviews and email DHSC-S1
NHS England (NHSE)	1	NHSE-S1	Interviews and email
NHS Digital	1	NHSD-S1	Email and FOI request
Central and North West London NHS Foundation Trust	2	NHST-S1	FOI request
Imperial College Health care NHS Trust	2	NHST-S2	FOI request

The health sector uses a Data Security and Protection Toolkit(DSPT) ("Data Security and Protection Toolkit - NHS Digital," 2017) for regulatory assessments, as mentioned by NHSD-S1. DSPT incorporates the 10 data security standards (Refer Appendix-E) provided by National Data Guardian, an organization that advises DHSC on data confidentiality. This toolkit is focused on data and information security. Research in 2017, after the WannaCry attack, has highlighted that effective cybersecurity goes beyond data security (Martin, Guy, Martin Paul, Hankin Chris, Darzi Ara,

2017). DCMS-S1, NHSD-S1 and the NHS trusts(NHST-S1 and NHST-S2), confirmed that the DSPT, rather than the NCSC CAF will be used to self-assess a health sector organization's outcome-based NIS compliance. DHSC-S1 confirmed that DHSC are in the process of updating the DSPT to include the NIS CAF elements. DHSC-S1 and DHSC-S2 confirmed that the plan is to increase alignment with the NCSC CAF requirements from 2019/20. NHS-S1 also mentioned that pilots have been planned with a small group of 10 organizations to refine the risk framework prior to a wider DSPT rollout. As noted by DHSC-S1 "Data security has been included in the Care Quality Commission's (CQC) safety inspection regime (CQC Inspection Framework, 2018) to cover the overlaps between safety and security".

DHSC-S1 also mentioned that the DHSC will ensure that the OES undertake an independent onsite assessment for Cyber Essentials Plus, an NCSC assessment framework used to assess the cyber security technical controls of an organization, to ensure a clear understanding of their cyber security risks and vulnerabilities. However, as mentioned by DHSC-S2 and the Public Accounts Committee(PAC) report, NHS Digital and Care Quality Commission (CQC) audited 200 NHS trusts post 2017 Wannacry attack, and found that all 200 trusts failed the Cyber Essentials Plus on-site assessments (House of Commons, 2018). DHSC-S1 also confirmed, "the technical controls within this tool may not cover the full range of CAF IGP". As mentioned by NHSE-S1, in 2017/18, key NHS Trusts received £21m to address cyber vulnerabilities and to address vulnerabilities of legacy systems; further £25m were also provided (House of Commons, 2018).

In response to vulnerabilities caused by medical devices and IoT, DHSC-S1 confirmed that the national supply resilience strategies for critical medical devices and clinical consumables continue to be developed and implemented("Emergency Preparedness, Resilience and Response (EPRR)", 2017), however, DHSC-S1 confirmed, "smart medical devices and IoT are not specifically covered by the NIS CAF framework". The new Medical Devices Regulations will fully apply from May 2020 and include a greater emphasis on the cyber security of medical devices("Medical devices: EU regulations for MDR and IVDR - GOV.UK," 2018). As explained by DHSC-S1, NHS are in the process of reviewing the guidance and standards for the management and patching of medical devices by Trusts, specifically where the devices are connected to hospital systems.

The National Health Service(NHS) and Public Health England(PHE), as in other sectors, have good levels of emergency response and recovery for non-cyber elements(Cabinet Office, 2017a). In event of a cyber-attack, DHSC-S1 confirmed that the business continuity plans are owned by the trusts and the sector specific emergency response and recovery pilot exercises have been completed by the health sector. The key points from the above analysis are summarized in Table 3 below.

Table 3 Summary of the NIS implementation within the Health Sector in England

NIS Implementation	Health Sector
CA	• DHSC (CA) and CQC (conducts safety inspections) are experienced regulators in health sector • NHS Digital provides technical support to the sector for cyber-security matters
Guidelines	• DHSC has published NIS guidelines which include OES thresholds and incident thresholds • Incident triaging thresholds are currently under development • DSPT updates are in progress to assess the NCSC CAF outcome requirements
Existing frameworks prior to NIS	• DHSC has multiple tools within the framework to assess risks to the health system, notably the DSPT
Regulatory overlaps	Health safety regulatory overlaps with cyber security; health sector combines the safety and security audits.
NIS Assessment framework	• DSPT - DHSC plans to update DSPT with the required CAF elements • Cyber Essentials plus assessment for adequate security measures
Key Technology threats	• Smart medical devices and IoT
Researcher's analysis	Although health sector has mature processes and good governance and processes in place, the current cyber assessment framework is focused on data and information security. Health sector will be the only sector expecting all OESs to go through the cyber essentials plus audit. However, it is noteworthy, that as of today, no OES has passed the Cyber Essentials Plus audit. Current gaps: 1) There is an increased cyber-physical threat from smart medical devices, which, as of today, are not covered under CAF and DSPT. 2) There are overlaps between safety and security regulations which are currently audited by CQC. However, CQC auditors are do not have experience in conducting outcome-based risk management audits. 3) Cyber security risks for legacy systems are not specifically covered by the CAF. 4) A robust supply chain framework is not available for cyber security.

4.4 Drinking Water supply and Distribution

The water sector has published a high level cyber security strategy summarizing what water and sewerage companies need to do to reduce the risks of the cyber-attacks (Defra, 2017). The CAs within the water sector are the Department for Environment, Food and Rural Affairs (Defra) and the Drinking Water Inspectorate (DWI)(DCMS, 2018d). The DWI stakeholder (hereafter DWI-S1), in an email in response to an FOI request suggested, "All of the NIS requirements are in their infancy and need to be shaped". Defra has indicated to the water companies that "this first year of NIS implementation will be formative". The guidance for the OES within the water sector is available at a very high level, OT security measures are being worked out and CAF are yet to be customized for the sector. DWI-S1 mentioned that the water sector is currently relying heavily on support from the NCSC, specifically due to insufficient established cyber security frameworks. Defra has also engaged the DWI inspectors on its behalf due to their expertise gained by regulating the water industry against the Water Quality Regulations. DWI-S1 added that further work is required in the water sector to improve emergency response specific to cyber incidents. The key points from the above analysis are summarized in Table4 below.

Table 4 Summary of the NIS implementation within the Water Sector in England

NIS Implementation	Water Sector
CA	• Defra
Guidelines	• High level NIS guidelines are published
Existing frameworks prior to NIS	• Insufficient established cyber security frameworks
NIS Assessment framework	• CAF
Key Technology threats	• OT
Researcher's analysis	The analysis of the above is that water sector is in a formative stage for cyber-physical security. It will be a challenge for this sector to meet the CAF IGP in the given timelines without a methodology to bring a stepped change in the capabilities. Current gaps: 1) Inclusion of cyber-physical elements for water sector in the CAF 2) There is lack of audit experience within the CA and hence DWI inspectors will be involved in the sector's cyber security. However, DWI inspectors do not have the experience in conducting outcome-based risk management audits. 3) Emergency response specific to cyber incidents are to be developed at sector level.

4.5 Energy

The Office of Gas and Electricity Markets (OfGem) and Business, Energy and Industrial Strategy (BEIS) are the CAs for the energy sector in England (BEIS, 2018). The OfGem stakeholder (hereafter OfGem-S1), in an interview, provided the information on NIS compliance activities. BEIS also provided information in response to an FOI query. BEIS will develop guidelines for the CA and the OES in autumn 2018, OES assessment against the NCSC CAF in 2019, the implementation of the action plans in 2020, and compliance audits post 2020 (BEIS, 2018). DCMS-S1 explained that considering the regulatory experience required to enforce NIS compliance framework, BEIS will leverage the Health and Safety Executive (HSE) inspectors. OfGem-S1 confirmed that the NCSC CAF will be used as the NIS enforcement framework, except for those aspects of the OES services which fall within the scope of the requirements laid out in in the Smart Energy Code. DCMS-S1 confirmed that pilot exercise planning is in progress for sector-specific cyber disruption and recovery exercises. OfGem-S1 also expressed a personal view that the issue of the cyber security of supply chain needs to focus on strengthening the weaker links rather than making the strong link stronger. The key points from the above analysis are summarized in Table 5 below.

Table 5 Summary of the NIS implementation within the Energy Sector in England

NIS Implementation	Energy Sector
CA	• Ofgem
Guidelines	• High level NIS guidelines are published, specific guidance will be published for the CA and the OES on the security practices and self-assessment needs by autumn 2018
Existing frameworks prior to NIS	• Insufficient for managing cyber risks
NIS Assessment framework	• CAF
Key Technology threats	• Smart energy
Researcher's analysis	Energy sector is in a formative stage for management of cyber risks. Current gaps: 1) There is an increased cyber-physical threat from smart energy, which is not covered under CAF but is managed separately under Smart Energy code. 2) There is lack of audit experience within the CA and hence HSE inspectors will be involved in the sector's cyber security. However, HSE inspectors do not have the experience in conducting outcome-based risk management audits. 3) Robust supply chain framework is not available for cyber security.

4.6 Digital Infrastructure

The Office of Communications (OfCom) is the CA of the Digital Infrastructure sub-sector. (Refer Appendix F) The Digital Infrastructure sector is based on electronic and communication services, and includes elements of internet infrastructure such as internet exchanges, domain name service providers, internet exchange point operators (OfCom, 2018). For Ofcom this is a change in scope from their responsibilities for the telecom networks, economic regulation and media ("Oral evidence - Cyber Security: Critical National Infrastructure," 2018). Ofcom, under the FOI Act provided the published interim guidance which includes identification of the OES, use of the NCSC CAF for self-assessment of the OES and incident reporting thresholds (OfCom, 2018). Ofcom is proactively working with government and the NCSC to implement a scheme called Transit Boardings Estimation and Simulation Tool (TBEST) ("Oral evidence - Cyber Security: Critical National Infrastructure," 2018), similar to the CBEST framework to test vulnerabilities within the NIS. DCMS-S1 also confirmed that Ofcom has carried out sector-specific emergency response pilot exercises on fixed and mobile networks, lessons are being learnt, and improvements implemented. The key points from the above analysis are summarized in Table 6 below.

Table 6 Summary of the NIS implementation within the Digital Infrastructure Sector in England

NIS Implementation	Digital Infrastructure
CA	• Ofcom
Guidelines	• OfCom has published NIS guidelines, which include OES thresholds and incident thresholds.
Existing frameworks prior to NIS	• None that address cyber security of the CNI. This is change of scope for the sector's regulator.
NIS Assessment framework	• CAF
Researcher's analysis	Current gaps: 1) OfCom is an experienced regulator in media and communications. However, auditors are not experienced in conducting outcome-based risk management audits for cyber security.

4.7 Digital Service Providers

The Information Commissioner's Office (ICO) is the CA for the DSP (Refer Appendix F) and is guided by The Cooperation group and the ENISA (DCMS, 2018b). In response to an FOI request, the ICO noted that required initial guidance to the relevant DSPs has been published on the ICO website ("The Guide to NIS," 2018). As per this guidance, to facilitate identification of DSPs, all DSPs are required to register with the ICO within a timeframe specified by the ICO. The ICO also stated that the DSPs are currently working towards ISO27001 certification for their entire digital services using the Octave Allegro framework identified by the NCSC ("Table view of principles and related guidance," 2018b). DCMS-S1 confirmed that the ICO is using this framework for NIS regulatory compliance. Concerns have been raised on overlaps between GDPR and NIS for DSPs who are also data controllers (DCMS, 2018d). Table7 below summarizes the key points from the above analysis.

Table 7 Summary of the NIS implementation within the DSP in England

NIS Implementation	DSP
CA	• ICO
Guidelines	• Initial guidance has been published for DSPs
Existing Risk assessment framework prior to NIS	• Frameworks for GDPR, data and information security
NIS Assessment framework	• ISO27001 (Risk management) certification using Octave Allegro Framework.
Researcher's analysis	ICO is an experienced regulator currently regulating GDPR Current gaps: 1) Data and information assurance auditors for GDPR are not experienced in conducting outcome-based business assurance audits

5. Results - Case Studies

5.1 Case Study 1: Analysis of Health sector's Cyber security Assessment Framework

This case study was conducted to assess the gaps between the current cyber security regulatory framework within the health sector and the NIS framework. To understand the gaps for the health sector against the compliance with the NIS, the DHSC has provided an initial mapping of the 14 NCSC CAF principles ("Table view of principles and related guidance," 2018a) against the DSPT security standards (Refer Appendix-E), the assessment framework for NIS compliance in health. As mentioned by DHSC-S1, DSPT was recently modified to include GDPR elements using a checklist approach. DSPT will be updated again in autumn 2018 to include the CAF elements. The work-in-progress comparative analysis presented here was provided by the DHSC only for the purpose of research. The researcher conducted an independent assessment by mapping expected outcomes within the NIS CAF principles to the DSPT standards. The output of this analysis provided the NCSC CAF compliance assessment areas, which were not covered by the assessment questionnaires in DSPT (see table 8 below).

Table 8 Comparative Analysis of Health Sector's Assessment Framework and NCSC CAF

NIS Objectives	NIS PRINCIPLES (NCSC CAF)	Mapping with DSPT v5.1	Is the NIS Principle covered by DSPT ?	Gaps (as provided by DHSC based on the work-in-progress so far)
" **Objective A:** Appropriate organizational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services."	A1 Governance	Data Security Standard 1	Full	The requirement for "empowered to make decisions on how services are protected" will be added in detail to the guidance.
	Researcher's analysis:- Considering the outcomes of the three controls "A1a) Board Direction A1b) Roles and Responsibilities A1c) Decision-making", as mentioned in the CAF, effectiveness of Governance process and controls in all three areas was identified as an additional gap. DSPT is only checking the presence or absence of an accountable role (Senior Information Risk owner).			
	A2. Risk Manage-ment	Data Security Standards 1, 4, 8, 9	Partial	Whilst there is some risk management and threat assessment undertaken by organisations completing the DSPT, this is not at the level outlined in the NIS document. Key Gaps: 1) Threat assessment 2) Vulnerability Assessment
	Researcher's analysis:- DSPT focuses on data protection, information security, data processing, access control, unsupported software/systems risks and Data Security Improvement Plan based on risk assessments. Considering the outcomes of "A1a) Risk Management Controls A2b) Assurance" as mentioned in the CAF, the effectiveness of risk management process and controls and the assurance of the risk management process were identified as additional gaps.			

NIS Objectives	NIS PRINCIPLES (NCSC CAF)	Mapping with DSPT v5.1	Is the NIS Principle covered by DSPT ?	Gaps (as provided by DHSC based on the work-in-progress so far)
" **Objective A:** Appropriate organizational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services."	A3. Asset Management	Data Security Standard 1, 2	Partial	Whilst some risk management and threat assessment is undertaken by organisations completing the DSPT, this is not at the level outlined in the NIS document. Supporting infrastructure needs to be understood and assessed
	Researcher's analysis:- Considering the outcomes of "A3a. Asset Management" as mentioned in the CAF, the focus for asset management to include data, people and systems, as well as any supporting infrastructure (such as power or cooling) as mentioned in the principle was identified as an additional gap.			
	A4. Supply Chain	Data Security Standard 10	Partial	Covered both in the GDRP and Contacts section of the DSPT. The key gap lies in understanding the accountability for outsourcing.
	Researcher's analysis:- Considering the outcomes of "A4a. Supply chain" as mentioned in the CAF, assessment against a risk-based framework for managing supply chain cyber security, as mentioned in the principle, was identified as an additional gap.			
" **Objective B:** Proportionate security measures are in place to protect essential services and systems from cyber attack."	B1. Service Protection Policies and Processes	Data Security Standard 1	Partial	Policies are well covered in DSPT, minor gaps on confirming the measures undertaken in the DSPT cover the requirement for validating the implementation and effectiveness of policies.
	Researcher's analysis:- Considering the outcomes of "B1a Policy and Process Development B1b. Policy and process implementation" as mentioned in the CAF, there is additional gap - how to ensure that the security benefits achieved can be demonstrated and the implementation validated. The data, information and staff awareness policies partially map to the risk of cyber security-related disruption to the essential services.			
	B2. Identity and Access Control	Data Security Standard 1, 4, 10	Partial	Access Control review is included, Gaps: verifying user identity to access systems, specifying higher level access requiring two factor authentication and the ability to demonstrate different types of unauthorised user are unable to access systems.
	Researcher's analysis:- DSPT includes physical, personnel and data access guidance. Considering the outcomes of "B2a. Identity verification, authentication and authorisation, B2.b Device management, B2.c Privileged user management and B2.d IDAC management and maintenance", as mentioned in the CAF, an additional gap regarding access control of all services and NIS exists. There is also no mention of medical and IoT devices in the CAF and DSPT.			

NIS Objectives	NIS PRINCIPLES (NCSC CAF)	Mapping with DSPT v5.1	Is the NIS Principle covered by DSPT ?	Gaps (as provided by DHSC based on the work-in-progress so far)
" **Objective B:** Proportionate security measures are in place to protect essential services and systems from cyber-attack."	B3. Data Security	Data Security Standard 1 to 10	Partial	Lifecycle management and destruction included but not explicit reference to mobile devices.
	Researcher's analysis:- DSPT includes wide range of data security controls in all standards. CAF defines the outcomes "B3.a Understanding data, B3.b Data in transit, B3.c Stored data, B3.d Mobile data and B3.e Media / equipment sanitisation". The gaps in DSPT in addition to the above, include access control of all services and NIS, third parties storing, or accessing data and the transit of data that is important to the delivery of an essential service.			
	B4. System Security	Data Security Standard 2, 4, 8	Partial	DSPT contains support for patching, supported systems, access control, and physical protection but not at the level described in CAF. The gaps include control over software installation by users, removable media, network connections, hardware and software management, APIs and wi-fi device authentication and disabling network ports by default.
	Researcher's analysis:- Considering the outcomes of "B4.a Secure by design, B4.b Secure configuration, B4.c and Secure management and B4.d", mentioned in the CAF, researcher came up with similar gaps as above. The additional gap identified was the element of vulnerability of IoT devices and the need for security by design in any new products or services, which is not addressed as the CAF does not include IoT.			
	B5. Resilient Networks and Systems	Data Security Standard 7	Partial	Included as part of the GDPR, protection by design and business continuity but not to the level described. Restrictions on the use of management accounts to be included
	Researcher's analysis:- Considering the outcomes of "B5.a Resilience preparation, B5.b Design for resilience and B5.c Backups" as mentioned in the CAF, gaps identified include tests for simplistic hygiene such as secured current backups of data and information and an overall resilience specific to the design, implementation, operation and management of systems.			
	B6. Staff Awareness and Training	Data Security Standard 2, 3	Full	Data Security awareness training mandatory for staff with graduating levels depending on role.
	Researcher's analysis:- Considering the outcomes of "B6.a Cyber security culture, B6.b Cyber security training", as mentioned in the CAF, the gaps identified include evaluation of training, recognition of incident reporting, building ownership, creating a security culture or management involvement and commitment to build the right behaviours.			

NIS Objectives	NIS PRINCIPLES (NCSC CAF)	Mapping with DSPT v5.1	Is the NIS Principle covered by DSPT ?	Gaps (as provided by DHSC based on the work-in-progress so far)
" **Objective C**: 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	Data Security Standard 9	Partial	Encryption included. Also covered if organisation has implemented another framework as part of standard 9. Log monitoring, use of tools and skilled analysis to be included
	Researcher's analysis:- Considering the outcomes of "C1.a Monitoring coverage, C1.b Securing logs, C1.c Generating alerts, C1.d Identifying security incidents, C1.e Monitoring tools and skills", as mentioned in the CAF, the additional gap identified relates to the alerts based on threats for all the systems within the critical NIS service (not just the data and information critical systems).			
	C2. Anomaly Detection	Data Security Standard 5,7	Partial	Some elements covered under business continuity response and process review. Understanding normal operations and detecting activity outside the norm to be included
	Researcher's analysis:- Considering the outcomes of "C2.a System abnormalities for attack detection and C2.b Proactive attack discovery", mentioned in the CAF, additional gap includes processes for understanding, searching and alerting for abnormalities for all the NIS.			
" **Objective D:** Capabilities to minimise the impact of a cyber-security incident on the delivery of essential services including the restoration of those services where necessary."	D1. Response and Recovery Planning	Data Security Standard 7	Full	The document only mentions data security. It is covered by business continuity Standard 7 but will require guidance to be updated.
	Researcher's analysis:- DSPT is focused on the response and recovery of data loss. It is not clear if the systems and networks are included. Considering the outcomes of "D1.a Response plan, D1.b Response and recovery capability and D1.c Testing and exercising", mentioned in the CAF, additional gaps include evaluation of training, recognition of incident reporting, building ownership, creating security culture or management involvement and commitment in building the right behaviours.			
	D2 Lessons Learned	Data Security Standard 5,7	Partial	Some elements covered by business continuity and process review standards. Key gap - Addressing root cause, not just the issue
	Researcher's analysis:- Considering the outcomes of "D2.a Incident root cause analysis, D2.b "Using Incidents to drive Improvements", mentioned in the CAF, additional gap was identified for the root cause analysis of all the NIS incidents which include data breach for remediating action to protect against future incidents.			
*Assumption: The DSP toolkit is the only NIS compliance assessment tool being used in the health sector in England for cyber security risk management. The on-site assessments against Cyber Essentials Plus also contributes to cyber security assessment however, it focuses on technical controls and not the service risk management and resilience as in NCSC CAF. This was validated with DHSC-S1.				

As seen in the analysis captured in Table 8, the DSPTv5.1 self-assessment checklist does not cleanly map to the 14 CAF principles. This is because the NIS regulation is about cyber risk management rather than the data and information security management as managed in DSPT. The analysis also strongly suggests that modifying the DSPT for CAF elements might not be enough to move away from a checklist mentality. It might therefore miss the opportunity to meet the NIS objective of outcome-based assessments to improve the cyber security risk management capabilities of the health sector. The DSPT assessment framework will be more effective if the toolkit assesses the management of the dynamically prioritized key risks and the effectiveness of the risk management controls. Under NIS regulation the CA is not mandated to use the CAF, nor is the OES required to meet all the CAF outcomes if the OES has taken appropriate and sufficient security measures. However, this flexibility calls for a governance mechanism for continuous independent assessments of the NIS implementation to ensure that the implementation meets the NIS strategic objectives. KPIs for NIS framework need to be defined, measured and analyzed to support this process.

5.2 Case study 2: Cyber security in Smarter London Together Roadmap

The Chief Digital Officer (CDO) of London, appointed by the Mayor of London, engaged with the researcher and provided inputs as well as further contacts to make this study successful. The transport and health sectors within Smart London have already been analysed in the sections 4.1 and 4.2 and therefore have not been included in the case study. The data in this section was collected from the following stakeholders:

Table d – Stakeholders for Smart London Case Study

Organization	No of Stakeholders	Stakeholder Reference	Data Collection method
Greater London Authority (GLA)	3	GLA-S1, GLA-S2, GLA-S3	Interview
London Metropolitan Police	1	LMP-S1	Interview
London Fire Brigade	2	LFB-S1, LFB-S2	Interview
London Resilience Group	1	LRG-S1	Interview
CPNI		CPNI-S1	Interview
Hitachi Vantara	1	HV-S1	Interview
ORR	1	ORR-S1	Interview
BSI	1	BSI-S1	Email

GLA-S1 explained that the Smart London planning includes collaboration at corporate level within "33 local authorities, 40 NHS regional centres and private utility companies fragmented across 650 lines of business", as mentioned by the CDO. GLA-S1 also pointed out that "the plan is intended to join up specific vertical sectors (e.g. utilities, transport, health, etc.) across organizational boundaries into a whole-city approach". GLA-S1 further explained that the Smart London aims to deliver an open, service-oriented, city-wide world-class connectivity, with user-designed secure services and data sharing across public-private sectors. This requires city-wide collaboration, enhanced digital capabilities and a solid cyber security strategy. As stated by GLA-S2 there is a plan to identify the cyber security risks associated with the governance and accountability, the data sharing across organizations and the (lack of) common standards across an array of technologies. GLA-S3 expressed concerns over the cloud security within Smart London organizations.

LMP-S1 mentioned that the Metropolitan Police cyber security is in the formative stage. LMP-S1 emphasized that there is a rise in cybercrimes due to the imbalance between cybersecurity, accessibility and functionality of the systems. The main concerns expressed were:

1. People are aware that the cyber security threats are catastrophic, but there is very little understanding of what can be done to address the threats.
2. There needs to be a change in people's behaviour to make them understand the risks of negligence, such as lack of a strong password
3. Systems should be secure by design. Ethical hacking and vulnerability tests such as penetration tests are undertaken too late in the lifecycle. Regulatory frameworks should

look at mandating these tests for design stage.

LMP-S1 had a perception - “this is a Jurassic park moment where we are focusing on how to build more interconnected digital systems rather than thinking of whether they should build them at all without causing harm”. LMP-S1 pointed out that cyber security risk management is not mature within most organisations - people generally accept the risks due to lack of understanding of how to mitigate them.

LFB-S1 and LFB-S2 mentioned a good cyber security risk identification and governance existed within London Fire Brigade. The critical cyber threats are minimal as alternate channels such as telephones are available for communication during emergency within London Fire Brigade. The London Resilience Forum oversees the work of the London Resilience Partnership, setting the strategy and objectives for resilience and preparedness for emergencies in London. The Forum and Partnership represents more than 170 organizations ranging from the emergency services, local authorities, the NHS, the utility providers and transport service providers. As mentioned by LRG-S1, the London Community Risk Register (London Resilience Partnership, 2017) underpins the resilience planning/preparedness activity of the London Resilience Partnership (“London Resilience Partnership,” 2013). LRG-S1 also mentioned that “the London Resilience Forum retains strategic oversight of the work of the London Resilience Partnership, development of capabilities and the accountability for the emergency preparedness arrangements in London” (“London Resilience Forum,” 2013). In response to a query, LRG-S1 confirmed that the Partnership’s generic plans and emergency response arrangements are designed to cover any eventuality, which would include an emergency because of a cyber-attack. The London Resilience Partnership’s plans do not currently include specific arrangements for the response to a cyber-attack, but a project is in place to develop these arrangements.

HV-S1 mentioned that there exist multiple smart infrastructure testing facilities in London such as
a) the Building Research Establishment (BRE) to test smart homes and
b)Transport Research Lab (TRL) to test smart vehicles with TfL
He added that these smart space operators are regulated under HAZOP (Hazard and Operability) for safety of smart spaces, but not under specific cyber security risk management regulations. Based on inputs from ORR-S1, multiple national and international standards are defined for Smart City. Amongst these, the Publicly Available Specification(PAS) 185:2017, commissioned by CPNI and facilitated by British Standards Institute(BSI), is the UK specification for establishing and implementing a city-wide, strategic-level, security-minded information sharing approach for smart city(CPNI, 2017). PAS 555, Cyber security risk – Governance and management standard uses an outcomes-based approach to cyber security for a smart city, however, it does not specifically

address the security issues that arise in a smart city (BSI, 2017).

The stakeholder interviews confirmed that there is a need to enforce a common requirement for cyber security risk management capability across all organisations to prevent development of silos of smart spaces instead of an integrated Smart London city. The gap in cross sector resilience highlighted in section 4.1 is supplemented by lack of emergency planning and recovery responses to a cyber-attack within London. Many of the public sector organizations within the GLA need to extend the responsibilities of the cyber security risk management beyond their IT divisions, and include both senior and executive leadership across all key departments as responsible and accountable contributors. The non-CNI organizations can benefit from the best practices from the enforcement of the NIS legislation within CNI sectors and possible support from NCSC. Cyber security risk management should be integrated into the design cycle of the smart city services and products rather than refactoring these with more expensive and difficult solutions later. This means inculcating the right behaviors in people, contributors, suppliers and consumers.

6. Discussion

NIS implementation is a business transformation model that is intended to deliver valuable capabilities in the industry in a scalable and sustainable manner. Based on the interviews and material provided by stakeholders across sectors, a number of key themes have emerged with regards to the elements of this business transformation model.

1. **NIS Organization and Governance:** Although there is awareness that holistic security measures across cyber, physical and personnel security need to be implemented, there is currently a danger of not addressing the key overlaps between cyber and non-cyber security measures. There could also be possible duplication within NCSC and CPNI frameworks. For example the CPNI security management guidelines refer to ISO 28000:2007 which is specific to information security and also includes NCSC CAF elements (CPNI, 2018). This can result in inefficiencies due to OES/DSP working towards separate physical, cyber and personnel security regulatory compliance for overlapping requirements. The supply chain principle and assessment guidelines are published by the CPNI(CPNI, 2018a) with relevant IGPs. These guidelines can be included in the NCSC CAF.

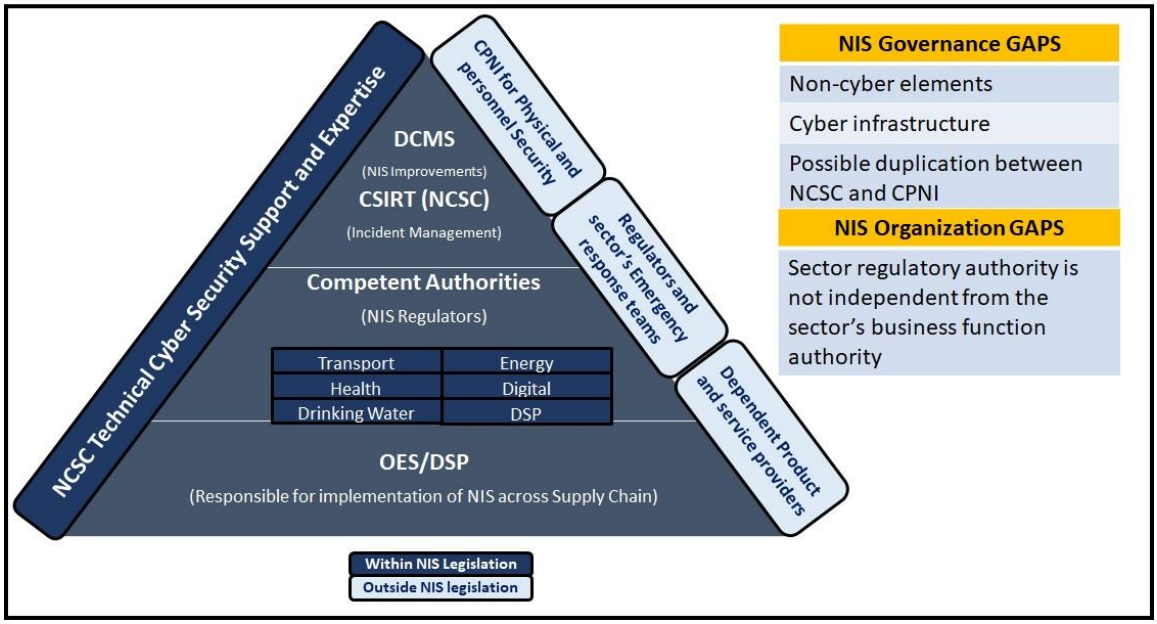
   The cyber infrastructure such as data centres and transmission lines are a gap not covered by the NCSC and CPNI frameworks which was raised by the DSPs to the DCMS in the public consultation (DCMS, 2018a). The reporting of cyber risks in the data centres is already part of the US cyber security framework (Department of Homeland Security, 2015). Hence, it is recommended that these gaps need to be assessed further for business and critical risk impacts. A holistic security governance approach can possibly resolve the above gaps.

   Recommendation 1: Cyber, physical and personnel areas to be included in NCSC CAF in the first year of NIS implementation with holistic security governance

   The UK has implemented a multiple CA model for NIS enforcement. The Government departments that have business responsibilities for a specific sector are also tasked with the CA responsibility of regulating the NIS, wherein they make judgements of what are appropriate and proportionate security measures. As a result, there is a possibility that a compliance judgement might be influenced by the budgetary or business constraints. As an example of budgetary challenges in the context of NIS, it will be extremely counter intuitive if the DHSC issues heavy monetary fines on the budget starved NHS trusts for cyber security non-compliance, as this could take away critical budgets from health care provision. However, insufficient cyber security can

be a threat to healthcare provisioning, both, in health and data risks, which makes it a very difficult issue to resolve. As evidenced in section 5.1, the DSPT does not map fully to the 14 NIS principles. However, the DHSC is empowered to take decisions on what assessment needs to be included within the DSPT based on their decision of appropriate and proportionate security measures, which may not be consistent across sectors for end-to-end service resilience. For reference, the framework in Figure 4 summarizes the current NIS Governance and considered gaps.

Figure 4: Organization and Governance - NIS Framework



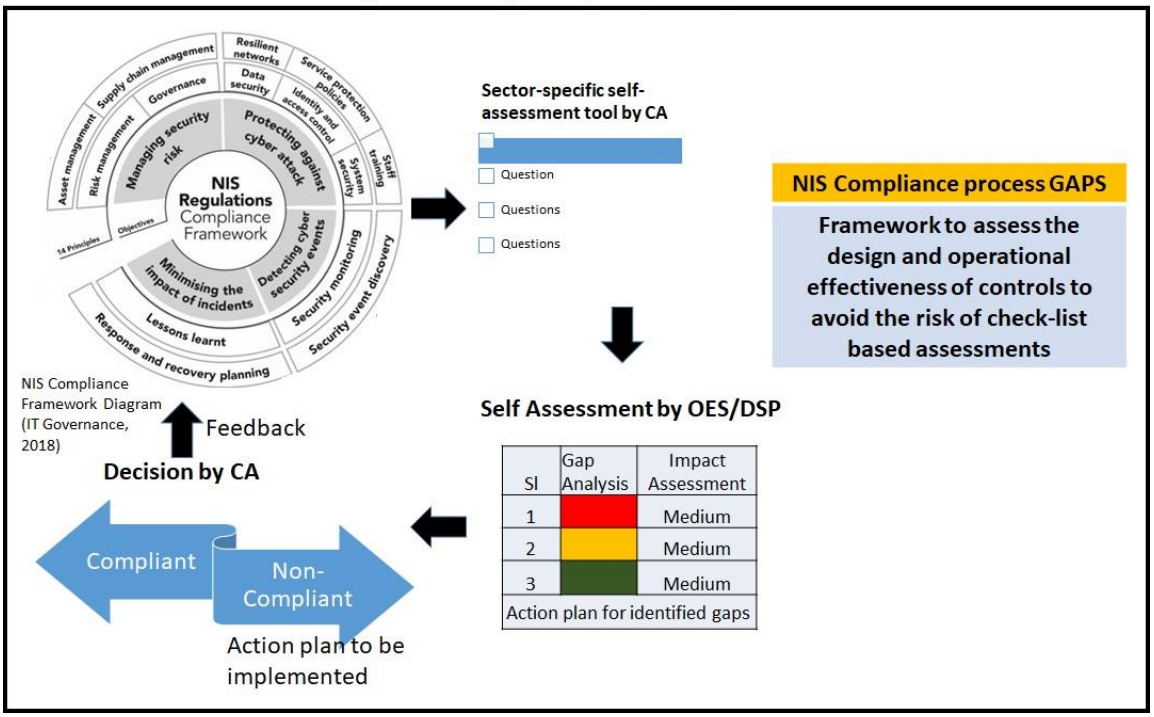
A specialist team consisting of sector CA representatives, DCMS and NCSC is required to validate that the up-to-date NIS regulatory assessments are in place across sectors and these are in-line with the NIS principles. This governance measure can provide an independent assessment for the NIS audit framework and provide a quality check on the CA decisions for consistent appropriate and proportionate security measures for NIS compliance across sectors.

Recommendation 2: DCMS to work with CA and NCSC to introduce an outcome-based NIS audit framework oversight and governance. This governance is intended to ensure appropriate implementation and assessment of NIS principles by an authority independent from the CA business functions.

2. **Process: Compliance Assessment:** This year, since May 2018, the OES and DSP have been assessing themselves using the self-assessment guidance provided by the sector's CA. The CAs are engaging with the OES and DSPs to understand the self-assessment gaps, action plans and strategies for regulating the sector in the first year. Figure 5, depicts the compliance assessment

process whereby the CA will be reviewing the gaps from the OES and DSP self-assessment to determine compliance with NIS legislation.

Figure 5: NIS regulatory compliance process



The NIS CAF is an outcome-based approach that specifies what needs to be achieved rather than exactly what needs to be done. The CAF compliance approach provides space for quality judgements, which unfortunately can make assessment strategy a subjective issue across sectors. For example, the self-assessment tool in the health sector seen in the case study in Section 5.1, currently uses a tick box exercise approach for checking for presence of selective controls. In contrast, the finance and banking sectors have recognized that a check-list based compliance assessment itself may not successfully assess the effectiveness of the risk management process (H.M.Treasury, 2016). Therefore, the organizations in the finance and banking sectors conduct effective regulatory assessments of the design and operational effectiveness of key controls that have been mapped to the top risks that the organizations face (Chartered Institute of Internal Auditors, 2018). To achieve the outcome-based objective of the NIS CAF, a similar risk-based audit framework is recommended for all NIS compliance assessments across all sectors. The best practices from the CBEST tool described in Section 4.1, can also be re-used by other sectors for self-assessment to provide common tools for the NIS assessment framework.

Recommendation 3: NIS Audits to assess the effectiveness of key controls of top business and service assurance risks

3. **Processes: Incident Management AND Emergency Response and Recovery:**

OES/DSP are required to share incidents beyond a defined threshold to their CAs within 72 hours of being aware of the occurrence. As explained by DFT-S1 in Section 4.2, the CAs will conduct post-incident analysis of incidents beyond a pre-defined threshold. However, as per the NCSC CAF, the lessons learnt from incident root-cause analysis are limited to the OES and DSP organizations. It is recommended that the CAF IGP include cross-sector lessons learned to ensure that the knowledge gathered is utilized by the entire industry.

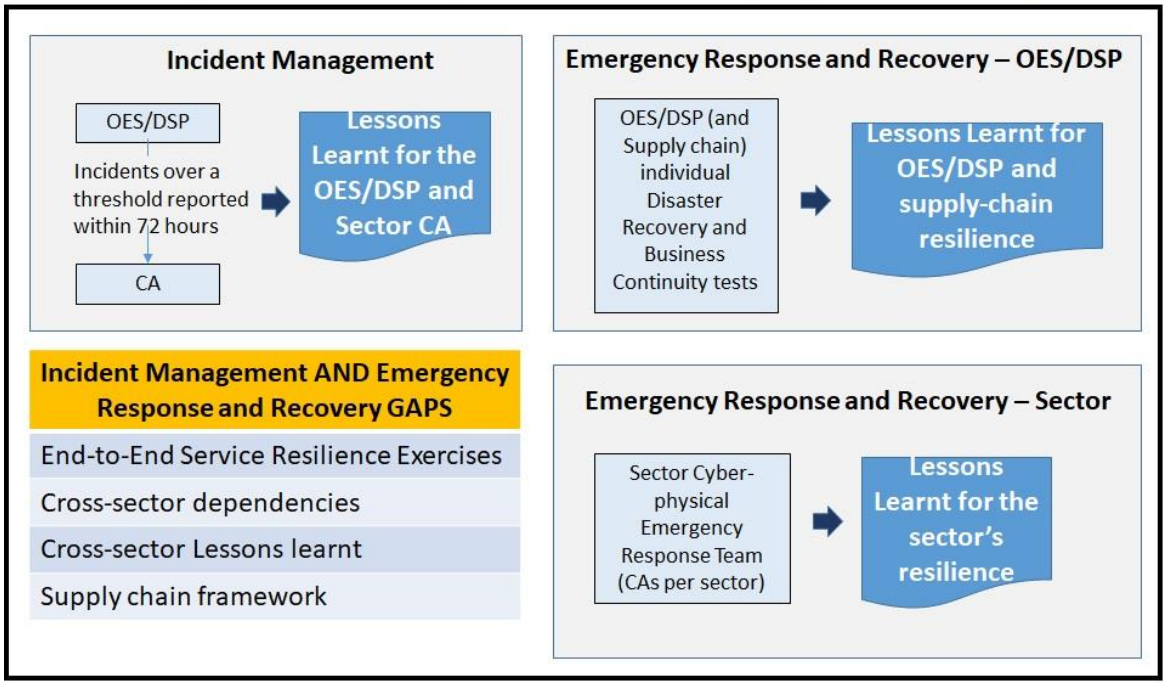
The growing concern in cross-sector cyber security is the emergence of circular dependencies between different critical sectors. Cyber-attacks can have catastrophic consequences due to the ripple effect of failure of a single system on other inter-connected systems. For example, a failure in regular electricity supply can cause harm to critical transport or medical services and, in extreme circumstances blackouts, which can spread globally. The cross-sector security risk and emergency recovery processes are currently at different stages within different sectors. The finance sector is compiling the lessons from 34 live disaster recovery exercises at sector level, and Ofcom and NHS are past the pilot phase in their sectors, however, there is a total lack of structured coordination, registration and escalation for cross-sector resilience tests even between these leading sectors. ("Oral evidence - Cyber Security: Critical National Infrastructure," 2018). More focus is required within the NIS on cross-sector resilience to understand and strengthen cross sector dependencies (UKRN, 2015). The members of cross-sector regulatory collaborative forums such as the UKRN are facilitators and the experts within the regulatory organisations are not currently not actively participating in the forum ("Oral evidence - Cyber Security: Critical National Infrastructure," 2018). The end-to-end impact on a common service due to different levels of cyber capability maturity of the organisations operating this service across sectors is not managed by UKRN or NIS. The cross-sector security and resilience processes are not covered by the CAF. Cross-sector lessons learnt can be strengthened by the voluntary information sharing of incidents and threats across the private, Government and public sectors (NCSC, 2017).

Recommendation 4: NCSC CAF to include cross-sector End-to-End holistic service resilience. CA forums to collate and share cross-sector lessons learnt with the industry.

The international supply chain comes with multiple threats, such as the impact of global security vulnerabilities, personnel and physical risks on CNI services in the UK. Under NIS, the OES and DSP are responsible for appropriate and proportionate measures to be applied by the supply chain.

Figure 6 summarizes the process and gaps in this section.

Figure 6: Incident Management AND Emergency Response and Recovery



Supply chain cyber security general awareness and approach are discussed in some of the CA guidelines. It is recommended that supply chains should be Cyber Essentials Plus certified to resolve the supply chain cyber security issues (CPNI, 2018a), but in health sector the difficulty in achieving this even for the OES is evident, as seen in Section 4.3. In the public consultation with DCMS, the OES and DSPs have shared their concerns that the NIS legislation is not directly applicable to the supply chain and there is a lack of a robust supply chain cyber risk management framework across sectors (DCMS, 2018a). Currently there is no clear mitigation for this gap as explained by FCA-S1 in Section 4.1.

People Capabilities: The NIS regulation is part of the NCSC's cyber security strategy 2016-2021 and £1.9 billion funding has been provided for its implementation strategy (H.M.Government, 2018a). However, a lack of skills at operational and governance levels, as well as difficulties associated with the estimation of infrastructure costs are just some of the key budgeting issues associated with mitigating cyber security risks (DCMS, 2018a). Each sector seems to have their own approach to address this shortfall in regulatory experience. BEIS are planning to use retrained in-house Health and Safety (HSE) capacity, and Defra plans to use DWI inspectors for audit activities. Figure 7 summarizes the gaps for each sector.

Figure 7: NIS people skills

Sector	CA and Audits
Health	Department of Health and Social Care(DoH) – Experienced Regulator Care Quality Commission(CQC)– Experienced Safety inspector
Transport	CAA – Experienced Regulator, audit for existing framework with experienced auditors DfT – Audit framework is work-in-progress
Energy	BEIS and OfGem – not experienced in the cyber-security audits Health and Safety (HSE) inspectors to be used for audit activities
Water	Defra – not an Experienced Regulator DWI inspectors to be used for audit activities
Digital Infrastructure	OfCom – Experienced regulator previously in communications and media, will re-use existing audit capability
DSP	ICO – Experienced in GDPR enforcement Will reuse ISO 27001 and GDPR audit team

NIS People Capability GAPS
Outcome focused auditors

As mentioned in point 2, 'Process-Compliance Assessment' of this section, business and service assurance-based audits, which assess the quality of risk management, are recommended for NIS assessments. Control engineers and security engineering can combine best practices to design controls that are focused on NCSC strategic objectives for cyber security such as defend, deter and develop, rather than testing fault tolerance. This approach needs professionals who understand programme management, risk management and business/service assurance. Developing audit collaboration from resources in these roles will potentially address the issue of skills shortage as well as transform the checklist-based audit approach to an outcome-based approach.

Recommendation 5: Setup cross-disciplinary teams of management, risk, security, quality, audit and assurance professionals to develop an outcome-based audit team

Technology: The Industrial Control Systems (ICS) such as supervisory control and data acquisition (SCADA) in manufacturing and industrial environments are the key OT vulnerabilities compounded by the IoT. As mentioned by ORR-S1, the physical devices/machines controlled by ICS connected to the internet to enable real time monitoring and control, were not designed with cyber security in mind (legacy), and thus are potentially vulnerable to cyber-attacks. There is limited knowledge about legacy systems and the associated risk and security simply due to age and loss of knowledge. Additionally, there needs to be a clear understanding of why the security of these OT systems is different from the security

of IT systems and what the risks are (EECSP, 2017). As a simple mitigation, the IT and the OT systems or networks need to be completely separated to prevent cyber-attacks within the IT systems causing damage to the physical OT systems (Ruffle Simon, Daffron Jeniffer, Copic Jeniffer, Leverett Éireann, Evan Tamara, 2017). CPNI has provided best practice guidelines on ICS and technology project security which also map to the NIST framework (CPNI, 2015). These guidelines have been reflected on NCSC webpage ("Security for Industrial Control Systems," 2018). However, the ICS and OT risk management compliance outcomes are not part of NCSC CAF.

There is no appropriate regulation for the IoT, the connected network of physical devices. The challenge lies in the fact that IoT devices can be owned by anyone and may be able to form an unauthorized connection with an organization's systems or critical assets or devices, for example, within a hospital a pacemaker embedded within a patient (Urquhart & McAuley, 2018). Innovative technology guidelines have been provided in some instances such as CAV by DfT (*The Key Principles of Cyber Security for CAV*, 2017), BSI smart city standards (BSI, 2014) and IoT guidelines by DCMS and NCSC (*Secure by Design*, 2017). However, it is recognised that to be truly effective, work to improve IoT security cannot be taken forward in isolation and needs to be a part of an integrated approach to smart cities, device management, and personal accountability in both a professional and private capacity. The NCSC CAF currently does not specifically include outcomes for management of risk and resilience from technological threats from the smart transport, smart medical devices and smart energy.

Legacy OT systems are functional; however, they operate in the same cyber space as the sophisticated smart IoT devices. This will result in the connected smart city more vulnerable. Lack of timely patching of the OT can cause severe threats to the CNI, for example, the patching of medical devices was one of the key issues pointed out by the Chief Information Officer's review of the WannaCry attack (House, 2018). Currently there is limited mitigation available for legacy systems and the alternative of replacing these systems is very expensive.

Figure 8 summarizes these technology gaps in the NIS CAF.

Figure 8: NIS – Technology risk management outcomes in CAF

Technology	Outcomes in CAF
IT	IT systems and Network Risks covered in CAF
OT including ICS	Legacy issues
Smart Devices	Smart transport, smart medical devices and smart energy frameworks and regulations separate from NIS

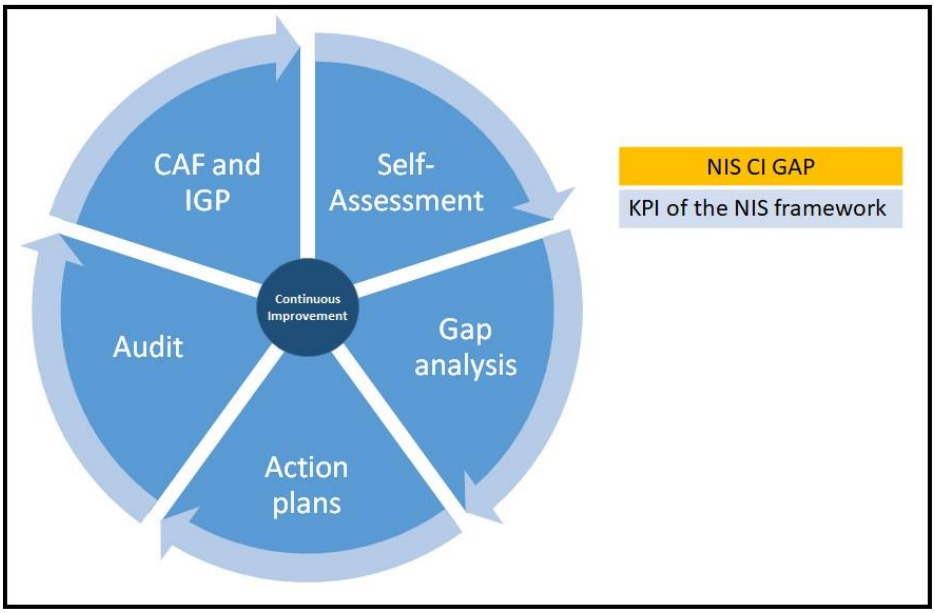
NIS Technology GAPS in CAF
IoT, OT, ICS and smart devices
Patching legacy systems

Recommendation 6: NCSC CAF to include IGP specific to risk management of IoT, OT, smart products and smart services

4. **Continuous improvement:** The DCMS is committed to providing a report of assessment of the impact and effectiveness of the NIS by 2020 (H.M.Government, 2018). However, in the area of cyber security risk management, there is a lack of agreed KPIs across industry globally, which will make the measurement of the success of NIS implementation challenging (Parliament Select Committee-June, 2018).

Figure 9 summarizes the gap specific to lack of KPI for NIS regulation.

Figure 9: NIS – Continuous Improvement Gaps



The success criteria for NIS legislation can also be defined based on the CAF assessments. The KPIs need to be embedded as a part of this process for continuous improvements rather than be added as a retrofit measure. The CPNI PDCA checklist, already provides the guidelines to define measures for security management and effectiveness assessment (CPNI, 2018).

Recommendation 7: NIS KPIs to be defined in the first year in order that data is gathered to manage NIS performance for continuous improvements.

5. **Security culture:** The need for products and services to be secure by design has been in the industry prior to the advent of smart infrastructure. It is concerning that a regulation is required for cyber security for CNI and smart city operations, ideally all designs and engineering lifecycles should consider security from the very earliest stages. NCSC CAF and smart city initiatives need to include IGP for building security into the engineering lifecycle of connected smart spaces, CNI services and smart products.

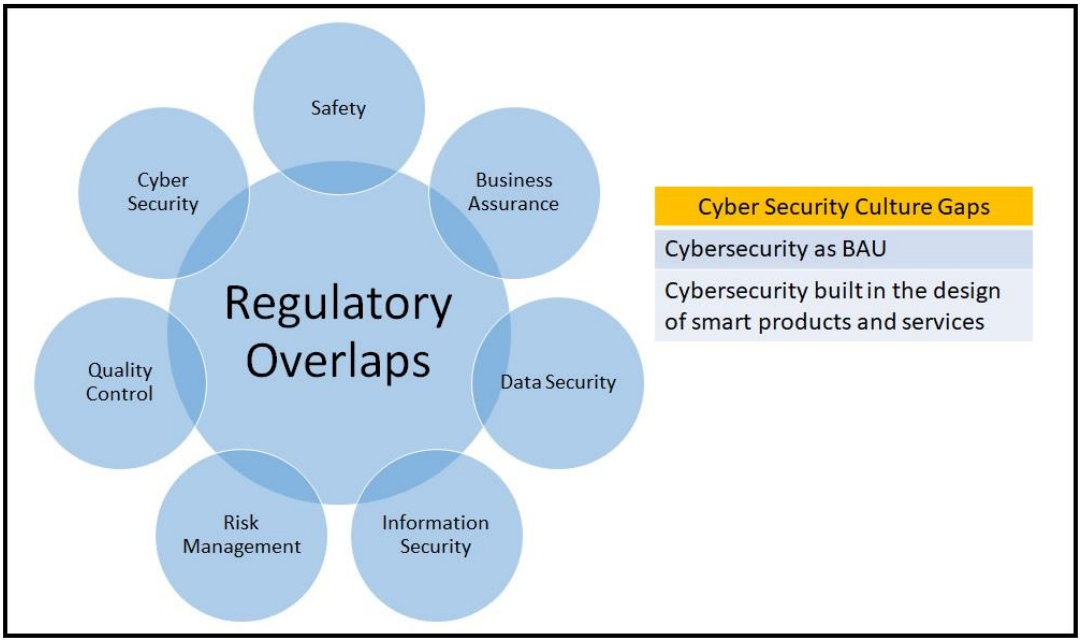
Recommendation 8: Smart city initiatives and CAF IGP to include cyber security as business-as-usual (BAU) approach within engineering lifecycle (including design) of products and services.

As seen in the analysis in sections 5.2, there needs to be a cultural shift to understand that cyber security is a part of every employee's BAU task rather than the IT manager's responsibility. Cyber security by design and holistic security governance discussed in point 1 'NIS Organization and Governance' of this section, will addresses this issue.

Concerns on penalties across multiple regulations for the same breach across NIS and GDPR stems from overlapping regulations. Multiple overlapping controls spanning across quality control, risk and business assurance practices also bring in audit inefficiencies.

Figure 10 summarizes these gaps.

Figure 10: Cyber Security Culture Gaps



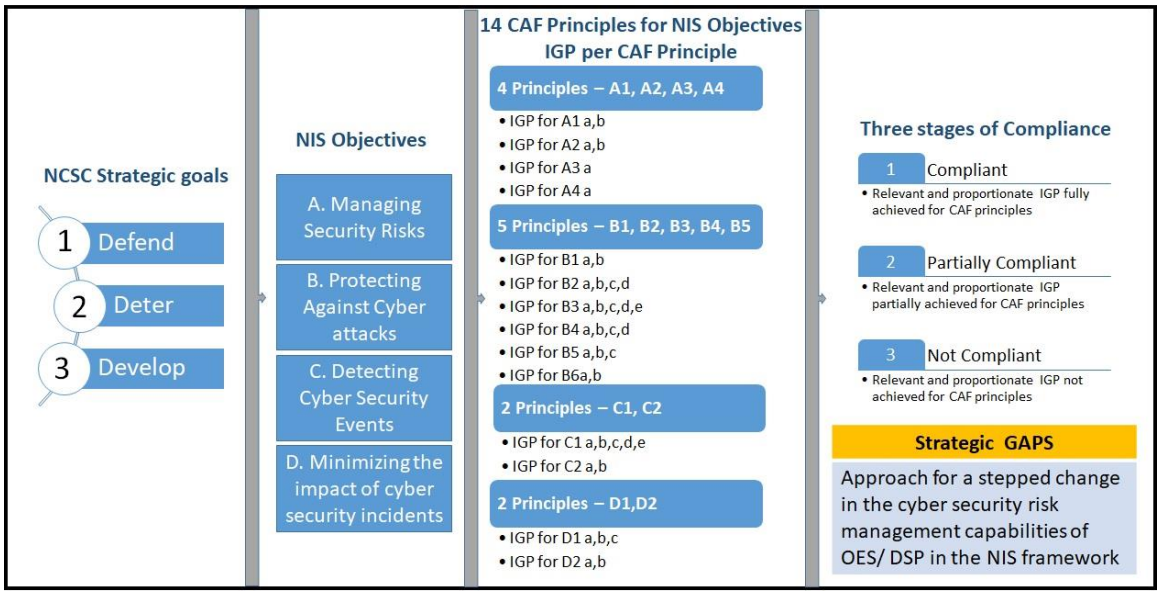
Integration of cyber security and holistic security principles into safety, quality, risk management and business assurance frameworks can result in a BAU approach towards cyber-security. CPNI has published integrated core principles of safety, security and quality using Plan-Do-Check-Act (PDCA), an iterative four-step continuous improvement method (CPNI, 2018). Annex-SL is an initiative from BSI which aims to rationalize ISO quality frameworks, and, looks at a core set of generic requirements for quality to avoid duplication of requirements across the ISO frameworks (BSI, 2015).

Recommendation 9: ***Holistic security frameworks to be mapped and integrated with safety, quality, risk management and business assurance frameworks.***

Key principles can be borrowed from Annex-SL to implement this recommendation.

6. **Strategic Goals:** The key strategic objective of NIS regulation is to bring a step change in the cyber security risk management capabilities of the OES and DSP organizations to improve the resilience of CNI services. The current CAF framework structure described in Figure 11 below and analyzed in sections 4 and 5.1, indicate that currently there is no clarity as to how the NIS framework intends to achieve these objectives considering the OES/DSP are at different levels of capability maturity as analyzed in Section 4.

Figure 11: NIS Strategic goals



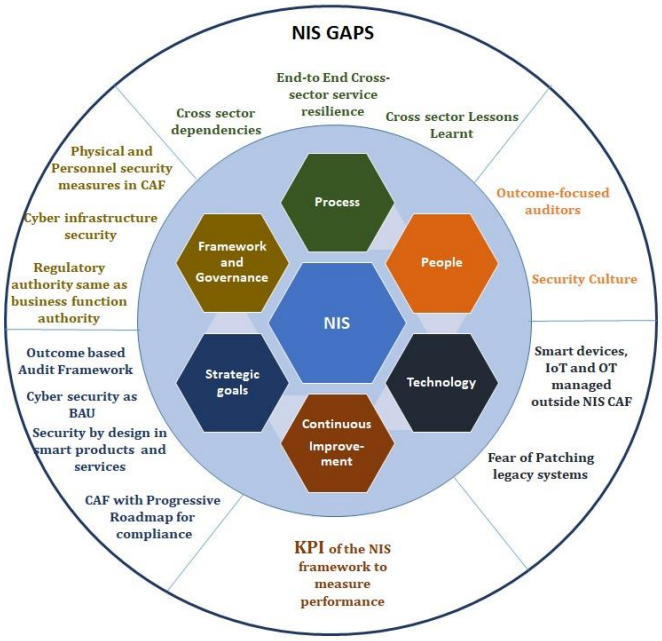
The NCSC is already working out the business processes that underpin the services in the CNI sectors to understand the critical systems and networks (NCSC, 2017). Mapped to the criticality of systems in a service, the NCSC needs to define multiple progressive levels of IGP corresponding to the 14 NIS principles. CAs need to work with OES and DSP to define consistent target levels of IGP for all CNI service components, specifically for common components within cross-sector services. The current self-assessed IGP, and target IGP for the systems will determine the progressive action plan for the OES/DSP at different levels of maturity.

Recommendation 10: Create multiple levels of CAF IGP. Define target IGP for service components. Create a progressive roadmap for OES/DSP to achieve the adequate level of IGP per service component.

It is important for the NCSC CAF to address the above recommendation at CAF framework level to not only ensure consistent levels of cyber security of a CNI service across sectors proportionate to the risks, but also bring a step-change in the OES and DSP capabilities. It is noteworthy that a similar approach has worked in the NIS framework which provides four tiers of implementation based on risk management practices of an organization (NIST, 2018). The organization defines current as well as target risk profile that maps to the appropriate implementation tier relevant to the organization's risk requirements (NIST, 2018).

The gaps and recommendations are summarized in the Figure 12 below.

Figure 12: Summary of NIS Gaps and Researcher's Recommendations



Sl	Ten Recommendations to Improve the Effectiveness of the NIS framework in UK
1	Holistic NCSC CAF and NIS governance (across cyber, physical and personnel security)
2	Outcome-based NIS audit framework oversight and governance
3	NIS Audits to assess effectiveness of key controls of top business and service assurance risks with an outcome-based approach
4	NCSC CAF to include Cross-sector End-to-End holistic service resilience CA forums to share cross-sector lessons learnt with the industry
5	Setup cross-disciplinary outcome based audit teams from various business functions
6	Include IoT, OT, smart products and smart services in NCSC CAF
7	Define KPIs by May 2019 to gather data and manage NIS performance
8	CAF-IGP and smart city plans to include cyber security-as-BAU approach within the engineering life-cycle (including design)
9	Integrate NIS framework with safety, quality, risk management and business assurance frameworks
10	Create multiple levels of CAF outcomes and target capability roadmap for OES/DSP

To summarize, the NIS legislation puts the maintenance of sound risk management and cyber-resilience control systems at the center of security governance. The noteworthy benefit is that it provides a method to deal with the evolving nature of cyber security risk mitigations without continuous amendments to the legislation, and therefore, is scalable and sustainable. With organizations that intend to follow the Smart London Together Roadmap co-existing with NIS compliant organizations, it is important to identify critical infrastructure of Smart London within the London Resilience arrangements and protect it in the same manner as the CNI. NIS can also provide a good benchmark for developing the smart city cyber security plans in London.

Similar to the approach followed by the USA, where the NIST framework has been extended to small businesses (Barth, 2018), NIS principles can be adopted by the other non-CNI organizations in UK. Organizations in a smart city such as London can also benefit from public-private data sharing through safe platforms such as those provided by NCSC. With the development of smart interconnected global products, shared services and shared data, it is important to integrate the standards and frameworks for cyber risk management globally. NIS CAF makes references to the NIST framework ("Table view of principles and related guidance," 2018a), which in turn claims to "serve as a model for international cooperation to strengthen cybersecurity" (NIST, 2018). If the

NIST and EU frameworks are integrated, that could be a starting point for a global standardized framework for holistic security and risk management.

7. Conclusion

The aim of this research was to explore how cyber risks are managed in UK's CNI sectors under NIS. The objectives were 1) to analyze the gaps in EU's NIS framework implemented in the UK, 2) to study the effectiveness of NIS legislation approach that supports the cyber-risk management maturity of OES/DSP, and 3) to study how NIS affects the development of the Smart London cyber security strategy. The research provided ten recommendations to address the NIS framework gaps, which include holistic security governance under NIS, an outcome-based audit approach, and a progressive roadmap to improve the cyber-capabilities of the OES and DSP. Cyber security is ultimately an arms race and we need to strengthen the defences with a flexible approach that allows learning and improving outcomes. The research also served as a discovery process for Smart London Together approach to cyber security and cyber security of non-CNI organizations as intended.

This research is a snapshot in time and limited in scope covering the deployment of the NIS in May 2018, and the subsequent months. Hence, it may not have captured the far-reaching impacts of the evolving NIS enforcement. The research has focused on the cyber security aspects influencing the NIS framework, to the exclusion of evolving individual cyber risks and its impact on the risk management framework. Further research is recommended to obtain better insights and supporting empirical evidence in relation to:

- UK NIS enforcement compared with other EU countries
- Integration points for cyber security frameworks between UK and other leading countries
- Cyber security strategies of other smart cities in UK or the world compared to London

The NIS legislation is the beginning of the journey into the reduction of cyber risks and the application of security measures that are proportional to the threat. However, regulation only reduces the risk of successful cyber-attacks, it cannot eliminate the risk altogether, a balance therefore needs to be maintained between security and compliance. The success of the NIS implementation depends on implementing the security measures to meet the intent of NIS regulation, which is to minimize risks on UK's CNI services, deter cyber security attacks and recover quickly from any service disruptions. This will provide the approach required to realize the UK's strategic vision "to be secure and resilient to cyber threats by 2021".

Bibliography

Ackermann, N. (2018). Smart city background stock photo. Image of digital - 89539472. Retrieved August 22, 2018, from https://www.dreamstime.com/stock-photo-smart-city-background-various-icons-image89539472

Bada, M., Ms, M. G., Ignatuschtschenko, E., Lara, M., Ms, P., Pijnenburg, L., … Upton, D. (2016). About the Global Cybersecurity Capacity Centre Lead Editor and Author Contact details. Retrieved from www.oxfordmartin.ox.ac.uk

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., … Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13. https://doi.org/10.1016/J.DIIN.2017.06.015

Barth, B. (2018, August). President signs NIST Small Business Cybersecurity Act into law. *SC Media*. Retrieved from https://www.scmagazine.com/president-signs-nist-small-business-cybersecurity-act-into-law/article/789147/?utm_source=newslehttps://www.scmagazine.com/president-signs-nist-small-business-cybersecurity-act-into-law/article/789147/?utm_source=newsletter&utm_

BEIS. (2018). *SECURITY OF NIS REGULATION*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

BoE. (2016). *CBEST Intelligence-Led Testing CBEST Implementation Guide*. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf?la=en&hash=1BFF85C8F9E6C0E8BE478BB22B422EDDA5E00DC0

BSI. (2014). *Smart cities-Vocabulary BSI Standards Publication Bio-based products-PAS 600:2013 Part 0: Subtitle BSI Standards Publication*. Retrieved from https://shop.bsigroup.com/upload/283870/PAS-180.pdf

BSI. (2015). *ISO Revisions Introducing Annex SL Whitepaper ISO Revisions*. Retrieved from https://www.bsigroup.com/LocalFiles/nl-nl/iso-9001/BSI-Annex-SL-Whitepaper.pdf

BSI. (2017). *Smart cities-Guide to establishing a decision-making framework for sharing data and information services BSI Standards Publication*. Retrieved from http://shop.bsigroup.com/upload/279894/PAS_183_(2017).pdf

CAA. (2017). *CAP 1574, Version 1.0*. *CAA*. Retrieved from http://publicapps.caa.co.uk/docs/33/26 security controls for regulation_V4.pdf

Cabinet Office. (2017). National Risk Register Of Civil Emergencies. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

Cabinet Office. (2017a). Public Summary of Sector Security and Resilience Plans. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

Cerrudo, C., Hasbini, M. A., Russell, B., Cracciolo, C., Fedon, G., Figuigui, A., … Tiwari, A. (2016). *Cyber Security Guidelines for Smart City Technology Adoption*. Retrieved from https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

Chapman, E. (2018). *The Internet of Insecure Things*. Retrieved from https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-03/Internet of insecure things.pdf?HjRoCgRu0txun_nKD3vtIe10PT8ISF3F

Chartered Institute of Internal Auditors. (2018). Financial services code. Retrieved August 6, 2018, from https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/?downloadPdf=true

CPNI. (2015). Security for ICS - Framework Overview. Retrieved July 31, 2018, from https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS - Framework Overview Final v1 1.pdf

CPNI. (2018). *PROTECTIVE SECURITY MANAGEMENT SYSTEMS (PSEMS) CHECKLIST*. Retrieved from https://www.cpni.gov.uk/system/files/documents/d6/4d/PSeMS_Checklist.pdf
CPNI. (2018a). *Supply chain security collection*. Retrieved from https://www.cpni.gov.uk/system/files/documents/2e/87/Supply_Chain_Security_Collection_Jan2018.pdf
CPNI, B. (2017). PAS 185:2017 Smart Cities - Specification for establishing and implementing a security-minded approach. Retrieved from https://www.cpni.gov.uk/system/files/documents/4e/b0/PAS_185_2017_Introduction_Smart_Cities.pdf
CQC Inspection Framework. (2018). Retrieved from https://www.cqc.org.uk/sites/default/files/20180130_9001100_well-led_Trust-wide_inspection_framework_NP_v4.pdf
Critical National Infrastructure | CPNI | Public Website. (2018). Retrieved February 1, 2018, from https://www.cpni.gov.uk/critical-national-infrastructure-0
Cyber and data security good practice guides - NHS Digital. (2018). Retrieved July 31, 2018, from https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/cyber-guides-and-policies/cyber-and-data-security-good-practice-guides
Data Security and Protection Toolkit - NHS Digital. (2017). Retrieved July 31, 2018, from https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit
DCMS. (2016). *Cyber Security Regulation and Incentives Review*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf
DCMS. (2017). UK Finance response to Department for Digital, Culture, Media and Sport consultation on the implementation of the NIS Directive. Retrieved from https://www.ukfinance.org.uk/wp-content/uploads/2017/09/UK-Finance-Response-to-DCMS-Consultation-NIS-Directive-v03.pdf
DCMS. (2018). *Security of Network and Information Systems, Analysis of responses to public consultation*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677066/NIS_Consultation_Response_-_Analysis_of_Responses.pdf
DCMS. (2018b). *Security of Network and Information Systems Guidance for Competent Authorities*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf
DCMS. (2018c). *The Network and Information Systems Regulation 2018*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf
DCMS. (2018a). Security of Network and Information Systems Department for Digital, Culture, Media and Sport. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf
Defra. (2017). *Water Sector Cyber Security Strategy*. Retrieved from www.nationalarchives.gov.uk/doc/open-government-licence/version/3/
Department of Homeland Security. (2015). *The Cybersecurity Act of 2015*. Retrieved from www.sullcrom.com
DfT. (2016). Rail Cyber Security. Retrieved from https://forms.dft.gov.uk
DfT. (2018). *Implementation of the NIS Directive Moving Britain Ahead*. Retrieved from www.gov.uk/dft
DoH. (2018). *Title: The Network and Information Systems Regulations 2018: Guide for the health sector in England*. Retrieved from www.nationalarchives.gov.uk/doc/open-government-licence/
EECSP. (2017). *EECSP Report: Cyber Security in the Energy Sector*. Retrieved from

https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
Emergency Preparedness, Resilience and Response (EPRR). (2017). Retrieved July 8, 2018, from https://www.england.nhs.uk/ourwork/eprr/
ENISA. (2017). NIS Directive. Retrieved July 11, 2018, from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive
European Commission. (2015). *Public Private Partnership on CYBERSECURITY* (Vol. 11). Retrieved from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf
European Commission. (2018). Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity | Digital Single Market. Retrieved July 26, 2018, from https://ec.europa.eu/digital-single-market/en/news/commission-asks-member-states-transpose-national-laws-eu-wide-legislation-cybersecurity
European Parliament. (2016). Directives. Retrieved May 7, 2018, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
GLA. (2018). *Smarter London Together*. Retrieved from https://www.london.gov.uk/sites/default/files/smarter_london_together_v1.64_-_published.pdf
H.M.Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
H.M.Government. (2018). *EXPLANATORY MEMORANDUM TO THE NIS REGULATIONS 2018, No 506*. Retrieved from http://www.legislation.gov.uk/uksi/2018/506/pdfs/uksiem_20180506_en.pdf
H.M.Government. (2018a). National Security Capability Review – March 2018. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf
H.M.Treasury. (2016). *G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/559186/G7_Fundamental_Elements_Oct_2016.pdf
House, S. (2018). William Smart , Chief Information Officer for Health and Social Care Lessons learned review of the WannaCry Ransomware Cyber Attack. Retrieved from www.nationalarchives.gov.uk/doc/open-government-licence/
House of Commons. (2018). *Cyber-attack on the NHS Thirty-Second Report of Session 2017-19*. Retrieved from www.parliament.uk.
Implementation of the NIS Directive in Germany | Digital Single Market. (2018). Retrieved August 1, 2018, from https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-germany
Implementation of the NIS Directive in the UK | Digital Single Market. (2018). Retrieved June 26, 2018, from https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-uk
Introduction to the NIS Directive. (2018). Retrieved August 1, 2018, from https://www.ncsc.gov.uk/guidance/introduction-nis-directive
IT Governance. (2018). NIS Regulations Compliance Framework and Solutions. Retrieved August 19, 2018, from https://www.itgovernance.co.uk/nis-regulations-compliance-solutions?utm_source=Email&utm_medium=Autoresponder&utm_campaign=T1-GP-EU-NIS-UK&utm_content=EM4
James Black. (2018). Self Driving Cars “Game Changing” for FBI...& ISIS. Retrieved April 15, 2018, from https://www.thecipherbrief.com/article/exclusive/international/self-driving-cars-game-changing-fbi-isis
London Resilience Forum. (2013). London Resilience Partnership Strategy. Retrieved from https://www.london.gov.uk/sites/default/files/london_resilience_partnership_strategy_2016.pdf
London Resilience Partnership. (2013). Retrieved from

https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/London Resilience Partnership Strategy v1 web version.pdf
London Resilience Partnership. (2017). London Risk Register. Retrieved from www.londonprepared.gov.uk
Maglaras, L., Drivas, G., Noou, K., & Rallis, S. (2018). NIS directive: The case of Greece. https://doi.org/10.4108/eai.15-5-2018.154769
Martin, Guy, Martin Paul, Hankin Chris, Darzi Ara, K. J. (2017). Cybersecurity and healthcare: how safe are we? *theBMJ*, *358:j3179*, 4. https://doi.org/10.1136/bmj.j3179
Martin, R. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552
Medical devices: EU regulations for MDR and IVDR - GOV.UK. (2018). Retrieved July 2, 2018, from https://www.gov.uk/guidance/medical-devices-eu-regulations-for-mdr-and-ivdr
Microsoft. (2018). *Risk Management for Cybersecurity: Security Baselines Risk Management for Cybersecurity*. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/MS-riskmanagement-securitybaselines-WEB.pdf
NCSC. (2017). *Introduction*. *NCSC Annual Review*. Retrieved from https://www.ncsc.gov.uk/content/files/NCSC-2017-Annual-Review.pdf
NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018
OfCom. (2018). *GUIDANCE Ofcom's interim guidance for Operators of Essential Services in the digital infrastructure subsector under the Network and Information Systems Regulations 2018*. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0017/113750/Interim-guidance-for-OES-in-the-digital-infrastructure-subsector-under-the-NIS-Regulations.pdf
Oral evidence - Cyber Security: Critical National Infrastructure. (2018). Retrieved July 31, 2018, from http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/oral/81998.html
Parliament Select Committee-June. (2018). *Evidence Session No. 4 Heard in Public Questions*. Retrieved from http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/oral/86108.pdf
Quigley, K., & Roy, J. (2012). Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America. *Social Science Computer Review*, *DOI: 10.11*(30(1)), 83–94. https://doi.org/10.1177/0894439310392197
Rao, A., Carreon, N., Lysecky, R., & Rozenblit, J. (2018). Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. *IEEE Software*, *35*(1), 38–43. https://doi.org/10.1109/MS.2017.4541031
Regulating Cyber: the UK's plans for the NIS Directive. (2017). Retrieved from https://www.slaughterandmay.com/media/2536536/regulating-cyber-the-uks-plans-for-the-nis-directive.pdf
Ruffle Simon, Daffron Jeniffer, Copic Jeniffer, Leverett Éireann, Evan Tamara, R. D. (2017, December 14). Cyber Security: Critical National Infrastructure Inquiry. https://doi.org/10.1186/s13174-017-0059-y
Secure by Design. (2017). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
Security for Industrial Control Systems. (2018). Retrieved August 17, 2018, from https://www.ncsc.gov.uk/guidance/security-industrial-control-systems
Smith, F., & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642–660. https://doi.org/10.1080/10357718.2017.1320972org/10.1080/10357718.2017.1320972

Štitilis, D., Pakutinskas, P., & Malinauskait\.e, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, *30*(4), 1151–1168. https://doi.org/10.1057/s41284-016-0083-9

Table view of principles and related guidance. (2018a). Retrieved June 28, 2018, from https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance

Table view of principles and related guidance. (2018b). Retrieved July 31, 2018, from https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance

The Guide to NIS. (n.d.). Retrieved July 31, 2018, from https://ico.org.uk/for-organisations/the-guide-to-nis/

The Key Principles of Cyber Security for CAV. (2017). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf

The Network and Information Systems Regulations 2018. (2018). https://doi.org/No 506

The NIS Guidance Collection. (2018). Retrieved July 31, 2018, from https://www.ncsc.gov.uk/guidance/nis-guidance-collection

UK Legislation. (2018). The Network and Information Systems Regulations 2018. Retrieved August 1, 2018, from http://www.legislation.gov.uk/uksi/2018/506/regulation/1

UKRN. (2015). *Cross-sector Resilience – Phase 1 report*. Retrieved from http://www.ukrn.org.uk/wp-content/uploads/2016/07/2015AprCSR-Phase1Report.pdf

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, *34*(3), 450–466. https://doi.org/10.1016/J.CLSR.2017.12.004

VIIRA, T. (2018). INTERDEPENDENCIES OF SERVICES. In *Lessons Learned: Critical Information Infrastructure Protection* (pp. 24–27). IT Governance Publishing. https://doi.org/10.2307/j.ctt1xhr7hq.10

Walker-Osborn, C., & Patel, N. (2014). EU Cybersecurity Directive. *ITNOW*, *56*(2), 38–39. https://doi.org/10.1093/itnow/bwu048

Welcome to GCHQ. (2017). Retrieved August 1, 2018, from https://www.gchq.gov.uk/

Appendices

Appendix A –Questionnaire for DCMS and CPNI Stakeholders

Sl	Category	Questions for NIS compliance and cyber security Assessment Framework analysis
1	NIS Framework	What is the approach for NIS in UK? What is the mechanism to ensure that the NIS framework is assessed and enforced effectively? How will it contribute to imprvement of the cyber security maturity across sectors?
2		How do you assess that the CAF list of outcomes and IGPs is complete? Are there any gaps? How do you assess that the Cas have the right level of competence within their organisations to enforce NIS directive?
3	Sector / OES CSF	Do you have a current capability metrics across operators of essential services for sectors where NIS directive has been applied? Do you have data for risk management capabilities across sectors?
4	NIS compliance	Do you have any advance view of organisations who will not be able to meet appropriate levels of NIS specified security requirements in the first year and resulting impacts?
5	Governance	What controls will you be putting in place to govern how Competent authorities of the sectors manage Operators of Essential services to comply with NIS directive
6	Cross sector	Are cross sector dependency guidelines available for NIS compliance?
7	Ongoing Framework update	Do you assess your framework and guidelines regularly in light of dynamic innovations across sectors to ensure that the checklist and indicators in CSF are fit for purpose?
8	Emergency Response	Is emergency response plan and governance joined up for physical and cyber security considering London has a different Resilience team within GLA?

Appendix B – Questionnaire for Stakeholders from Competent Authorities

Sl	Category	Questions for NIS compliance and cyber security Assessment Framework analysis
1	Guidance	Do you have sector-specific guidance in place for organisations to implement cyber security to meet the four objectives and 14 principles published by NCSC under NIS directive ?
2		Is published sector-specific guidance available for supply chain cyber security in sync with NCSC supply chain guidelines?
3		Do you have any published sector-specific incident thresholds for reportable incidents (how to report, what incidents to report) and Incident Report Assessment guideline (Triage system to classify incidents in terms of importance for investigation) for NIS incident reporting compliance?
4	NIS Assessment	Have you done any initial self-assessment to understand the cyber security issues / vulnerabilities / risks within the organisation or sector?
5		Do you have a self-assessment checklist against NCSC Capability assessment framework to evaluate NIS compliance? (When planned?)
6		Have you analysed NIS compliance for your organisation or within organisations of your sector ?
7		Do you understand the areas/organisations that will not be able to meet appropriate levels of NIS specified security requirements in the first year"? (please mention which ones in the comment section)
8	Enforcement	Do you have a framework/process/regulation in place to assess, assure and enforce NIS directive compliance(such as audits or inspections)?
9		Do you have cyber risk management maturity assessment for your sector currently ?
10	Cross sector	Do you have a process for resolving cross sector dependencies?
11	Emergency Response	Is emergency response plan and governance defined for your sector's recovery from high impact cyber incidents which may overlap with physical incidents?

Appendix C –Questionnaire for Stakeholders from Operator of Essential services

Sl	Category	Questions for NIS compliance and cyber security Assessment Framework analysis
1	Guidance	Do you now of sector-specific or organisational guidance to implement cyber security to meet the four objectives published by NCSC under NIS directive ?
2		Is there any sector-specific or organisational guidance available for supply chain cyber security to meet NIS requirements ?
3		Do you have any incident thresholds for reportable incidents (how to report, what incidents to report) and Incident Report Assessment guideline (Triage system to classify incidents in terms of importance for investigation) for NIS incident reporting compliance?
4	NIS Assessment	Do you take up ongoing self-assessment to understand the cyber security issues / vulnerabilities / risks within your organisation?
5		Have you analysed NIS compliance for your organisation using any self-assessment tool or otherwise?
6		Do you understand the areas/organisations that will not be able to meet appropriate levels of NIS specified security requirements in the first year"? (please mention which ones in the comment section)
7	Enforcement	Do you have a plan/process in place to continuously assess NIS compliance and the risk assessment process in your organisation (such as audits or inspections)?
8		Do you have cyber risk management maturity assessment available for your organisation currently ?
9	Emergency Response	Is emergency response plan and governance defined for recovery from high impact cyber incidents which may overlap with physical incidents?

Appendix D – List of Stakeholders

Sl	Stakeholders	Referred as
1	Isabel Bonachera Martin, EU Cyber Security Regulatory Policy, Department for Digital, Culture, Media and Sports (DCMS)	DCMS-S1
2	Department of Health and Social Care (DHSC)	DHSC-S1, DHSC-S2
3	Theo Blackwell, Chief Digital Officer of London, GLA	GLA-S1
4	Department of Transport (DfT)	DfT-S1, DfT-S2
5	Simon Onyons, Finance Conduct Authority(FCA)	FCA-S1
6	Nick Davey, Payment System Regulator (PSR)	PSR-S1
7	Centre for Protection of National Infrastructure (CPNI)	CPNI-S1
8	The Office of Gas and Electricity Markets (OfGem)	OfGem-S1
9	National Health Service (NHS) England	NHSE-S1
10	Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Deutschland	GF-S1
11	David Tait, Civil Aviation authority (CAA)	CAA-S1
12	Nick Swanson, City Hall, GLA	GLA-S2
13	London Fire Brigade	LFB-S1, LFB-S2
14	London Metropolitan Police	LMP-S1
15	Steve Burton, Transport for London (TfL)	TfL-S1
16	Johnny Schute, James Walker, Ian Maxwell Office of Rail and Road (ORR)	ORR-S1, ORR-S2, ORR-S3
17	Hitachi Vantara	HV-S1
18	Toby Gould, London Resilience Group	LRG-S1
19	Graham Lane, City Hall, GLA	GLA-S3
20	Imperial College Healthcare	NHST-S1
21	North West London NHS Foundation Trust - CNWL	NHST-S2
22	NHS Digital	NHSD-S1
23	British Standards Institute (BSI)	BSI-S1
24	Network Rail	
25	Defra, Drinking Water Inspectorate(DWI)	
26	Business, Energy and Industrial Strategy (BEIS)	
27	Office of Communications (OfCom)	
28	Bank of England(BoE)	
29	Information Commissioner's office (ICO)	
30	Highways England	

*Stakeholders names have been included only where stakeholder's permission was given to do so.

Appendix E – Data Protection and Security Toolkit

The security standards in the Data Protection and Security Toolkit (DSPT) v5.1 provided by the DHSC are as follows:

Data Security Standard 1

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.

Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained in the relevant pieces of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal confidential data.

Data Security Standard 2

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

Data Security Standard 3

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

All staff complete an annual security module, linked to 'CareCERT Assurance'. The course is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Data Security Standard 4

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc).

Data Security Standard 5

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data

security.

Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.

Data Security Standard 6

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. [The Board] understands that it is ultimately accountable for the impact of security incidents, and bear the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Data Security Standard 7

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

A business continuity exercise is run every year as a minimum, with guidance and templates available from [CareCERT Assurance]. Those in key roles will receive dedicated training so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

Guidance and support is available from CareCERT Assurance to ensure risk owners understand how to prioritise their vulnerabilities. There is a clear recognition that not all unsupported systems can be upgraded and that financial and other constraints should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It’s about demonstrating that analysis has been done and informed decisions were made.

Data Security Standard 9

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

[CareCERT Assurance] assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes. There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Data Security Standard 10

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

Appendix F – The Competent Authorities within the NIS legislation

The Competent Authorities of various sectors in England and the criteria for OES under the NIS regulation have been summarized below. These have been articulated based on the information within the DCMS documents (DCMS, 2018d), (DCMS, 2018c).

Table 1: Sectors and Competent Authorities in England under NIS legislation

Sector	Sub-sector	Competent Authority in England	Essential Services	Relevant Entities
Drinking water supply and distribution	N/A	The Secretary of State (Department) for Environment, Food and Rural Affairs - Defra	The supply of potable water to households Entities involved in the wholesale supply of potable water	
Energy	Electricity	The Secretary of State for Business, Energy and Industrial Strategy(BEIS) and the Office of Gas and Electricity Markets (Ofgem). (Joint Competent Authorities)	Electricity supply Electricity distribution Electricity transmission	Electricity supply businesses, distribution and transmission companies
	Gas	For natural gas undertakings that carry out the function of production, operators of natural gas refining and treatment facilities, storage system operators and LNG system operators, the Secretary of State for Business, Energy and Industrial Strategy (BEIS). Otherwise, the Secretary of State for Business, Energy and Industrial Strategy and the Gas and Electricity Markets Authority (GEMA), acting jointly	Gas supply	Gas supply businesses, distribution and transmission companies, storage and LNG operators, and operators of refining and treatment facilities
	Oil	The Secretary of State for Business, Energy and Industrial Strategy (BEIS)	Oil transmission Oil production, refining and treatment and storage	Oil pipeline (transmission), production, refining and treatment and storage businesses
Digital Infrastructure	N/A	The Office of Communications (Ofcom)	Provision of internet infrastructure service	Internet exchange points (IXPs) Domain name service providers (DNS) Top level
Health sector	Health care settings	In England, the Secretary of State for Health. (Department of Health and Care - DOH)	Non-primary NHS healthcare services	NHS Trusts and Foundation Trusts
Transport	Air Transport	The Secretary of State for Transport and the Civil Aviation Authority (CAA)	Passenger air transport Cargo air transport	Airport managing bodies Traffic management control operators Air carriers
	Maritime	The Secretary of State (Department) for Transport (DfT)	Passenger transport Cargo transport	Managing bodies of ports Passenger water transport companies Cargo water transport companies Operators of vessel traffic
	Road			
	Rail		Heaver rail passenger services (including international rail)	Licensed train operators which provide services on the national rail network under
			Light rail and metro passenger service (including underground)	Light rail operators subject to regulation for security under the railways act 1993
			Road transport	Roads authorities
Digital Service Providers	Cloud Services; online marketplaces; Search engines	The Information Commissioner's Office (ICO)		

Appendix G – Explanation of Terms

ARF - Authorities' Response Framework
BACS - Bankers' Automated Clearing Services
BAU – Business-as-usual
BoE – Bank of England
BEIS - Business, Energy and Industrial Strategy
BRE - Building Research Establishment
BSI - British Standards Institute
CA – Competent Authority
CAA - Civil Aviation Authority
CAF – Capability Assessment Framework
CAP - Civil Aviation Publication
CAV - Connected and Automated Vehicles
CBEST - cyber threat assurance framework
CCT - Cyber Compliance Team
CDO – Chief Digital Officer of London
CEA - Cybersecurity Enhancement Act
CiSP - Cyber-security Information Sharing Partnership
COTS - Commercial Off The Shelf
CNI – Critical National Infrastructure
CNWL - North West London NHS Foundation Trust
CPNI - Centre for Protection of National Infrastructure
CPP - Cyber-Physical-Personnel
CSIRT - Computer Security Incident Response Team
CQC - Care Quality Commission
DCMS – Department for Digital, Culture, Media and Support
Defra - Department for Environment, Food and Rural Affairs
DfT - Department of Transport
DHSC – Department of Health
DSP – Digital Service Providers
DSPT - Data Protection and Securtiy Toolkit
DWI - Drinking Water Inspectorate
ECTA - European Train Control System
ENISA - European Network and Information Systems Agency
ERTS - European Rail Traffic Management System
EU – European Union
FCA - Finance Conduct Authority
GCHQ - Government Communications Headquarters
GDPR - General Data Protection Regulation
GLA – Greater London Authority
HAZOP - Hazard and Operability
HMT – HM Treasury
HSE - Health and Safety
ICO - Information Commissioner's Office
ICS – Industrial Control Systems
IGP – Indicators of Good Practice
IoT – Internet of Things
ISO – Institute of Standardization
IT – Information Technology
KPI - Key Performance Indicators
KY3P - Know your third party
NATO - North Atlantic Treaty Organization
NCSC – National Cyber Security Centre

NHS - National Health Service
NII - National Information Infrastructure
NIS – Networks and Information Security
NIST - National Institute of Standards and Technology
OES – Operators of Essential Services
OfCom –Office of Communications
OfGem - Office of Gas and Electricity Markets
OfWat – Office of water services
ORR – Office of Rail and Road
OT – Operational Technology
PAC - Public Accounts Committee
PRA – Prudential Regulation Authority
PAS - Publicly Available Specification
PDCA – Plan-Do-Check-Act
PHE - Public Health England
RM^3 - Risk management maturity model
SCADA - Supervisory Control and Data Acquisition
TBEST - Transit Boardings Estimation and Simulation Tool
TfL – Transport for London
TRL - Transport Research Lab
UCL – University College London
UKRN - UK Regulators Network
VMS - Virtual Memory Systems

List of Figures

Icons in Figures:

1) Figure 5 Reference to the NIS Regulations Compliance icon (IT Governance, 2018)
2) Figure 8 Reference to the Smart City icon (Ackermann, 2018)

List of Tables

Short non-Technical Document_WC_1000

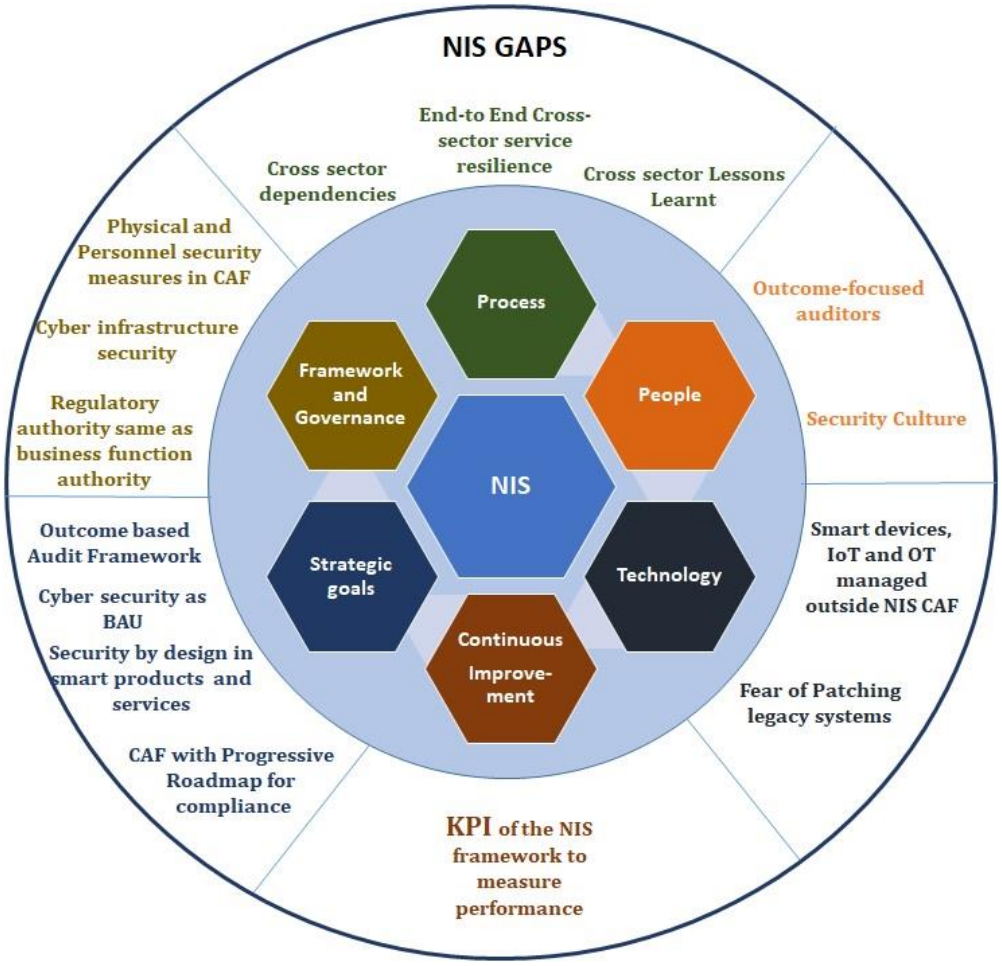
Cyber Risk management of UK's Critical National Infrastructure under the NIS Legislation

With the development of offensive capabilities in the cyber arms race, increasing attacks on Critical National Infrastructure (CNI) are a fact in today's society. The Ukraine power infrastructure cyber-attack in 2016, the German rail cyber-attack in 2017, Wannacry ransomware in the UK hospitals in 2017 and the Atlanta water supply disruption in 2018 have demonstrated today's cyber-physical threats. In response, the European Union (EU) proposed the Networks and Information Security (NIS) directive, the first cyber security legislation to improve the CNI service resilience. The NIS, a part of the National Cyber Security Center (NCSC) strategy 2016-2021, was implemented in the UK on 9th May 2018 and is expected to mature in the first year.

The research reported here, explored how the Operators of Essential Services (OES) and the DSPs as mandated by the NIS legislation manage cyber security risks in the UK's CNI sectors (water, transport, energy, health, digital infrastructure and Digital Service Providers (DSPs)). The research indicated that NIS follows a collaborative approach to improve the cyber-risk management capabilities in the CNI sectors. However, more work needs to be done for NIS to address the integrated national security across cyber and non-cyber elements and to strengthen end-to-end resilience of the CNI services.

Study of NIS Framework

The first objective of the research was to review whether there were any gaps in the NIS framework. The researcher analyzed the data gathered by interviewing professionals from 30 organizations within the CNI sectors and identified fourteen gaps, which if not addressed, may limit the objective of implementing appropriate and proportionate security measures for reliability and security of essential services.



Four key gap areas are discussed below:

1. **Holistic security Measures:** There is awareness that the NCSC CAF does not provide non-cyber measures for the CNI services. The researcher recommended an early integration of cyber, physical and personnel national security governance under NIS as cyber-risks cannot be mitigated in isolation.
2. **Implementation approach for outcome-based assessments:** NCSC, the single point of contact for technical expertise under NIS has developed Capability Assessment framework (CAF) for NIS compliance assessment. The CAF is outcome-based, i.e. specifies what needs to be achieved rather than exactly what needs to be done by the OES/DSP and Competent

authorities(CA), also the regulators, to move away from checklist based regulatory approach. The researcher found a risk in the planned mitigation strategies of some of the CA to address the lack of regulatory experience with outcome-based assessments; i.e. the use of Health and Safety (HSE) auditors in the energy sector, and Drinking Water Inspectorate (DWI) auditors in the water sector. The auditors experienced in checklist and tolerance based audits may not have the experience for outcome-based NIS assessments. A case study that compared the Health sector's self-assessment tool with the NIS principles confirmed the above gaps. The researcher recommended:

i) Create a central outcome-based NIS audit framework (an approach that has worked well in the finance sector)

ii) Setup combined audit teams of management, risk, security, quality, audit and assurance professionals

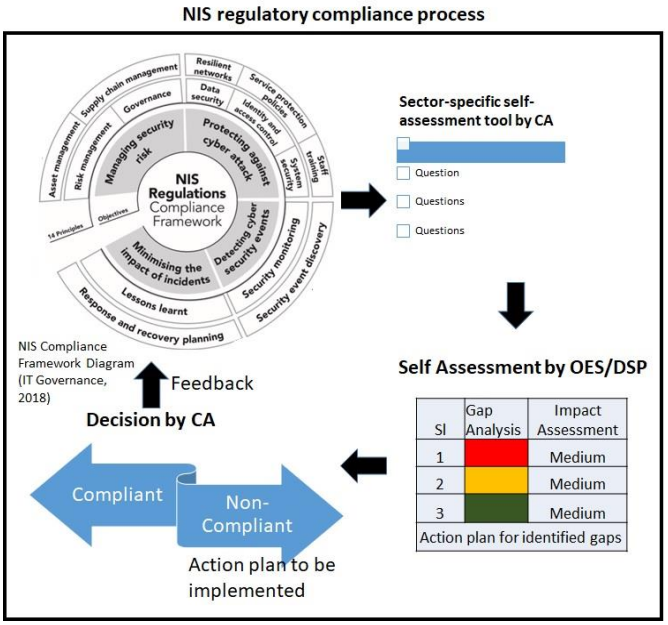
iii) Provide centralized outcome-based audit governance

3. **Cross-sector security measures:** A lack of focused governance of cross-sector dependencies, Emergency response and recovery exercises, and cross-sector lessons learnt can result in end-to-end service vulnerabilities. Common components across critical services are also operated by the supply chain, which amplifies the issue of lack of consistent cyber security framework for supply chain across sectors. The cyber security of the CNI services is as strong as its weakest link and hence, it is recommended that these gaps are bridged.
4. **Risk assessment of smart technologies:** The researcher recommended that controls for smart technologies and Operational Technology (OT) are included in the CAF to reduce cyber-physical threats.

Cyber-risk management capabilities

The second objective was to review the effectiveness of the NIS implementation approach to meet the key strategic objective of upgrading the capabilities of OES and DSP in a progressive manner.

The researcher studied the cyber-capability and NIS regulatory compliance process. The air transport sub-sector was found to be the most mature and possibly has minimal gaps with NIS CAF. DSPs are already working towards Risk Management certification (ISO 27001), which is expected to provide NIS compliance. Health, rail and marine sectors are upgrading their existing security frameworks. Energy, Digital service providers, road sub-sector in transport and water sector are in a formative stage and need to invest the most effort to implement the NIS requirements by May 2019.



As seen in the figure 'NIS compliance process' NIS does not provide multiple levels of compliance based on capability maturity. The researcher recommended providing a progressive roadmap to the OES/DSP that are at various stages of the cyber-security capability maturity, similar to the National Institute of Standards and Technology (NIST) framework of the USA.

Impacts on Smarter London Together planning

The third and final objective of the research was to study the non-CNI organizations within London to understand whether the NIS cyber security approach can be applied to the Smarter London Together plan. The case study found that more focus is required on planned exercises to test resilience to a cyber-attack within London, and a clear need for cyber security as business-as-usual (BAU) by embedding default security by design in smart products and services. A shift in cyber security culture would help avoid the development of smart spaces in silos instead of a comprehensive cross (CNI) sector smart city by design. This research provided the available national framework elements and "pitfalls to avoid" for developing a stronger cyber-security strategy for the CNI and non-CNI sectors within the Smarter London Together plan.

Recommendations: The ten recommendations provided by the researcher are summarized below:

TEN Recommendations to improve the Effectiveness of the NIS framework in UK
1. Holistic Capability Assessment Framework (CAF) and NIS governance (across cyber, physical and personnel security)
2. Outcome-based NIS audit framework oversight and governance
3. NIS Audits to assess effectiveness of key controls of top business and service assurance risks with an outcome-based approach
4. NCSC CAF to include cross-sector End-to-End holistic service resilience Regulatory forums to share cross-sector lessons learnt with the industry
5. Setup cross-disciplinary outcome based audit teams from various business functions
6. Include Internet-of-things (IoT), Operational Technology (OT), smart products and smart services in NCSC CAF
7. Define NIS Key Performance Indicators (KPIs) in the first year of implementation to gather data and manage NIS performance
8. CAF Indicators of Goof Practices(IGP) and smart city plans to include cyber security as Business-As-Usual (BAU) approach within the engineering life-cycle (including design)
9. Integrate NIS framework with safety, quality, risk management and business assurance frameworks
10. Create multiple levels of CAF outcomes and target capability roadmap for Operators of Essential Services(OES) and Digital Service Providers(DSP)

The NIS regulation is in its infancy and provides the first step towards improving the cyber security capabilities of the nation. However, it is noteworthy that although the finance sector is exempt from NIS legislation as equivalent principles are already operational, cyber-attacks within the finance sector continue. So it remains to be seen if the NIS legislation can effectively prevent cyber-physical attacks in the UK.

References for the icons in the cover picture:

(Proliance Automation and Training, 2018), (King & Rucker, 2018), (GROW Learning Company, 2018), (TECHSYS Solutions Pvt.Ltd., 2014), (City of Fort Collins, 2018), (City-Data.com, 2010), (HUGHES, 2017), (Whitelaw, 2015), (Bendor-Samuel, 2018), (City of Albany NY, 2018), (Story Blocks, 2018), (West Virginia American Water, 2018), (Freedom in Creation, 2018), (Ofri Danielle, 2018), (Electronic Product Design and Test, 2017), (IT Governance, 2018)

Bibliography

Bendor-Samuel, P. (2018). https://blogs-images.forbes.com/peterbendorsamuel/files/2018/06/Trends-in-Third-Party-Service-Providers-Transitioning-To-Digital-Services-blog-888477728.jpg (960×720). Retrieved August 29, 2018, from https://thumbor.forbes.com/thumbor/960x0/https%3A%2F%2Fblogs-images.forbes.com%2Fpeterbendorsamuel%2Ffiles%2F2018%2F06%2FTrends-in-Third-Party-Service-Providers-Transitioning-To-Digital-Services-blog-888477728.jpg

City-Data.com. (2010). 3608475365_189200eaa5.jpg (500×375). Retrieved August 29, 2018, from http://farm4.static.flickr.com/3350/3608475365_189200eaa5.jpg

City of Albany NY. (2018). Water_1.sflb.ashx (1308×981). Retrieved August 29, 2018, from https://www.albanyny.gov/Libraries/Water/Water_1.sflb.ashx

City of Fort Collins. (2018). 0.jpg (480×360). Retrieved August 29, 2018, from https://i.ytimg.com/vi/uAexdggpssM/0.jpg

Electronic Product Design and Test. (2017). 135627 (580×280). Retrieved August 29, 2018, from http://www.epdtonthenet.net/global/showimage/Article/135627/

Freedom in Creation. (2018). FIC-Circle-diagram-How-it-Works.jpg (1600×1956). Retrieved August 29, 2018, from https://www.freedomincreation.org/wp-content/uploads/2012/04/FIC-Circle-diagram-How-it-Works.jpg

GROW Learning Company. (2018). Theme - Land Transport - Foundation Phase | Grow Learning Company. Retrieved August 29, 2018, from https://www.grow-it.co.za/products/theme-land-transport-foundation-phase

HUGHES, M. (2017). 34163555514_d24bc780e2_k-796x482.jpg (796×482). Retrieved August 29, 2018, from https://cdn0.tnwcdn.com/wp-content/blogs.dir/1/files/2017/07/34163555514_d24bc780e2_k-796x482.jpg

IT Governance. (2018). NIS Regulations Compliance Framework and Solutions. Retrieved August 19, 2018, from https://www.itgovernance.co.uk/nis-regulations-compliance-solutions?utm_source=Email&utm_medium=Autoresponder&utm_campaign=T1-GP-EU-NIS-

UK&utm_content=EM4

King, A., & Rucker, A. (2018). energy-week-900x600-min.jpg (900×600). Retrieved August 29, 2018, from https://www.cmu.edu/energy/news-multimedia/2018/images/energy-week-900x600-min.jpg

Ofri Danielle. (2018). ICD.jpg (410×357). Retrieved August 29, 2018, from https://danielleofri.com/wp-content/uploads/2013/06/ICD.jpg

Proliance Automation and Training. (2018). renewable-energy-services-logo.jpg (383×268). Retrieved August 22, 2018, from http://www.prolianceautomation.com/upload/content/renewable-energy-services-logo.jpg

Story Blocks. (2018). Weblet Importer. Retrieved August 29, 2018, from https://d2v9y0dukr6mq2.cloudfront.net/video/preview/-Vg6Oxx/growing-global-network-across-the-world-map-internet-and-business-concept-blue-version-4k_htmexueq__SB_PM.mp4

TECHSYS Solutions Pvt.Ltd. (2014). Railway.jpg (600×348). Retrieved August 29, 2018, from https://www.tecsys.in/blog/wp-content/uploads/2014/06/Railway.jpg

West Virginia American Water. (2018). examples of source water contamination.jpg (1257×697). Retrieved August 29, 2018, from https://dnnh3qht4.blob.core.windows.net/portals/15/Water Info/Water Learning Center/Source Water/examples of source water contamination.jpg?sr=b&si=DNNFileManagerPolicy&sig=%2B2i5CX4QlzrskJeDXYyx2zwACu40yVztiMr2IIPgRpM%3D

Whitelaw, J. (2015). Digital Infrastructure Hub front page image.jpg (382×254). Retrieved August 29, 2018, from http://www.infrastructure-intelligence.com/sites/default/files/styles/large__382_x_254_/public/field/image/Digital Infrastructure Hub front page image.jpg?itok=S_fkVqT-