Cyber Security 2019 Conference

Does the NIS implementation strategy effectively address cyber security risks in the UK?

Meha Shukla
Department of Security and Crime Science,
University College London
London, UK
meha.shukla.17@ucl.ac.uk

Shane D. Johnson
Department of Security and Crime Science ,
University College London
London, UK
shane.johnson@ucl.ac.uk

Peter Jones
Department of Civil, Environment and Geomatic Engineering,
University College London
London, UK
peter.jones@ucl.ac.uk

***Abstract*—This research explored how cyber security risks are managed across UK Critical National Infrastructure (CNI) sectors following implementation of the 2018 Networks and Information Security (NIS) legislation. Being in its infancy, there has been limited study into the effectiveness of this national framework for cyber risk management. The analysis of data gathered through interviews with key stakeholders against the NIS objectives indicated a collaborative implementation approach to improve cyber-risk management capabilities in CNI sectors. However, more work is required to bridge the gaps in the NIS framework to ensure holistic security across cyber spaces as well as non-cyber elements: cyber-physical security, cross-sector CNI service security measures, outcome-based regulatory assessments and risks due to connected smart technology implementations alongside legacy systems. This research proposes ten key recommendations to counter the danger of not meeting the NIS key strategic objectives. In particular, it recommends that the approach to NIS implementation needs further alignment with its objectives, such as bringing a step-change in the cyber-security risk management capabilities of the CNI sectors.**

Keywords—NCSC, NIS, OES, DSP, CA, CNI, Cyber security, Cyber Risk management, Network and Information Security Directive

I. 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 [1]. The hardware and software used to monitor and control these smart systems, also known as Operational Technology (OT), connect the physical infrastructure to Information Technology (IT) systems and networks. 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 [2] Cyber-attacks on CNI such as Wannacry attack in 2017 [3] and Ukraine power infrastructure in 2016 [4], has resulted in CNI sectors working harder to strengthen their approaches to cyber risk management [4]. These global cyber security breaches 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 [5]. Cyber security risk management involves understanding the critical business The processes supporting critical services and the underlying components, systems, networks, physical assets and personnel [6].

European Union (EU) has recognized that cyber-incidents can disrupt the essential services of CNI across borders, and the existing capabilities across the EU countries are insufficient individually and collectively for Networks and Information Security (NIS) [7]. In response, the EU launched the NIS Directive on 6 July, 2016 to "improve the EU's preparedness for cyber-attacks" [8], also termed as 'resilience to cyber-attacks'. NIS is the first legislation within EU member states which mandates cyber risk management by the Operators of Essential Services (OES) and Digital Service Providers (DSP) [9]. As required by NIS Directive, the EU member states have nominated at least one national Competent Authority (CA) to monitor the NIS implementation [7].

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 [10]. In UK, NIS was implemented by the OES and DSP across six economic CNI sectors on 9 May, 2018 [9]. The NIS legislation plays a key part in delivering UK's National Cyber Security Strategy 2016-2021 [11] and informs the regulatory framework intended to protect the UK's CNI [12].This is described through the four NIS objectives mapped to the three NCSC cyber security strategic goals - Defend, Deter and Develop [11] as seen in Fig. 1 below. This research, conducted from May 2018 to Sep 2018, explored a timely question: "How are cyber security risks currently managed under the NIS Directive across the UK's CNI sectors?" The objective of the research was to assess:

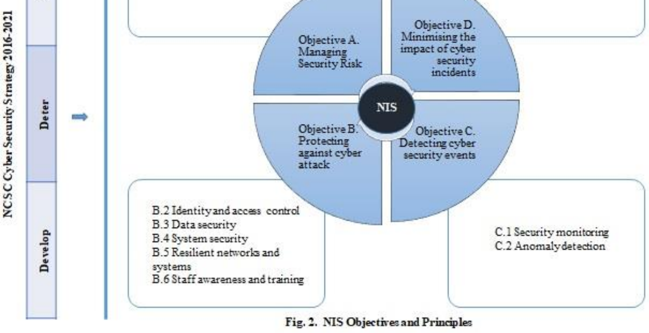

NCSC Cyber Security Strategy 2016-2021
Defend
Deter
Develop
A.1 Governance
A.2 Risk management
A.3 Asset management
A.4 Supply chain
D.1 Response and recovery planning
D.2 Improvements
Objective A. Managing Security Risk
Objective D. Minimising the impact of cyber security incidents
NIS
Objective B. Protecting against cyber attack
Objective C. Detecting cyber security events
B.2 Identity and access control
B.3 Data security
B.4 System security
B.5 Resilient networks and systems
B.6 Staff awareness and training
C.1 Security monitoring
C.2 Anomaly detection

Fig. 2. NIS Objectives and Principles

(1) the current implementation approach of the NIS framework across CNI sectors (water, transport, energy, health, digital infrastructure and DSPs,

(2) the effectiveness of the NIS directive's approach, aimed at bringing a step change in the cyber security risk management across UK's CNI sectors, and

(3) the cyber security processes within the Smart London's non-CNI sectors to examine whether the lessons learnt from national implementation of the NIS can be applied to the security strategy of a major city.

Absent prior research that has examined the effectiveness of cyber-risk management under NIS regulation, this research focused on collecting data through interviews with professionals within the OES and regulatory bodies. A case study was conducted with a sampled CNI sector to analyse the self-assessment process that determined the gaps between existing and expected risk management capabilities. A second case study focussed on the cyber security challenges associated with the 'Smarter London Together Roadmap' published in June 2018 [13] to assess the current state of cyber security across Smart London organizations.

II. BACKGROUND

A. *Literature review*

The study of cyber security strategies of the European Union (EU) and North Atlantic Treaty Organization (NATO) countries has revealed that the service resilience, meaning quick recovery from a security incident, is the main goal of their cyber security strategies and that this is achieved through various forms of public-private partnerships [14]. The cooperation and collaboration across public-private sectors is a common thread in cyber security strategies in multiple countries such as Israel [14], Brazil [15], Australia [15], USA [16] and China [17]. However, these strategies differ in the legislative and implementation approaches taken. The Australian cyber security strategy has a state level ownership but focuses on voluntary governance and self-regulation [15]. Israel has a hybrid model between "liberalism and statism" [15]. The Chinese Cyber security Law (CS Law) implemented in Nov 2016 has similarities with the NIS directive. For example, the requirement to report important incidents [17]; 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 [16] 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 [18].

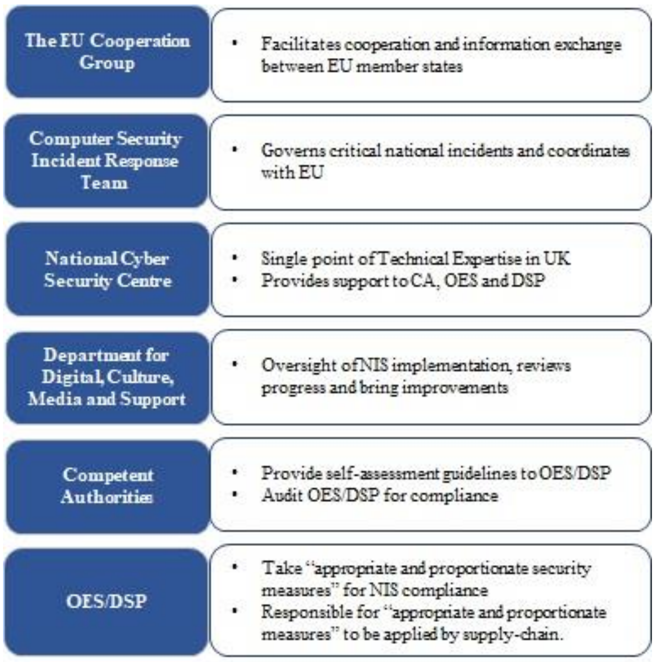
Sufficient research is not available to analyse the cyber security legislations across the world to understand "what works". In UK, the cyber capabilities of sampled sectors to support the National Cyber Security Strategy were analysed in 2016 and organizations were found to have varying levels of abilities [19]. The cross-organizational incident management model for NIS directive was studied in the design stage and found to be designed effectively [20]. rese Another research suggested that the NIS approach is designed to address a compliance problem rather than an opportunity to improve cyber security [21]. Although there is such research available on the NIS approach, none exists on the actual effectiveness of the NIS legislation since its implementation in May 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 the optimal management of legacy systems, reporting incidents within the expected timeframe and insufficient resilience of the Internet-of-Things (IoT) products [22]. The need to focus on the interdependence of critical services within the NIS legislation was also identified in an analysis of approaches to protecting CNI [23].

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 the EU. There is also lack of clarity as to how NIS legislation will be impacted by Brexit [24]. Due to the limited availability of academic literature on cyber security risk management practices of CNI and NIS regulation, this research analyses the information available from Government documents, organisational websites, Freedom of Information requests and interviews of key stakeholders within Critical National infrastructure governing bodies.

B. *NIS Governance*

The structure of NIS governance bodies (see Fig. 2.) is explained in a report by Department for Digital, Culture, Media and Support (DCMS) [12]. DCMS is one of the lead UK government departments responsible for cyber security policy and provides oversight of NIS implementation, reviews progress and recommends improvements [12]. Each of the six sectors under NIS have a lead Department termed as the 'Competent Authority' (CA) that identifies which infrastructure qualifies as a CNI asset in their sector and who are the OES [12]. 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 [12].



The EU Cooperation Group	• Facilitates cooperation and information exchange between EU member states
Computer Security Incident Response Team	• Governs critical national incidents and coordinates with EU
National Cyber Security Centre	• Single point of Technical Expertise in UK • Provides support to CA, OES and DSP
Department for Digital, Culture, Media and Support	• Oversight of NIS implementation, reviews progress and bring improvements
Competent Authorities	• Provide self-assessment guidelines to OES/DSP • Audit OES/DSP for compliance
OES/DSP	• Take "appropriate and proportionate security measures" for NIS compliance • Responsible for "appropriate and proportionate measures" to be applied by supply-chain.

Fig. 2. Key Organizations in NIS Legislation in the UK

Under NIS legislation, the Computer Security Incident Response Team (CSIRT) governs critical incidents in the UK [25] and coordinates with the EU. The DCMS is the UK representative at the EU NIS Cooperation Group [12]. The National Cyber security Centre (NCSC) is a part of the Government Communications Headquarters (GCHQ), which aims to protect critical services [26] and is the single point of technical expertise under NIS legislation which aims to protect critical services [26] and is the single point of technical expertise under NIS legislation. In addition to these agencies, the Centre for Protection of National Infrastructure (CPNI), is the national technical authority for physical security and personnel/people security [27] and coordinates with the NCSC to provide cross-cutting security, but is not covered by the NIS legislation.

C. Cyber Security Risk Management under NIS

NIS principles define a set of required outcomes that result in good cyber security practice for OES/DSP [27].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 NIS objectives to each of the 14 principles (see Fig. 1) for NIS compliance assessment [27].Against each NIS principle, the CAF lists the standards followed and a set of Indicators of Good Practice (IGPs) for cybersecurity risk management. NIS also focuses on the organizational resilience i.e. the ability to operate normally in the event of failures, incidents or cyber/physical attacks. The NCSC CAF mandates dry runs of emergency response and recovery plans of services provided by all organizations. [27]. The outcome-based CAF IGP for NIS compliance ensure that regulatory assessments do not become a tick-box exercise and instead work as a means of achieving improved cyber risk management practices.

D. Cyber Security Incident Management under NIS

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 it [12]. The DCMS report also states that if a cyber and/or physical incident has an impact on European services, the CSIRT needs to inform the Cooperation group that facilitates cooperation and communication within EU member states. The UK Government proposes to issue penalties similar to those in the General Data Protection Regulation (GDPR) for breaches of NIS compliance [28].

III. Research Methodology

Due to insufficient empirical data on NIS implementation, in May 2018 the lead researcher gathered data by interviewing professionals from 30 organizations within the CNI sectors and in this way addressed the first objective of understanding the NIS framework implementation across sectors. A sampling approach was used to identify key areas for the research. The sampling frame consisted of key organizations impacted by the NIS legislation in England from the DCMS report [8]. These included NCSC, DCMS and the CA for each sector in England (see Appendix-A for a list). The rail transport, road transport and health sectors were also 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 National Health Service (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 that are exempt from NIS [24]. This approach led to 35 stakeholders from 30 organisations being identified as targets for the research (see Appendix-A for the full list).

To address the objective of assessing the effectiveness of the NIS legislation, a case study approach was taken to compare the current cyber security framework against the NIS regulatory framework of a sampled CNI sector. The health sector was selected for this case study because the stakeholders within this sector volunteered to provide detailed information to support the analysis.

A second case study analysed the cyber security needs of the Smarter London Together Roadmap to meet the third objective of understanding how the lessons learned from NIS implementation can be applied to London’s cyber security strategy. 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 national 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 also included in the sampled organizations.

IV. Results

A. Results - NIS Implementation Approach

This section summarizes the results from the interviews with DCMS, CPNI and multiple stakeholders across the NIS sectors. 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 the CA to review the application of NIS regulation within their respective sectors. Information published by the NCSC (including the CAF) is intended to support the CAs in their role. A DCMS stakeholder provided insight into NIS implementation journey, which is summarised in Fig. 3.

DCMS has published guidance for the CA to implement the NIS risk management framework. This includes direction on how to create sector-specific guidance for the OES/DSP [12]and the criteria to identify the OES in their sectors [8]. A DCMS stakeholder 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 need 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. Responses from the interviews with multiple stakeholders suggested that CAs are not experienced in cyber security

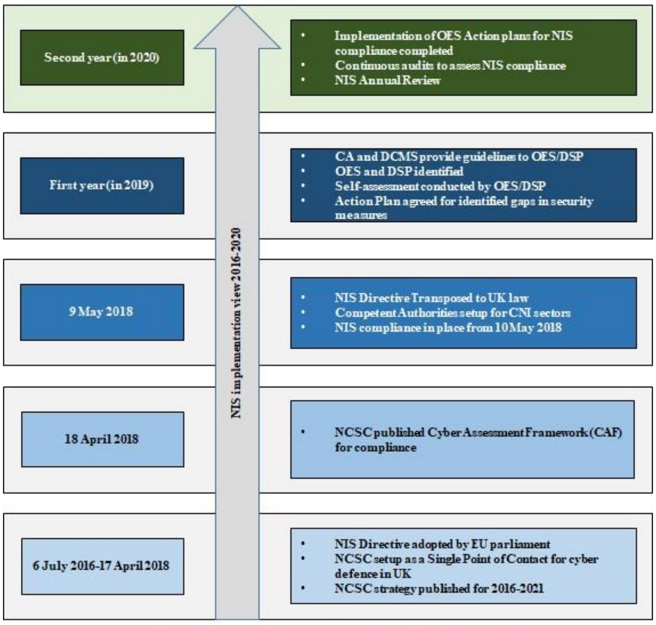

Second year (in 2020)
Implementation of OES Action plans for NIS compliance completed
Continuous audits to assess NIS compliance
NIS Annual Review
First year (in 2019)
CA and DCMS provide guidelines to OES/DSP
OES and DSP identified
Self-assessment conducted by OES/DSP
Action Plan agreed for identified gaps in security measures
9 May 2018
NIS Directive Transposed to UK law
Competent Authorities setup for CNI sectors
NIS compliance in place from 10 May 2018
18 April 2018
NCSC published Cyber Assessment Framework (CAF) for compliance
6 July 2016-17 April 2018
NIS Directive adopted by EU parliament
NCSC setup as a Single Point of Contact for cyber defence in UK
NCSC strategy published for 2016-2021
NIS implementation view 2016-2020

Fig. 3. Business Transformation for UK CNI under NIS Legislation

regulatory tasks and that some were reluctant to accept regulatory responsibilities in this area. So, even after NIS implementation, efforts were on-going to ensure buy-in from the CAs, the OES and the DSPs.

In order to coordinate, support, and to help develop methods to assess compliance with NIS, 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. The NIS enforcement requires an outcome-focused approach as opposed to a tick-box exercise provided by the CAF to achieve a step change in good risk management practices [28]. 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 the OES in their sectors.

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 exercise with the CAs to assess themselves against the CAF and report 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 [12] A DCMS stakeholder expects that in a year's time, there should be a clear understanding of how different sectors manage cyber security under the NIS legislation. They 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. As noted by the DCMS stakeholder, there is no governance to ensure that the decisions made by the CAs for appropriate and proportionate security are consistent across sectors, especially for cross-sector services.

A CPNI stakeholder observed that the CAF may not be a complete list, and currently does not include the non-cyber elements required for the cyber risk management. This is problematic as cyber, physical and personnel security are an integral part of holistic security. Additionally, the NCSC CAF currently does not include non-cyber elements; it needs to mature to take into account risk assessment and resilience tests for cyber-physical attacks and risks from smart infrastructure, and the IoT, including medical devices accessible through the internet. This risk is not currently evaluated within the CAF. A DCMS stakeholder confirmed that the NIS framework key performance indicators (KPI) are yet to be defined. The intention is to develop the CAF based on industry feedback and further research by NCSC.

In response to a holistic governance query, a CPNI stakeholder and DCMS stakeholder confirmed that for NIS, there is an on-going discussion on the governance of 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. A DCMS stakeholder confirmed that the cyber infrastructure such as 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 to address this gap.

1) Finance Sector: The finance and banking sectors are exempt from NIS [24] and historically, are heavily regulated at a local and global scale. As per the Financial Conduct Authority (FCA) stakeholder, these sectors have already made considerable efforts to mature and evaluate their cyber security framework for continuous learning. However, there is a gap in terms of a robust agreed supply chain framework across the industry. The CBEST framework implemented by the finance sector [29], an intelligence-led ethical hacking tool, is widely considered to be a world-leading framework [30]. The Payments Systems Regulator (PSR) stakeholder suggested the development of the fraud prevention and detection monitoring systems (such as the ones prevalent in the banks) for other industries.

2) The Transport sector: In England, on behalf of the Secretary of State for Transport, the Cyber Compliance Team (CCT) in Department of Transport (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 Civil Aviation Authority (CAA) share the roles and responsibilities of the CA". The sub-sectors are at varying degrees of NIS maturity i.e. some are just starting to implement cyber risk management practices while others already have stringent measures in place. For example, CAA stakeholder mentioned that the Civil Aviation Publication (CAP) 1574 framework was published in Dec 2017. This 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 NIS deter and concluded that the controls that are already operational appropriately support the delivery of NIS [31]. A CAA stakeholder also confirmed that self-assessment is under way to comply with the legally binding aspects of NIS legislation and European safety regulations.

For the rail sub-sector, an Office of Rail and Road (ORR) stakeholder confirmed, "There are significant overlaps between the NIS regulatory requirements and the current rail regulations. There are also overlaps between safety and security regulations which need to be understood." However, the 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 CPNI and ORR stakeholders also confirmed that the functionality of old legacy systems is not always understood, some of these are not patched regularly as operators are fearful about losing functionality. As a result although the security framework is being upgraded, it is difficult to resolve the vulnerabilities in the legacy systems.

The maritime sub-sector Cyber Security codes of practice for Ports and Port Systems were published in August 2016 and in September 2017 for Ships [32]. However, a Department of Transport (DfT) stakeholder agreed that the NIS principles go further than these Codes of practice and hence a self-assessment for NIS compliance is currently under-way to upgrade the security framework.

A key stakeholder for road sub-sector, Highways England, confirmed that unlike aviation, maritime and rail, "there are no existing regulations for cyber security or requirements that overlap with NIS regulations. The cyber security vulnerabilities are being self-assessed and risk management measures will progress based on the upcoming threat landscape. As a result, the current guidance from DfT to the road service operators is to work within their existing licensing agreements for NIS compliance."

3) Health Sector: The Department of Health and Social Care (DHSC), the CA for the health sector, has published sector-specific NIS implementation guidance [33]. An NHS stakeholder confirmed that, as per the guidelines from DHSC, all NHS Trusts and Foundation Trusts in England are designated as OES. Although the health sector has mature processes and good governance and processes in place, the current cyber assessment framework is focused on data and information security. The health sector will be the only sector expecting all OESs to go through the audit for 'Cyber Essentials Plus', an NCSC assessment framework used to assess the cyber security technical controls of an organization, to analyse their cyber security risks and vulnerabilities. However, as mentioned by a DHSC stakeholder and the Public Accounts Committee (PAC), the NHS Digital and Care Quality Commission (CQC) audited 200 NHS trusts post the 2017 Wannacry cyber-attack, and found that all of them failed the 'Cyber Essentials Plus' on-site assessments [34]. A DHSC stakeholder also confirmed, "the technical controls within this tool may not cover the full range of CAF IGP". As mentioned by an NHS England stakeholder, in 2017/18 key NHS Trusts received £21m to address cyber vulnerabilities of legacy systems; a further £25m were also provided [34]. It remains to be seen whether this results in imrpoved cyber security risk management within NHS trusts.

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 cyber-attacks [35]. The CAs within the water sector are the Department for Environment, Food and Rural Affairs (Defra) and the Drinking Water Inspectorate (DWI) [36]. 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. In response to a Freedom of Information (FOI), a DWI stakeholder suggested that "All of the NIS requir ements are in their infancy and need to be shaped".

5) Energy Sector: The Office of Gas and Electricity Markets (OfGem) and Business, Energy and Industrial Strategy (BEIS) are two of the key CAs for the energy sector [37]. They are is in a formative stage of developing procedures for the management of cyber risks. A DCMS stakeholder explained that considering the regulatory experience required to enforce the NIS compliance framework, BEIS will deploy the Health and Safety Executive (HSE) inspectors for NIS assessments.

6) Digital Infrastructure: The Office of Communications (OfCom) is the CA for the Digital Infrastructure sub-sector. This include electronic communication services, and includes elements of internet infrastructure such as internet exchanges, domain name service providers, and internet exchange point operators [38]. For Ofcom this is a change in scope from their responsibilities for the telecom networks, economic regulation and media [30], work is in progress to figure out the security vulnerabilities.

7) Digital Service Providers: The Information Commissioner's Office (ICO) is the CA for the DSPs and is guided by the European Network and Information Systems Agency (ENISA) and the Cooperation Group [12]. In response to an FOI request, the ICO noted that required initial guidance to the relevant DSPs has been published on the ICO website [40]. As per this guidance, to facilitate identification of the DSPs, all DSPs are required to register with the ICO within a timeframe specified by 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 [39]. This is intended to enable compliance with multiple NIS requirements.

The assessment of NIS implementation for the above sectors identified common issues across the sectors including (1) the limited experience of the CA and the auditors for cyber-risk management in many sectors, (2) the lack of a robust supply-chain framework, (3) overlaps between the safety and the security regulations and (4) the legacy Industrial Control Systems (ICS) not being patched due to fear of losing functionality. The air transport sub-sector was found to be the most mature and possibly has minimal gaps with the 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 the water sector is in a formative stage and needs to invest the most effort to implement the NIS requirements.

B. Results- Effectiveness of NIS

The second objective of the research was to review the effectiveness of the NIS implementation approach to meet the key strategic objective of upgrading the capabilities of the OES and the DSP in a progressive manner. A case study was conducted to assess the gaps between the current cyber security regulatory framework within the health sector and the NIS framework. Currently, the health sector uses a Data Security and Protection Toolkit (DSPT) [40] for regulatory assessments (Refer Appendix-C). To understand the gaps in the health sector against compliance with NIS, DHSC has provided an initial mapping of the 14 NCSC CAF principles [27] against DSPT security standards (Refer Appendix-D), the assessment framework for NIS compliance in the health sector. As mentioned by a DHSC stakeholder, DSPT was recently modified to include elements of GDPR using a checklist approach. DSPT was 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 purposes of research. The main researcher conducted an independent assessment by mapping the expected outcomes within the NIS CAF principles to the DSPT standards.

As seen in the output of this analysis (see Appendix-D), the DSPTv5.1 self-assessment checklist does not cleanly map onto the 14 CAF principles. This is because the NIS regulation is about cyber risk management rather than data and information security management, as tested by the DSPT. The analysis found that the DSPT followed a checklist audit approach and using this approach misses out a few qualitative aspects of the outcome-based CAF. This strongly suggests that modifying the DSPT for CAF elements might not be enough to move away from a checklist mentality. It might therefore fail to meet the NIS objective of outcome-based assessments to improve 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 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. The KPIs for NIS framework need to be defined, measured and analysed to support this process.

C. Results- Non-CNI Sectors within Smart London Together planning

The third and final objective of the research was to study the non-CNI organizations within London to assess whether the best practices of the NIS cyber security approach can be applied to the Smarter London Together plan. A Greater London Authority (GLA) stakeholder 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". They further explained that the Smart London initiative 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. A varying degree of cyber security risk identification and governance already existed across organizations. 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. There is also a clear need for cyber security as business-as-usual (BAU), by embedding default security by design in smart products and services. 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.

The Publicly Available Specification (PAS) 185:2017, commissioned by CPNI and facilitated by the British Standards Institute (BSI), is the UK specification for establishing and implementing a city-wide, strategic-level, security-minded information sharing approach for a smart city [41]. PAS 555, Cyber security risk – Governance and management standard – which uses an outcomes-based approach, however, does not specifically address the security issues that arise in a smart city [42]. The case study found that the cyber security risk management principles under NIS can be mandated in the non-CNI organizations to provide consistent standards and upgrade the current capability of the organizations. This can help prevent the emergence of smart silos rather than an integrated smart city. The customisation of the NCSC CAF and integration into the design cycle of smart city services and products can be beneficial rather than refactoring it later with expensive solutions.

V. Discussion

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

A. 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 overlaps between cyber and non-cyber security measures not being addressed. There could also be possible duplication within the 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 the NCSC CAF elements [43]. 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 CPNI [11] with relevant IGPs. These guidelines can be included in the NCSC

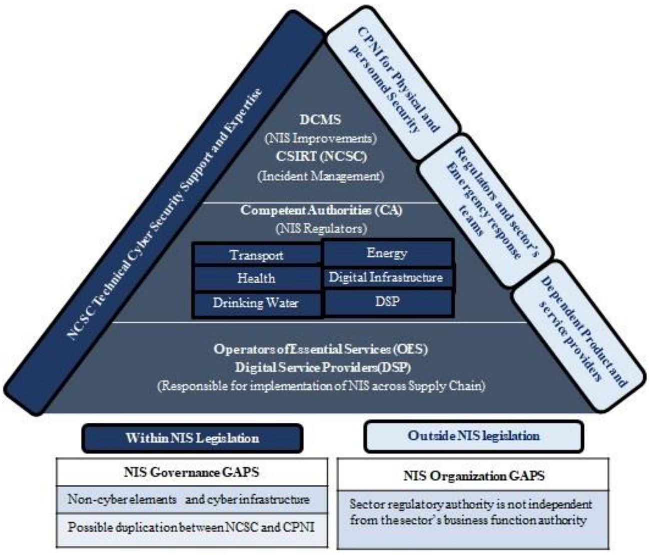

NCSC Technical Cyber Security Support and Expertise
CPNI for Physical and personnel Security
Regulators and sector's Emergency response teams
Dependent Product and service providers
DCMS
(NIS Improvements)
CSIRT (NCSC)
(Incident Management)
Competent Authorities (CA)
(NIS Regulators)
Transport
Energy
Health
Digital Infrastructure
Drinking Water
DSP
Operators of Essential Services (OES)
Digital Service Providers (DSP)
(Responsible for implementation of NIS across Supply Chain)
Within NIS Legislation
Outside NIS legislation
NIS Governance GAPS
Non-cyber elements and cyber infrastructure
Possible duplication between NCSC and CPNI
NIS Organization GAPS
Sector regulatory authority is not independent from the sector's business function authority

Fig. 4. Organization and Governance - NIS Framework

CAF. Cyber infrastructure, such as data centres and transmission lines, are not covered by the NCSC or CPNI frameworks – an issue raised by the DSPs to DCMS in a public consultation [44]. In contrast, the reporting of cyber risks in data centres is already part of the US cyber security framework [18]. 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 address the above gaps. Fig. 4. summarizes the current NIS governance and gaps.

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

The Government departments that have business responsibilities for a specific sector are also tasked with the CA responsibility of regulating NIS, wherein they make judgements of what are appropriate and proportionate security measures. Consequently, it is possible for compliance judgements to be influenced by budgetary or business constraints. As an example of a budgetary conflict, it would be extremely counter-productive 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 IV above, the DSPT does not map fully onto the 14 NIS principles. However, DHSC is empowered to take decisions on what assessment needs to be included within the DSPT, based on their judgement of appropriate and proportionate security measures. Moreover, these may not be consistent across sectors for end-to-end service resilience. It is suggested that a specialist team consisting of sector CA representatives, DCMS and NCSC is required to validate that up-to-date NIS regulatory assessments are in place across sectors and these are in line with the NIS principles. This would 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.

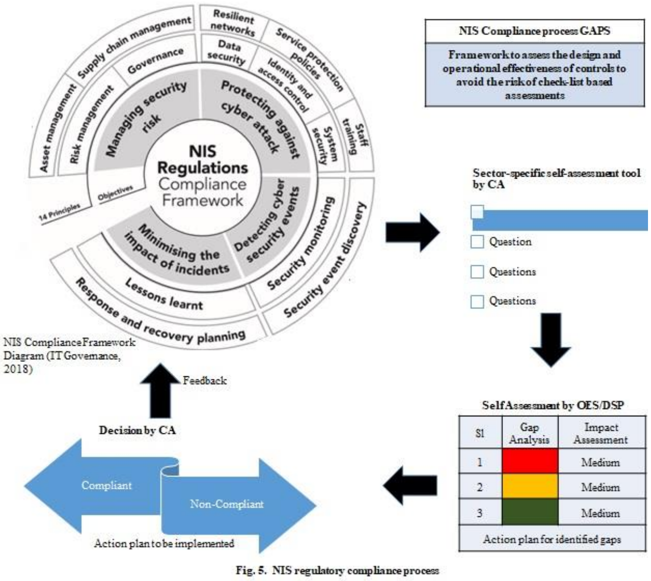
Recommendation 2: DCMS to work with CA and NCSC to introduce an outcome-based NIS audit framework for oversight and governance. This governance is intended to ensure appropriate implementation and assessment of NIS principles by an authority independent from the CA business functions.

B. Processes: Compliance and Assessment

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 gaps identified through self-assessment, action plans and strategies for regulating the sector in the first year. Fig. 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. The NIS CAF is an outcome-based approach that specifies what needs to be achieved rather than exactly what needs to be done. However, as seen in the health sector case study in section IV, the NIS compliance framework in many cases uses a tick box approach for checking the presence of selective controls. In contrast, the finance and banking sectors have recognized that a check-list based compliance assessment may not successfully assess the effectiveness of the risk management process [45]. Therefore, the organizations in the finance and banking sectors conduct regulatory assessments of the design and operational effectiveness of key controls that have been mapped to the top organizational risks [46]. To achieve the outcome-based objective of the NIS CAF, the recommendations is to implement a similar risk-based audit framework is for NIS compliance assessments across all sectors. . Some best

practices from the CBEST tool described in Section IV above (A. NIS Implementation approach, 1. Finance and Banking Sector), 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


NIS Regulations Compliance Framework
Managing security risk
Protecting against cyber attack
Detecting cyber security events
Minimising the impact of incidents
Asset management
Risk management
Supply chain management
Governance
Resilient networks
Data security
Service protection policies
Identity and access control
System security
Staff training
Security monitoring
Security event discovery
Lessons learnt
Response and recovery planning
14 Principles
Objectives
NIS Compliance Framework Diagram (IT Governance, 2018)
Feedback
Decision by CA
Compliant
Non-Compliant
Action plan to be implemented
NIS Compliance process GAPS
Framework to assess the design and operational effectiveness of controls to avoid the risk of check-list based assessments
Sector-specific self-assessment tool by CA
☐ Question
☐ Questions
☐ Questions
Self Assessment by OES/DSP

Sl	Gap Analysis	Impact Assessment
1	🟥	Medium
2	🟨	Medium
3	🟩	Medium
Action plan for identified gaps		

Fig. 5. NIS regulatory compliance process

C. Processes:Incident Management and Emergency Response and Recovery

OES/DSP are required to share details of incidents with impacts above a defined threshold to their CAs within 72 hours of being aware of them. The CAs are subsequently expected to conduct post-incident analysis of such incidents. 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.

A 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 the 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 across national borders.The cross-sector security risk and emergency recovery processes are currently at different stages within different sectors. The finance sector is compiling lessons from 34 live disaster recovery exercises at sector level, while 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 [30]. More focus is required within the NIS on cross-sector resilience to understand and strengthen cross sector dependencies [47]. The members of cross-sector regulatory collaborative forums such as the UK Regulators Network (UKRN) are facilitators but the experts within the regulatory organisations are currently not actively participating in the forum [30]. Cross-sector security and resilience processes are also not covered by the the NCSC CAF. 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 also not managed. Cross-sector lessons learnt could be strengthened by voluntary information sharing of incidents and threats across the private, Government and public sectors [48].

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

The reliance on international supply chains comes with multiple threats, such as the impact of global security vulnerabilities, and 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. However, there is a lack of a robust supply-chain framework for cyber security. Some of the cross-sector end-to-end services are operated by a common supply-chain and hence it remains to be seen how OES and DSP will ensure that supply-chains are compliant to NIS CAF requirements.

D. People Capabilities

The NIS regulation is a part of the NCSC's cyber security strategy 2016-2021 and £1.9 billion of funding has been provided for its implementation strategy [49] . However, the lack of skills at operational and governance levels, as well as the difficulties associated with estimation of the infrastructure costs, are just some of the key budgeting issues associated with mitigating cyber security risks [44]. Each sector has its own approach to address this shortfall in regulatory experience. BEIS is planning to use retrained in-house Health and Safety (HSE) capacity, and Defra plans to use DWI inspectors for audit activities. Table 1 summarizes the gaps for each sector specifically in outcome-focussed audits. As mentioned earlier in this section (B. Processes: Compliance and Assessment), the business and service assurance-based audits, which assess the quality of risk management, are recommended for NIS assessments.

TABLE1 PEOPLE CAPABILITY GAPS

Sector	**CA and Auditors (England)**
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 ommunications and media, will re-use existing audit capability
Digital Service Providers	ICO – Experienced in GDPR enforcement Will reuse ISO 27001 and GDPR audit team

Control engineers and security engineering can combine best practices to design process controls that are focused on the 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 multi-disciplinary teams for NIS audit 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 one.

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

E. Technology

Industrial Control Systems (ICS), such as the supervisory control and data acquisition (SCADA) in manufacturing and industrial environments are the key OT vulnerabilities compounded by the IoT [22]. As mentioned by ORR stakeholders, the physical devices/machines controlled by ICS connected to the internet in order 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 their age and loss of knowledge. Additionally, there needs to be a clear understanding of how the security of OT systems is different from the security of IT systems and what the risks are [9]. As a simple mitigation, the IT and the OT systems need to be completely separated to prevent cyber-attacks within one system causing damage to the other [44]. CPNI has provided best practice guidelines on ICS and technology project security which also map to the U.S. NIST framework discussed above [50], and these guidelines are reflected on the NCSC webpage [51]. However, the ICS and OT risk management compliance outcomes are not part of the NCSC CAF.

There is currently 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 (e.g. a hospital a pacemaker embedded within a patient [22]). Innovative technology guidelines have been provided in some instances, such as Connected Automated Vehicles (CAV) by DfT [52], British Standard Institute (BSI) smart city standards [53] and IoT guidelines by DCMS and NCSC [54]. 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 the management of risk and resilience from technological threats from the smart transport, smart medical devices and smart energy.

Legacy OT systems are functional, but operate in the same cyber space as smart IoT devices, which may result in the connected smart city being more vulnerable. Lack of timely patching of the OT systems 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 [55]. Currently, there is limited mitigation available for legacy systems and the alternative of replacing these systems is very expensive.

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

F. Continuous Improvements

DCMS is committed to providing a report of assessment of the impact and effectiveness of the NIS by 2020 [56]. The KPIs need to be embedded as a part of this process for continuous improvements (see Fig. 6.) rather than being added as a retrofit measure. The CPNI Plan-Do-Check-Act (PDCA) checklist, provides guidelines to define measures for security management and effectiveness assessment which can be used to inform KPIs For the NIS framework[43]. The success criteria for the NIS legislation can also be defined based on the CAF assessments.

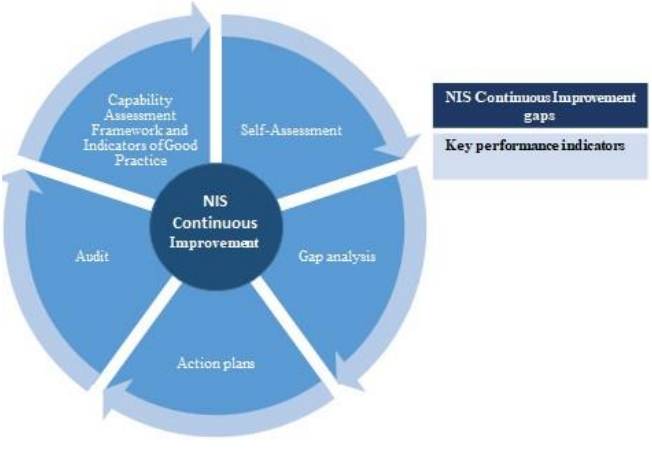

Capability Assessment Framework and Indicators of Good Practice
Self-Assessment
NIS Continuous Improvement
Audit
Gap analysis
Action plans
NIS Continuous Improvement gaps
Key performance indicators

Fig. 6. NIS Continuous Improvement Gap

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

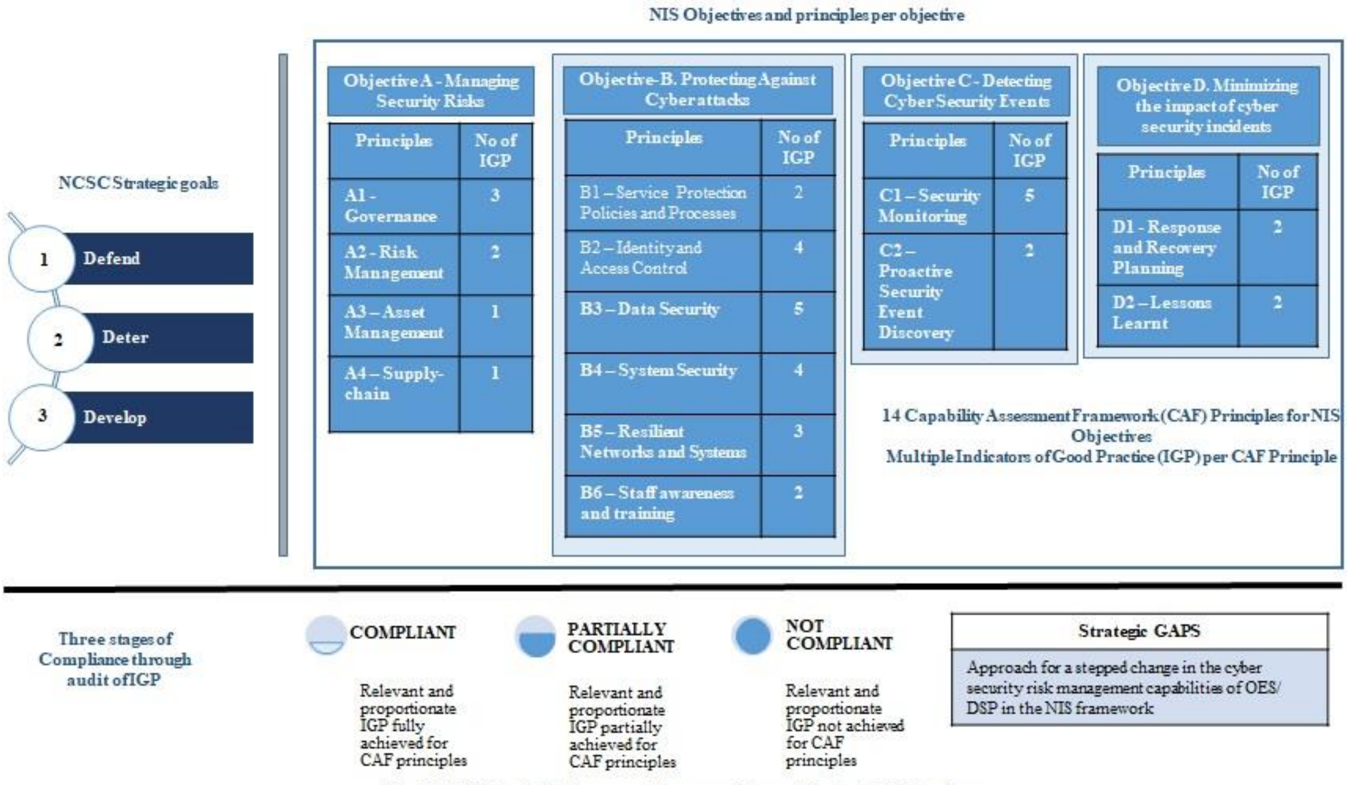
G. Security Culture

The need for products and services to be secure by design has been recognised by the industry prior to the advent of smart infrastructure. It is concerning that regulation is required for cyber security for CNI and smart city operations to this day. The 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. All designs and engineering lifecycles should consider security from the very earliest stages.

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

A Transport for London (TfL) stakeholder raised concerns about issuing penalties across multiple regulations for the same breach across NIS and GDPR. Multiple overlapping controls spanning quality control, risk, safety, quality, data privacy, information control and business assurance practices lead to audit inefficiencies.The integration of cyber security and holistic security principles into safety, quality, risk management and business assurance frameworks can lead to a BAU approach towards cyber-security. CPNI has published integrated core principles of safety, security and quality using PDCA, an iterative four- step continuous improvement method [43]. Annex-SL presents an initiative from BSI which aims to rationalize ISO quality frameworks, and looks at a core set of generic requirements to avoid duplication across the ISO frameworks [57].

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


NIS Objectives and principles per objective
NCSC Strategic goals
1 Defend
2 Deter
3 Develop
Objective A - Managing Security Risks
Objective-B. Protecting Against Cyber attacks
Objective C - Detecting Cyber Security Events
Objective D. Minimizing the impact of cyber security incidents
14 Capability Assessment Framework (CAF) Principles for NIS Objectives
Multiple Indicators of Good Practice (IGP) per CAF Principle
Three stages of Compliance through audit of IGP
COMPLIANT
Relevant and proportionate IGP fully achieved for CAF principles
PARTIALLY COMPLIANT
Relevant and proportionate IGP partially achieved for CAF principles
NOT COMPLIANT
Relevant and proportionate IGP not achieved for CAF principles
Strategic GAPS
Approach for a stepped change in the cyber security risk management capabilities of OES/DSP in the NIS framework

Principles	No of IGP
A1 - Governance	3
A2 - Risk Management	2
A3 – Asset Management	1
A4 – Supply-chain	1

Principles	No of IGP
B1 – Service Protection Policies and Processes	2
B2 – Identity and Access Control	4
B3 – Data Security	5
B4 – System Security	4
B5 – Resilient Networks and Systems	3
B6 – Staff awareness and training	2

Principles	No of IGP
C1 – Security Monitoring	5
C2 – Proactive Security Event Discovery	2

Principles	No of IGP
D1 - Response and Recovery Planning	2
D2 – Lessons Learnt	2

Fig. 7. NCSC Capability Assessment Framework to meet the strategic NIS goals

H. Strategic Goals

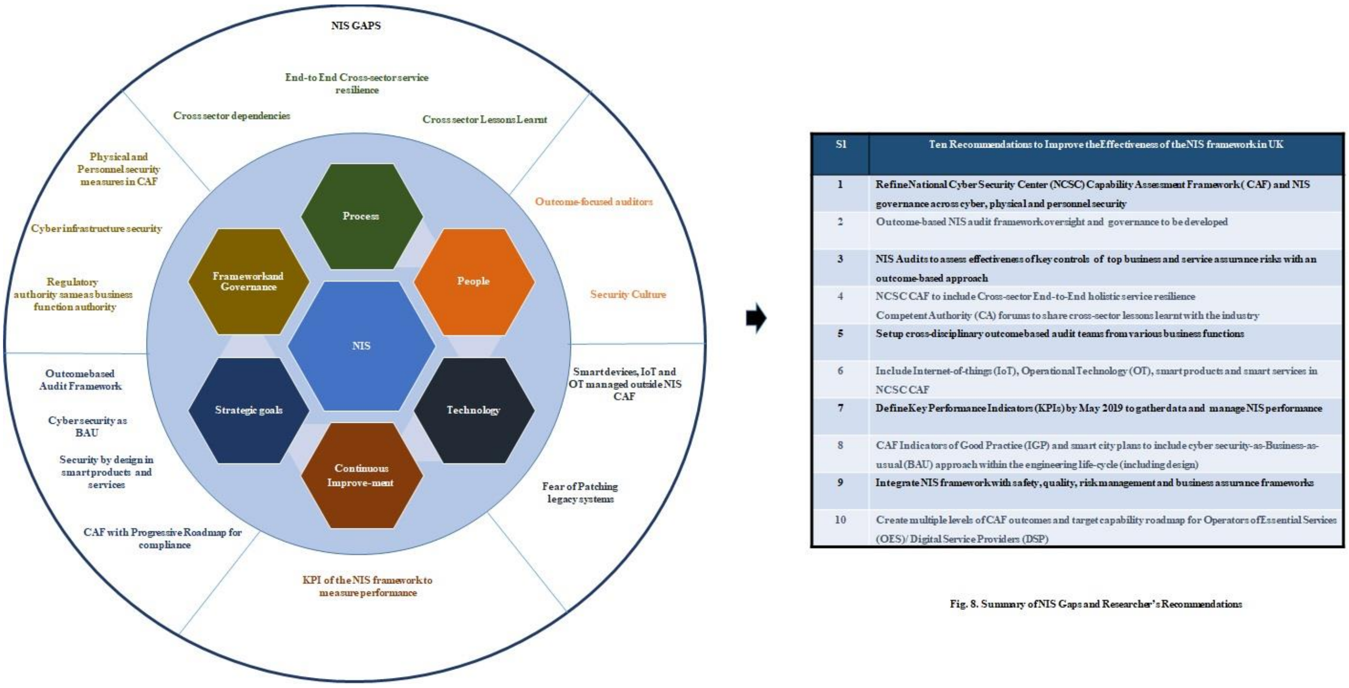
The key strategic objective of NIS regulation is to bring a step change in the cyber security risk management capabilities of the OES and DSP organizations to improve the resilience of the CNI services. The current CAF framework implementation strategy is described in Fig. 7. and was referenced in section II (D. Cyber Risk Assessment Framework). The NCSC is already examining business processes that underpin the services in the CNI sectors to understand the critical systems and networks [48]. But currently there is no clarity as to how the NIS framework will help to achieve these objectives considering the OES/DSP are at different levels of capability maturity as analyzed in Section IV above (A. NIS Implementation approach). 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. The CAs need to work with the 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: Provide multiple levels of NIS compliance and the CAF IGP. Define the required target level for NIS compliance. Create a progressive roadmap for OES/DSP to achieve an adequate level of IGP.

The gaps and recommendations are summarized in Fig.8. It is important for the NCSC CAF to address the above recommendation at CAF framework level to ensure consistent levels of cyber security of a CNI service across sectors proportionate to the risks, and bring a step-change in OES and DSP capabilities. It is noteworthy that a similar approach has worked in the U.S. NIST framework, which provides four tiers of implementation based on risk management practices of an organization [16]. The organization defines current as well as target risk profiles that map to the appropriate implementation tier relevant to the organization’s risk requirements [16].

To summarize, the NIS legislation puts the maintenance of sound risk management and cyber-resilience control systems at the centre 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 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 in the USA, where the NIST framework has been extended to small businesses [58], NIS principles could be adopted by the other non-CNI organizations in the 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 the 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. The U.S. NIST framework [27] claims to “serve as a model for international cooperation to


NIS GAPS
End-to End Cross-sector service resilience
Cross sector dependencies
Cross sector Lessons Learnt
Physical and Personnel security measures in CAF
Outcome-focused auditors
Cyber infrastructure security
Regulatory authority same as business function authority
Security Culture
Smart devices, IoT and OT managed outside NIS CAF
Outcomebased Audit Framework
Cyber security as BAU
Security by design in smart products and services
Fear of Patching legacy systems
CAF with Progressive Roadmap for compliance
KPI of the NIS framework to measure performance
Process
Framework and Governance
People
NIS
Strategic goals
Technology
Continuous Improve-ment

Sl	Ten Recommendations to Improve the Effectiveness of the NIS framework in UK
1	**Refine National Cyber Security Center (NCSC) Capability Assessment Framework (CAF) and NIS governance across cyber, physical and personnel security**
2	Outcome-based NIS audit framework oversight and governance to be developed
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 Competent Authority (CA) forums to share cross-sector lessons learnt with the industry
5	**Setup cross-disciplinary outcomebased 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 Key Performance Indicators (KPIs) by May 2019 to gather data and manage NIS performance**
8	CAF Indicators of Good Practice (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)/ Digital Service Providers (DSP)

Fig. 8. Summary of NIS Gaps and Researcher's Recommendations

strengthen cybersecurity" [16]. If the U.S. NIST and EU frameworks are integrated, that could be a starting point for a global framework for holistic security and risk management.

VI. CONCLUSIONS

The aim of this research was to explore how cyber risks are managed in the 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 the NIS legislation approach that supports the cyber-risk management maturity of OES/DSP, and (3) to study how NIS lessons learnt can be input into 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 our defences with a flexible approach that allows learning and continuously improving outcomes. The research also served as a discovery process for the Smart London Together approach to cyber security and the cyber security of non-CNI organizations.

This research covers a snapshot in time, is limited in scope and it examined the deployment of the NIS in May 2018, and subsequent months. Hence, it will not have captured the longer-term impacts of the evolving NIS process. The research has focused on cyber security aspects influencing the NIS framework, to the exclusion of individual cyber risks and their impact on the risk management framework.

Further research is recommended to obtain better insights and supporting empirical evidence in relation to (i) UK NIS enforcement compared with other EU countries and (ii) integration points for cyber security frameworks between UK and other leading countries. The NIS legislation is the beginning of the journey to achieve a reduction in 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 struck 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".

APPENDIX A – LIST OF STAKEHOLDERS

1) Isabel Bonachera Martin, EU Cyber Security Regulatory Policy, Department for Digital, Culture, Media and Sports (DCMS)
2) Department of Health and Social Care (DHSC)
3) Theo Blackwell, Chief Digital Officer of London, GLA
4) Department of Transport (DfT)
5) Simon Onyons, Finance Conduct Authority(FCA)
6) Nick Davey, Payment System Regulator (PSR)
7) Centre for Protection of National Infrastructure (CPNI)
8) The Office of Gas and Electricity Markets (OfGem)
9) National Health Service (NHS) England
10) Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Deutschland
11) David Tait, Civil Aviation authority (CAA)
12) Nick Swanson, City Hall, GLA
13) London Fire Brigade
14) London Metropolitan Police
15) Steve Burton, Transport for London (TfL)
16) Johnny Schute, James Walker, Ian Maxwell, Office of Rail and Road (ORR)
17) Hitachi Vantara
18) Toby Gould, London Resilience Group
19) Graham Lane, City Hall, GLA
20) Imperial College Healthcare
21) North West London NHS Foundation Trust - CNWL
22) NHS Digital
23) British Standards Institute (BSI)
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

Note: Stakeholders names have been included only where stakeholder’s permission was given to do so.

APPENDIX B – EXPLANATION OF TERMS

BAU – Business-as-usual
BoE – Bank of England
BEIS - Business, Energy and Industrial Strategy
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
CNI – Critical National Infrastructure
CPNI - Centre for Protection of National Infrastructure
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
ENISA - European Network and Information Systems Agency
EU – European Union
FCA - Finance Conduct Authority
GCHQ - Government Communications Headquarters
GDPR - General Data Protection Regulation
GLA – Greater London Authority
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
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
PAS - Publicly Available Specification
PDCA – Plan-Do-Check-Act
SCADA - Supervisory Control and Data Acquisition
TfL – Transport for London
UCL – University College London
UKRN - UK Regulators Network

APPENDIX C – DEPARTMENT OF HEALTH 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 D - An initial mapping of the 14 NCSC CAF principles against DSPT

1. TABLE 2 Self-Assessment against NIS requirements for Objective A

<table>
<tr><th rowspan="2">NIS Objectives</th><th colspan="4">Self-Assessment against NIS requirements for Objective A (Managing Security Risk)</th></tr>
<tr><th><i>NIS PRINCIPLES (NCSC CAF)</i></th><th><i>Mapping with DSPT v5.1</i></th><th><i>Is the NIS Principle covered by DSPT ?</i></th><th><i>Gaps (as provided by DHSC based on the work-in-progress so far)</i></th></tr>
<tr><td rowspan="8"><b>“Objective A:</b> 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.”</td><td>A1 Governance</td><td>Data Security Standard 1</td><td>Full</td><td>The requirement for "empowered to make decisions on how services are protected" will be added in detail to the guidance.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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).</td></tr>
<tr><td>A2. Risk Management</td><td>Data Security Standards 1, 4, 8, 9</td><td>Partial</td><td>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</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>A3. Asset Management</td><td>Data Security Standard 1, 2</td><td>Partial</td><td>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</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>A4. Supply Chain</td><td>Data Security Standard 10</td><td>Partial</td><td>Covered both in the GDRP and Contacts section of the DSPT. The key gap lies in understanding the accountability for outsourcing.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
</table>

2. **TABLE 3 Self-Assessment against NIS requirements for Objective B**

<table>
<tr><th rowspan="2">NIS Objectives</th><th colspan="4">Self-Assessment against NIS requirements for
Objective B (Protecting against cyber attack)</th></tr>
<tr><th><i>NIS PRINCIPLES (NCSC CAF)</i></th><th><i>Mapping with DSPT v5.1</i></th><th><i>Is the NIS Principle covered by DSPT ?</i></th><th><i>Gaps (as provided by DHSC based on the work-in-progress so far)</i></th></tr>
<tr><td rowspan="12"><b>“Objective B:</b> Proportionate security measures are in place to protect essential services and systems from cyber attack</td><td>B1. Service Protection Policies and Processes</td><td>Data Security Standard 1</td><td>Partial</td><td>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.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>B2. Identity and Access Control</td><td>Data Security Standard 1, 4, 10</td><td>Partial</td><td>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.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td></td><td>Data Security Standard 1 to 10</td><td>Partial</td><td>Lifecycle management and destruction included but not explicit reference to mobile devices.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>B4. System Security</td><td>Data Security Standard 2, 4, 8</td><td>Partial</td><td>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.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>B5. Resilient Networks and Systems</td><td>Data Security Standard 7</td><td>Partial</td><td>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</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
<tr><td>B6. Staff Awareness and Training</td><td>Data Security Standard 2, 3</td><td>Full</td><td>Data Security awareness training mandatory for staff with graduating levels depending on role.</td></tr>
<tr><td colspan="4"><b>Researcher's analysis</b>:- 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.</td></tr>
</table>

3. **TABLE 4 Self-Assessment against NIS requirements for Objective C**

NIS Objectives	**Self-Assessment against NIS requirements for Objective C (Detecting cyber security events)**			
	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.			

4. **TABLE 5 Self-Assessment against NIS requirements for Objective D**

NIS Objectives	**Self-Assessment against NIS requirements for Objective D (Minimizing the Impact of Cyber Security Incidents)**			
	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 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 stakeholder.				

ACKNOWLEDGMENTS

We would like to express our gratitude and thank all the 35 stakeholders (Refer Appendix-A) for participating in this research, helping in collating the required data for this research, being open about the current issues and validating the final contents of the dissertation. DCMS was instrumental in providing the facts specific to NIS implementation and Theo Blackwell, the Chief Digital Officer (CDO), support on the Smart London Together roadmap component of the research. We 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 and valuable feedback on the case study.

We would also like to acknowledge the help provided in locating relevant contacts by Maria Bada, Global Cyber Security Capacity Centre, University of Oxford; Prof Brian Collins, University College London; Barry Emerson 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 insights into the ongoing cyber security issues in the Health sector. Many thanks to consultants Marco Franken and Alexandra Luck for proof reading the initial text of the full research report.

REFERENCES

[1] C. Cerrudo *et al.*, "Cyber Security Guidelines for Smart City Technology Adoption," 2016.

[2] Z. A. Baig *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digit. Investig.*, vol. 22, pp. 3–13, Sep. 2017.

[3] K. J. Martin, Guy, Martin Paul, Hankin Chris, Darzi Ara, "Cybersecurity and healthcare: how safe are we?," *theBMJ*, vol. 358:j3179, p. 4, 2017.

[4] R. Piggin, "Protecting our critical infrastructure Understanding new cyber security laws," 2018.

[5] Microsoft, "Risk Management for Cybersecurity: Security Baselines Risk Management for Cybersecurity," 2018.

[6] K. Quigley and J. Roy, "Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America," *Soc. Sci. Comput. Rev.*, vol. DOI: 10.11, no. 30(1), pp. 83–94, 2012.

[7] European Parliament, "Directives," *Official Journal of European Union*, 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. [Accessed: 07-May-2018].

[8] DCMS-c, "The Network and Information Systems Regulation 2018," 2018.

[9] EECSP, "EECSP Report: Cyber Security in the Energy Sector," 2017.

[10] "Implementation of the NIS Directive in Germany | Digital Single Market," 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-germany. [Accessed: 01-Aug-2018].

[11] H.M.Government, "National Cyber Security Strategy 2016-2021," 2016.

[12] DCMS-d, "Security of Network and Information Systems Guidance for Competent Authorities," 2018.

[13] GLA, "Smarter London Together," 2018.

[14] D. Štitilis, P. Pakutinskas, and I. Malinauskait\.e, "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis," *Secur. J.*, vol. 30, no. 4, pp. 1151–1168, Oct. 2017.

[15] F. Smith and G. Ingram, "Organising cyber security in Australia and beyond," *Aust. J. Int. Aff.*, vol. 71, no. 6, pp. 642–660, 2017.

[16] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 2018.

[17] L. Maglaras, G. Drivas, K. Noou, and S. Rallis, "NIS directive: The case of Greece," 2018.

[18] Department of Homeland Security, "The Cybersecurity Act of 2015," 2015.

[19] M. Bada *et al.*, "About the Global Cybersecurity Capacity Centre Lead Editor and Author Contact details," 2016.

[20] A. Rao, N. Carreon, R. Lysecky, and J. Rozenblit, "Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems," *IEEE Softw.*, vol. 35, no. 1, pp. 38–43, Jan. 2018.

[21] C. Walker-Osborn and N. Patel, "EU Cybersecurity Directive," *ITNOW*, vol. 56, no. 2, pp. 38–39, Jun. 2014.

[22] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 450–466, Jun. 2018.

[23] T. VIIRA, "INTERDEPENDENCIES OF SERVICES," in *Lessons Learned: Critical Information Infrastructure Protection*, IT Governance Publishing, 2018, pp. 24–27.

[24] DCMS, "UK Finance response to Department for Digital, Culture, Media and Sport consultation on the implementation of the NIS Directive," 2017.

[25] "Introduction to the NIS Directive," 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/introduction-nis-directive. [Accessed: 01-Aug-2018].

[26] "Welcome to GCHQ," 2017. [Online]. Available: https://www.gchq.gov.uk/. [Accessed: 01-Aug-2018].

[27] "Table view of principles and related guidance," 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance. [Accessed: 28-Jun-2018].

[28] "Regulating Cyber: the UK's plans for the NIS Directive," 2017.

[29] BoE, "CBEST Intelligence-Led Testing CBEST Implementation Guide," 2016.

[30] "Oral evidence - Cyber Security: Critical National Infrastructure," 2018. [Online]. Available: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/oral/81998.html. [Accessed: 31-Jul-2018].

[31] CAA, "CAP 1574, Version 1.0," 2017.

[32] DfT, "Implementation of the NIS Directive Moving Britain Ahead," 2018.

[33] DoH, "Title: The Network and Information Systems Regulations 2018: Guide for the health sector in England," 2018.

[34] House of Commons, "Cyber-attack on the NHS Thirty-Second Report of Session 2017-19," 2018.

[35] Defra, "Water Sector Cyber Security Strategy," 2017.

[36] DCMS-b, "Security of Network and Information Systems Department for Digital, Culture, Media and Sport," 2018.

[37] BEIS, "SECURITY OF NIS REGULATION," 2018.

[38] OfCom, "GUIDANCE Ofcom's interim guidance for Operators of Essential Services in the digital infrastructure subsector under the Network and Information Systems Regulations 2018," 2018.

[39] "Table view of principles and related guidance," 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance. [Accessed: 31-Jul-2018].

[40] "Data Security and Protection Toolkit - NHS Digital," 2017. [Online]. Available: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit. [Accessed: 31-Jul-2018].

[41] B. CPNI, "PAS 185:2017 Smart Cities - Specification for establishing and implementing a security-minded approach," 2017.

[42] BSI, "Smart cities-Guide to establishing a decision-making framework for sharing data and information services BSI Standards Publication," 2017.

[43] CPNI, "PROTECTIVE SECURITY MANAGEMENT SYSTEMS (PSEMS) CHECKLIST," 2018.

[44] R. D. Ruffle Simon, Daffron Jeniffer, Copic Jeniffer, Leverett Éireann, Evan Tamara, "Cyber Security: Critical National Infrastructure Inquiry," 14-Dec-2017. [Online]. Available: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-

security-critical-national-infrastructure/written/81366.html. [Accessed: 26-Jul-2018].

[45] H.M.Treasury, "G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR," 2016.

[46] Chartered Institute of Internal Auditors, "Financial services code," 2018. [Online]. Available: https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/?downloadPdf=true. [Accessed: 06-Aug-2018].

[47] UKRN, "Cross-sector Resilience – Phase 1 report," 2015.

[48] NCSC, "Introduction," 2017.

[49] H.M.Government-a, "National Security Capability Review – March 2018," 2018.

[50] CPNI, "Security for ICS - Framework Overview," 2015. [Online]. Available: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS - Framework Overview Final v1 1.pdf. [Accessed: 31-Jul-2018].

[51] "Security for Industrial Control Systems," *NCSC*, 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/security-industrial-control-systems. [Accessed: 17-Aug-2018].

[52] "The Key Principles of Cyber Security for CAV," 2017.

[53] BSI, "Smart cities-Vocabulary BSI Standards Publication Bio-based products-PAS 600:2013 Part 0: Subtitle BSI Standards Publication," 2014.

[54] "Secure by Design," 2017.

[55] S. House, "William Smart , Chief Information Officer for Health and Social Care Lessons learned review of the WannaCry Ransomware Cyber Attack," 2018.

[56] H.M.Government, "EXPLANATORY MEMORANDUM TO THE NIS REGULATIONS 2018, No 506," 2018.

[57] BSI, "ISO Revisions Introducing Annex SL Whitepaper ISO Revisions," 2015.

[58] B. Barth, "President signs NIST Small Business Cybersecurity Act into law," *SC Media*, Aug-2018.