Post-Implementation Review of the Network and Information Systems Regulations 2018

Presented to Parliament
by the Secretary of State for Digital, Culture, Media and Sport
by Command of Her Majesty

May 2020

CP 242

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at NIS@culture.gov.uk

ISBN 978-1-5286-1939-4

CCS0320329850 05/20

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

SUMMARY **4**

RPC PRO FORMA **7**

FULL REPORT **10**

Scope of this review 10
The objectives and intended outcomes of the Regulations 11
Assessment of proportionality for level of evidence sought 14
Evidence collection and methodology 15
Are the Regulations working? 18
Assessment of the actual costs and benefits of the Regulations 24
Costs 24
Benefits 39
Aggregated costs and benefits 42
Is government intervention still required? 43
Is the existing form of government regulation still the most appropriate approach? 44
EU-derived regulations 45
What are the areas for improvement? 48
Next steps 51

ANNEXES **54**

Annex A: Questionnaire used to survey OESs 54
Annex B: Questionnaire used to survey RDSPs 67
Annex C: Competent Authority Report 79
Annex D: Assumptions Log 88

SUMMARY

Introduction

The 2016-2021 National Cyber Security Strategy committed the Government to ensuring the right regulatory framework is in place for cyber risk to be properly managed across the economy, including within organisations which provide our most important services. The Network and Information Systems (NIS) Regulations represent a cornerstone of this approach, as the first cross-cutting piece of cyber security focused regulation. The Regulations are designed to raise security standards across multiple critical sectors through outcomes-based regulation which enables the approach to consistently adapt in a rapidly evolving environment.

This post-implementation review (PIR) of the NIS Regulations aims to determine how effective the Regulations have been in achieving the original objectives to date, whether those objectives remain appropriate two years on, as well as looking at how the Regulations have been implemented and the costs and benefits incurred. The review comes at an important time for wider policy development in this area. Findings from this PIR will help to inform broader policy development on the key challenges which remain in ensuring organisations are effectively managing their cyber security risk. This contributes to our overarching goal of ensuring businesses are able to prosper, citizens are protected, and the UK is the safest place in the world to be online.

Background

The overarching objective of the NIS Regulations, which came into force on 10 May 2018, is to improve the security of network and information systems which are critical to the provision of essential services and certain digital services, which if disrupted, could cause significant economic and social harm to citizens, businesses, and critical national infrastructure. The Regulations set out legal measures required to boost the overall level of security of network and information systems of organisations in scope.

The UK was one of the first countries to fully transpose the EU derived NIS Directive into domestic legislation, and opted for an approach that minimised regulatory burdens on organisations in scope by not extending the Regulations to organisations covered by existing legislation that was already in place, and which was at least equivalent to the Directive.

The Regulations apply to Operators of Essential Services (OESs) in the transport, energy, water, health, and digital infrastructure sectors as well as to relevant Digital Service Providers (RDSPs). The Regulations specify that - if falling within the designation thresholds - an OES or RDSP must:

1. Take appropriate and proportionate measures to ensure the security of the network and information systems used to provide their essential services, both by managing risk and by minimising impact of any disruption;

2. Notify their Competent Authority about any incident which has an adverse effect on the security of the network and information systems used to provide their

essential services, according to criteria set out in incident reporting thresholds.

The implementation and enforcement of the NIS Regulations is the responsibility of designated Competent Authorities. Regulatory activity is supported by the UK's national technical authority, the National Cyber Security Centre.

Key findings and conclusions

The evidence gathered for this PIR suggests that while it is too early to judge the long term impact of the Regulations as they came into force only two years ago, organisations are taking measures to ensure the security of their networks and information systems, as a result of the Regulations being in place, in line with their objectives. We expect this action is leading to a reduction in the risks posed to essential services and important digital services relying on networks and information systems.

However, there is still room for further improvement. Although data suggests that improvements to security are being made, organisations need to continue to accelerate their improvements. Society and the economy at large rely extensively on the services in scope of the Regulations, and the failure or compromise of network and information systems in these sectors is a systemic risk to the services they provide. There remains a significant threat to the sectors in scope of the Regulations, and intervening to reduce the risk in this sphere remains appropriate.

Proportionate and targeted regulation - such as the NIS Regulations - is wholly appropriate and necessary considering the security challenges and threats facing the sectors in scope. While short-term data indicates that the Regulations have had a positive impact on incentivising operators to improve the security of their network and information systems, the full benefits of the Regulations are unlikely to have been felt in the short period of time since implementation in May 2018, and are unlikely to be fully realised for several more years. Future PIRs will be able to look in more detail at the long-term impact of the Regulations.

Next steps

As set out above, the evidence indicates that during the short time that the Regulations have been in force, progress has been made towards achieving the regulatory objectives. There remains a need for regulatory intervention in this area, and the Government plans to make technical changes to the regulatory regime as set out below to ensure that it remains proportionate and targeted.

Subject to the appropriate public consultations, amendments are being considered to a number of aspects of implementation.

The Review suggests a need to ensure that regulatory authorities have an effective cost recovery mechanism in place and that both OESs/RDSPs and Competent Authorities can make use of a robust but simplified system for appeals. To drive change, a clearer and more effective enforcement regime is needed, achieved by refining the current provisions around notices, penalties, and thresholds.

There is also work planned to explore the possibility of amending incident thresholds, and ensuring designation thresholds are fit for purpose where it has been identified that improvements could be made in this area.

Finally, the Regulations must remain flexible and able to adapt to the constantly-changing circumstances; measures to allow for this must be included in the current regime, so that they remain relevant, targeted, and efficient, and to enable the UK to go beyond the limitations of the Directive where there is a need to do so. Further work will also be taken forward on other key policy priorities identified during the course of the review, looking beyond the scope of the original Directive. For example, regarding reducing risks posed by insecure supply chains, the Government will look both at what additional steps can be taken within the policy framework of the NIS Regulations to consider where there is a case for further intervention to reduce these risks at scale.

Title: The Network and Information Systems Regulations 2018	Post Implementation Review
PIR No:	**Date:** 28/02/2020
Original IA/RPC No: RPC-4066(2)-DCMS	**Type of regulation:** EU
Lead department or agency: Department for Digital, Culture, Media & Sport	**Type of review:** Statutory
Other departments or agencies: BEIS, Cabinet Office, DfT, DHSC, Defra, National Cyber Security Centre, and HMT	**Date measure came into force:** 10/05/2018
	Recommendation: Retain and amend
Contact for enquiries: Stephanie Hedges (0207 211 6374, stephanie.hedges@culture.gov.uk)	**RPC Opinion:** Fit for purpose

Questions

1. What were the policy objectives of the measure?

The Network and Information Systems Regulations aim to improve the security of network and information systems critical to the provision of essential services and certain digital services, which if disrupted, could cause significant economic and social harm. The Regulations apply to Operators of Essential Services in the transport, energy, water, health, and digital infrastructure sectors, and to relevant Digital Service Providers (cloud computing services, online marketplaces, and online search engines).

2. What evidence has informed the PIR?

DCMS conducted online surveys of the organisations in scope of the Regulations. Participation was voluntary. There was a response rate of 23%, with responses submitted from a range of organisations in different geographic regions, sizes and sectors. The surveys were open for six weeks, and produced both quantitative and qualitative data. Regulatory authorities also provided formal feedback to the review, as did other government stakeholders (Cabinet Office and NCSC).

3. To what extent have the policy objectives been achieved?

As the statutory review period for the NIS Regulations is only two years, it is not yet possible to assess the long-term post-implementation impacts, as security improvements take time to deliver. In order to assess the effectiveness of the Regulations to date, DCMS developed a range of indicators of initial progress against the key policy objectives, and measured the extent to which these indicators of progress had been achieved. Data collected indicates that organisations in scope are taking steps to improve the security of their network and information systems following the introduction of the NIS Regulations, which we expect to lead to greater resilience and reduction in the number and impact of incidents in the longer term.

Sign-off for Post Implementation Review: Chief economist/Head of Analysis and Minister

I have read the PIR and I am satisfied that it represents a fair and proportionate assessment of the impact of the measure.

Signed: Matt Warman MP, Minister for Digital Infrastructure Date: 28/02/2020

Further information sheet

Please provide additional evidence in subsequent sheets, as required.

Questions

4. What were the original assumptions?

The NIS Impact Assessment sets out the costs that were expected to fall on organisations in scope (familiarisation costs, additional security spending, incident reporting, regulators' costs, and responding to enforcement activities) as well as costs incurred by Government relating to regulatory institutions and support functions. The expected benefit of the Regulations was improvement in security, and a consequent reduction of risks posed to the availability and resilience of essential services relying on networks and information systems. This in turn improves the safety and security of the critical services UK citizens rely on and benefits the UK's economic prosperity.

5. Were there any unintended consequences?

There is very limited evidence of any unintended consequences. A small proportion of organisations who responded to the survey reported incurring costs not explicitly set out in the Impact Assessment, for example reporting more time invested in attending meetings with regulators and agencies. Some regulatory authorities also reported unexpected benefits, for example increased collaboration between regulatory authorities and the sharing of best practice. However evidence in this area is very limited at this stage of the implementation; this can be tested again in future PIRs.

6. Has the evidence identified any opportunities for reducing the burden on business?

Some regulatory authorities believe that designation thresholds are set too low, bringing too many businesses into scope of the Regulations, whereas other Competent Authorities consider these to be broadly at the right level. The Department will consult further on this issue, and will take appropriate steps in order to ensure that designation thresholds are set at the right level for individual sectors.

7. For EU measures, how does the UK's implementation compare with that in other EU member states in terms of costs to business?

All Member States transposed the Directive differently, and the UK's approach was to minimise costs to businesses where possible whilst remaining within the confines of the Directive, and maintaining other existing sector specific legislation where applicable, if it was at least equivalent to the Directive. This translated into relatively fewer sectors in scope of NIS in the UK. On other aspects, such as penalties, the UK transposition included higher penalties than the EU average, but only as a civil contravention (i.e. cannot be criminally prosecuted) and does not include personal liability; furthermore penalties would only be issued as a last resort. Overall, it is too early to judge the UK's transposition in terms of costs to business compared to other EU Member States, as the NIS regulatory framework across the EU is still nascent.

FULL REPORT

Post Implementation Review of the Network and Information Systems Regulation 2018

1) Scope of this review

a) Statutory Requirements

This post-implementation review ('PIR') of the Network and Information Systems (NIS) Regulations 2018 is a statutory requirement, set out in Regulation 25 of the NIS Regulations.

Regulation 25 also states that, in accordance with Section 30(3) of the Small Business, Enterprise and Employment Act 2015, a review carried out under this regulation must, so far as is reasonable, have regard to how the 2016 Directive is implemented in other Member States.

It also requires that, in accordance with Section 30(4) of the Small Business, Enterprise and Employment Act 2015, the review published under this regulation must, in particular:

1) set out the objectives intended to be achieved by the regulatory provision;
2) assess the extent to which those objectives are achieved;
3) assess whether those objectives remain appropriate; and
4) if those objectives remain appropriate, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision.

b) Adhering to Guidance

Following the approach outlined in the Department for Business, Energy & Industrial Strategy's 'Principles of Best Practice' for producing PIRs, this PIR will answer the following questions:

1. To what extent is the existing regulation working?
2. Is government intervention still required?
3. Is the existing form of government regulation still the most appropriate approach?
4. If this regulation is still required what refinements could be made? If this regulation is not required, but government intervention in some form is, what other regulation or alternatives to regulation would be appropriate?

As the NIS Regulations are EU derived, the following additional issues are considered:

1. The impacts on UK based businesses relative to other European competitors, to ensure UK businesses are not put at a competitive disadvantage.
2. Improving transposition in the UK.

2) The objectives and intended outcomes of the Regulations

a) Policy background: implementation of the NIS Regulations

The Regulations set out the legal measures required to boost the overall level of security of network and information systems that are critical for the provision of essential services and certain digital services. The policy implementation of the NIS Regulations was strongly influenced by the National Cyber Security Strategy, which also acts as the official NIS Strategy, as required by the Regulations and the Directive.

Authorities involved in implementation

The implementation and enforcement of the NIS Regulations is the responsibility of designated Competent Authorities. Competent Authorities are responsible for designating OES, the monitoring and oversight of NIS implementation in their sector, and have sole authority and responsibility for all regulatory decisions they make in implementing the NIS Regulations. Competent Authorities are designated in the NIS Regulations[1] under Schedule 1.

Under the Regulations, the National Cyber Security Centre (NCSC), a part of the Government Communications Headquarters, has been designated as the UK's Single Point of Contact (SPOC) for incident reporting and as the Cyber Security Incident Response Team (CSIRT).

The Department for Digital, Culture, Media and Sport (DCMS) is the responsible department for the overall development, coordination, and delivery of the NIS Regulations policy, working alongside other government departments, the devolved administrations, and Competent Authorities.

Identifying organisations in scope

To ensure that only appropriate organisations were captured within the scope of the Regulations, thresholds were set to define which organisations would be designated as operators of essential services. These are set out in Schedule 2 to the Regulations. If an organisation is not captured by the thresholds, but does provide an essential service within scope of the Regulations as described in the legislation, then Competent Authorities may specifically designate that organisation under Regulation 8(3). RDSPs must register if they fulfil the requirements. Small and micro sized RDSPs are excluded from the remit of the NIS

[1] The UK's Competent Authorities are: the Secretaries of State for Business, Energy, and Industrial Strategy; Environment, Food, and Rural Affairs; Transport; Health and Social Care; Scottish Ministers; Welsh Ministers; Department of Finance, Northern Ireland; Ofgem (jointly with BEIS); Ofcom; Civil Aviation Authority; Drinking Water Quality Regulator for Scotland; and the Information Commissioner's Office.

Regulations. It was envisaged during the development of the designation thresholds that very few small businesses would be in scope as OES.

The Impact Assessment estimated that 611 organisations would be brought into scope of the Regulations: 432 OESs and 179 RDSPs.[2] Competent Authority submissions to DCMS for the Review indicated that a total of 610 organisations had been designated: 481 OESs and 129 RDSPs.

Responsibilities of OES, RDSPs, and Competent Authorities

OESs and RDSPs have a duty to notify their designated Competent Authority about any incident which has an adverse effect on the security of the network and information systems used to provide their essential services, according to criteria set out in incident reporting thresholds. For OES, these are set by each Competent Authority in guidance, and for RDSPs, this is set in the relevant Implementing Regulation.[3] Factors considered when judging the severity of an incident include the number of users affected by the disruption of this essential service, the duration of the incident and the geographical area affected. Information about an incident which meets or exceeds the reporting thresholds should be provided to Competent Authorities no later than 72 hours after the incident initially occurred.

The Regulations outline enforcement measures available to Competent Authorities when taking action against OESs and RDSPs, including information and enforcement notices. Penalties can be issued to service providers as a last resort if an OES or RDSP does not comply with the enforcement notice, or fails to take appropriate steps to rectify that problem following interventions from the Competent Authority. There are four levels of bandings which can be applied to an OES or RDSP under a penalty notice.[4] They range from fines of up to £1 million for minor contraventions which do not qualify as a NIS incident to a maximum of £17 million for extreme incidents which cause an immediate threat to life or significantly impact the UK economy.

Further information regarding the responsibilities of the Competent Authorities and the enforcement regime available in the UK is available in the Guidance to Competent Authorities, available on the official gov.uk website.

The NIS Regulations require OESs and RDSPs to take appropriate and proportionate measures to ensure the security of the network and information systems used to provide their essential services. It is for Competent Authorities to set out, through guidance, what defines appropriate and proportionate measures. In order to assist Competent Authorities to do this, the NCSC, as the relevant technical authority in the UK, has created a set of 14 cyber security principles, reflecting internationally-recognised cyber security good practice and defining recommended outcomes for OES to achieve in relation to the security of their systems. These principles form the basis of a Cyber Assessment Framework (CAF), incorporating indicators of good practice. Determinations on acceptable levels of cyber security can be made by Competent Authorities through the use of the CAF or an equivalent

[2] DCMS, NIS Regulations: Impact Assessment (2018)
[3] Commission Implementing Regulation (EU) 2018/151
[4] Network and Information Systems Regulations 2018, s 18(6).

tool, along with comprehensive guidance. Competent Authorities have been encouraged to use the CAF to set a common framework for all OES. The ICO has produced similar advice for RDSPs.

b) Objectives and intended outcomes

As set out in the original Impact Assessment and the public consultation of August 2017, network and information systems play a vital role in society. The overarching objective of the NIS Regulations is to improve the security of network and information systems critical to the provision of services which if disrupted, could cause significant economic and social harm. The Regulations aim to achieve this by ensuring that there is a culture of security across all sectors in scope, and as set out above, organisations are required to take appropriate and proportionate security measures and must notify NIS-specific incidents to relevant authorities.

The Impact Assessment noted that the key benefit of the Regulations was expected to be improvements in security that lead to a reduction in the risks posed to essential services relying on networks and information systems. It was envisaged that this would be achieved from both a reduction in the number of incidents that have significant disruptive effects, and by a reduction in the impact where appropriate incident response plans are put in place.

The Impact Assessment set out that the envisaged reduction in incidents and impact would be a benefit for the companies controlling the networks, other organisations operating on the network, and the wider economy where breaches and other incidents would otherwise disrupt everyday activity. This in turn would benefit the UK's economic prosperity as we rely on these services to support economic output.

The requirement to complete a PIR within two years of the Regulations being introduced was designed to precede the Commission's requirement to review implementation by May 2021 (Article 23(2) of the NIS Directive). Given the short time frame since the Regulations came into force, it is too early in the implementation to judge whether the full longer term benefits have been realised. Security investments and improvements take time to be implemented and effect change at this level.

However, at this two year point, we have developed a number of indicators of initial progress against the intended objectives outlined above which we tested through the surveys, to understand whether organisations are engaging with the Regulations and making improvements in areas which we would expect to lead to improved security outcomes, and a reduction in incidents in the longer term. Future PIRs will aim to look at the longer term impact of the Regulations; for example repeating the survey methodology used in this PIR should enable DCMS to look at whether a trend of longer term, sustained improvement is emerging, and in addition, we anticipate that more data should be available regarding the security improvements organisations have made in practice, providing an additional source of evidence to draw on in addition to the views of regulatory authorities and organisations in scope.

3) Assessment of proportionality for level of evidence sought

DCMS followed the framework set out in PIR guidance to determine the level of evidence and resourcing appropriate to this PIR, and assessed a medium resource approach as being proportionate to the scale of the policy and the length of time the Regulations have been in force, and therefore what is possible to measure at this stage. As the Regulations have only been in place for two years there was a lack of established data sources to provide evidence of the impact of the Regulations, therefore DCMS opted to carry out bespoke evidence gathering projects in order to gather information on the outcomes, costs and benefits to date.

The evidence gathering products set out in the following section were designed to answer the key research questions posed by both Regulation 25 and PIR guidance, as far as is possible at this early stage in the implementation of the Regulations. The products were developed, and analysis was carried out in-house by DCMS. All OESs and RDSPs in scope were given the opportunity to take part in the research. Our approach ensured that all stakeholders consulted were only asked to complete one survey or report, in order to minimise the burden to organisations of input into the PIR and ensure the input required was proportionate.

In addition, the approach to evidence gathering for this PIR was designed to be appropriate and proportionate to the length of time the Regulations have been in force. Due to the short length of time the Regulations have been in force, the evidence collected in this PIR focuses on the experiences of organisations and Competent Authorities in implementing the Regulations and initial security changes that have been made.

By the next PIR, due in 2022, more detailed data on security improvements should be available and we expect it will be possible for the Department to examine in more detail whether outcomes reflected in this PIR have been sustained and are translating into longer term impact, and achievement of the full benefits outlined in the original Impact Assessment.

In order to do this, DCMS intends to repeat the survey methodology used in this PIR to look at whether a trend of sustained long-term improvement is emerging. For example, future surveys could again go out to all OES and RDSPs (including those who answered the survey for this PIR) in order to gain as wide a variety of responses as possible regarding size, sector, and geographic regions. Where relevant, new questions would be included on elements of implementation highlighted for further consideration in this PIR and the surveys could remain open for longer in order to encourage increased participation in future reviews.

Building on this PIR, DCMS also intends to carry out a more detailed qualitative phase in the next PIR to understand the impact the Regulations have had in more detail than has been possible for this PIR, as well as drawing on any additional data on security improvements which we anticipate will be available at this later stage in the implementation of the Regulations.

4) Evidence collection and methodology

The Department undertook primary research to understand the initial impact that the Regulations have had since implementation, as well as examining implementation from a process perspective. After discussions with Competent Authorities, the Regulatory Policy Committee and other key cross Government stakeholders, the Department decided that due to the nature of the topic a secure online survey was the most appropriate research tool to use in order to encourage OES and RDSP participation.

DCMS then collaborated with key stakeholders to scope and design two surveys. Survey one focused on OESs, while survey two was distributed to RDSPs. Questions in each survey were tailored to their respective audience and reflected the policy areas identified in the original Impact Assessment and following policy scoping workshops with cross-Government stakeholders.

There was a mix of quantitative questions with multiple-choice answers and qualitative questions with the opportunity for free text responses. Please see Annexes A and B for further details regarding the questions that were included in the OES and RDSP surveys. It should be noted that the RPC's new innovation test was introduced after the surveys were designed, and therefore questions addressing this were not included; the innovation test will be designed into evidence gathering in future PIRs.

The surveys were distributed to the Competent Authorities who then shared them with the OESs or RDSPs that belong to their sector. All OESs and RDSPs had the opportunity to respond to the survey. Participation in the survey was voluntary and OES and RDSPs were given six weeks to respond and were provided with contact information in case they had any queries. Only DCMS analysts could see the individual responses to the survey that were submitted.

A pre-election period occurred during the fieldwork phase of the research, and limits on Civil Service public engagements during the pre-election period meant that the Competent Authorities were unable to contact OESs and RDSPs to remind them to complete the survey; this could have potentially affected the response rate. However, the Department received a positive response rate with 117 OESs responding and 21 responses from RDSPs. This is a response rate of 23%.[5] All OES and RDSPs were given the opportunity to complete the survey, and consequently we believe this is a robust basis to draw conclusions about the impact of the Regulations to date. We cannot guarantee that the surveys are representative as the survey was open to all OES and RDSPs to complete rather than simply a representative sample of them. However, the survey results provide the most up to data cost data currently available, and are therefore used to calculate the cost to organisations in scope of the Regulations.

[5] This response rate was based on the assumption that the Competent Authorities currently regulate a total of 610 OESs/RDSPs based on Competent Authority submissions to DCMS. The Impact Assessment estimated that 611 OESs/RDSPs would be in scope of the Regulations. DCMS, NIS Regulations: Impact Assessment (2018).

Responses submitted from OESs and RDSPs covered a range of different geographic regions, sizes and sectors.[6] It is important to note that there are statutory differences in the obligations of OES and RDSPs, and they are subject to different regimes, which may explain some of the differences in the responses exhibited by these two categories. Also, since there are no small RDSPs in scope of the Regulations, the small organisations identified in the table below are both OESs.

Table 1: Number of responses by size of organisation

Size of organisation[7]	Number of OESs and RDSPs that responded
Small	2
Medium	10
Large	122
Unknown[8]	4
Total	**138**

Analysts within DCMS undertook both quantitative and qualitative analysis of both surveys. The two surveys were analysed separately with a qualitative coding framework designed for both. These coding frameworks and thematic analysis allowed the free text responses in both surveys to be analysed and key themes to be identified. Closed questions in each of the surveys were analysed using descriptive statistics to enable findings and conclusions to be drawn from the research. The analysis was quality assured following departmental procedures and the findings have been incorporated into this PIR.

DCMS also planned a second phase of research, consisting of qualitative interviews with approximately 40 OESs and RDSPs. A topic guide was developed which was designed to explore some of the themes of the PIR in more depth and detail, and included questions which would have addressed the RPC's new innovation test. For this PIR, DCMS were unable to start the qualitative process earlier, as this would have meant beginning research when the Regulations had been in force for little over a year; this is likely to have been too short a time for any meaningful outcomes to have been felt by organisations. Qualitative views were still gathered as part of the online surveys, Competent Authorities' reports and in regulatory policy workshops, but future PIRs will further explore the possibility of including additional qualitative interviews with OESs and RDSPs.

To fully understand the impact that the Regulations have had to date, DCMS also commissioned each Competent Authority and other key Government stakeholders to

[6] Responses were received all sectors in scope of the Regulations: health, water, digital infrastructure, transport, energy and RDSPs.
[7] For definitions of size see question 3 and 4 in Annex A (OES survey), and question 2 in Annex B (RDSP survey).
[8] Unknown refers to respondents that chose not to provide us with their organisation's size.

complete a report in order to gather their perspectives as well as industry. The Competent Authority report asked each regulatory authority a series of open and closed questions. This included questions regarding the costs and the benefits that they feel have been realised since the introduction of the Regulations for both themselves as the Competent Authorities and sought their views on the cost and benefits to the organisations they regulate as well. The Competent Authorities were also asked questions regarding the effectiveness of the implementation of the Regulations.[9]

All Competent Authorities submitted a response to DCMS, their responses were in turn analysed and have informed this PIR. They were also invited to policy workshops with DCMS which discussed key policy issues such as the existing appeals mechanism and the enforcement regime (including the current penalty regime), which have an impact on the ability of Competent Authorities and organisations in scope to effectively implement the Regulations. Within these fora, the Competent Authorities, based on their collective regulatory experience, have raised a number of aspects in relation to the improvement of the NIS regime, in order to make it more effective. The outcomes and findings of these discussions have informed the findings outlined in this PIR.

DCMS also undertook desk research using publicly available information to understand how EU Member States have implemented the NIS Directive, and how these differ from the UK's approach. Findings from this literature review have been incorporated into this PIR.

[9] See Annex C for the questions asked in the Competent Authority report.

5) Are the Regulations working?

How effective are the Regulations in meeting regulatory objectives and outcomes?

There is initial evidence to suggest that advancements are being made as a result of the NIS Regulations, which we expect to lead to a longer-term improvement in the security of network and information systems, raising their resilience. As the statutory review period for the NIS Regulations is only two years, there is not sufficient qualitative and quantitative data to assess the long-term impacts. There is a degree of variation across Competent Authorities, some of whom are at the initial stages of implementation; updating their lists of OES in scope in their sectors, assessing OES security levels, and developing improvement plans which will take time to fully implement. There is, however, evidence as set out in the following sections to indicate that the Regulations have driven improvements in a range of areas in the short-term, whilst showing promise for long-term developments in others.

As this Review will be establishing the baseline for future assessments, subsequent PIRs will look at the long-term impacts of the NIS Regulations, in addition to the shorter term outcomes that will be explored in this document. DCMS's assessment is that this two year model of review is preferred at the present time, as it allows the Government to monitor implementation closely in the initial phases of implementation. Following the next PIR in 2022, which will mark a total of four years since the establishment of the Regulations, Government should move to a more standard 5-year review cycle, pending consultations, to ensure that monitoring the Regulations does not become a burden on business or Government. However, regulatory authorities will still regularly monitor progress of essential service providers, through the use of the CAF and other tools.

Security practices prior to the NIS Regulations

In developing a methodology to measure the impact of the Regulations to date, DCMS has looked at how organisations in scope approached the security of network and information systems before the introduction of the Regulations. This was to inform our assessment of whether the required standards would be likely to be reached at pace without regulatory intervention. All RDSPs and 99% of OESs that took part in the quantitative analysis reported taking some action to improve the security of their network and information systems before the NIS Regulations came into force.[10] Similarly, the majority of organisations (100% of RDSPs and 90% OESs) had processes and procedures in place for recovery from a security incident relating to their network and information systems.[11]

The 2018 NIS Regulations Impact Assessment envisaged that many organisations in scope would already be subject to a number of existing regulations and requirements.[12] The survey found that 83% of OES and 89% of RDSPs who responded cited complying with the General Data Protection Regulation (GDPR) as a reason for taking action to improve network and

[10] Base: 18 RDSPs and 109 OES
[11] Base: 111 OESs and 18 RDSPs
[12] DCMS, NIS Regulations: Impact Assessment (2018), pp. 13-18

information systems security prior to the introduction of the NIS Regulations. Further key drivers of action (prior to the NIS Regulations) included maintaining business continuity, protecting critical systems, and avoiding reputational damage. RDSPs were more likely to cite customer or supplier requirements and protecting intellectual property as a spur for action than OESs, while a greater proportion of OESs than RDSPs took action in response to industry guidance.[13] Many Competent Authorities also reported being in contact with organisations in scope in their sector prior to the introduction of the Regulations; many of the sectors in scope were already regulated by sector specific regulators from other perspectives, such as safety.

As the above indicates that OESs and RDSPs were motivated to act prior to the introduction of the Regulations (as stated in in their responses), it is reasonable to assume that these factors have continued to have an impact on security decisions taken by OESs and RDSPs since the introduction of the Regulations. It is also reasonable to assume that they would have continued to have an impact on improving network and information systems security had the Regulations not been introduced.

However, while the data suggests that organisations in scope were already taking action in this area, it also indicates that the Regulations are driving improvements, at a faster rate, which we would expect to lead to improved security outcomes. Furthermore, a majority of Competent Authorities reported that in their view, if the Regulations no longer existed, improvement in the security of network and information systems among OESs and RDSPs would still continue, but at a slower pace.[14] In view of societal reliance on the sectors in scope of the Regulations, and the substantial cyber threats posed to these sectors, there is a clear case for urgent improvements to their security posture.

Key outcomes

Regarding specific areas where PIR survey data suggests improvements have been made, although there is variation between sectors according to some metrics, the evidence indicates that many organisations are putting in place measures which we would expect to lead to improved security outcomes as intended by the Regulations, including:

OESs

- Several Competent Authorities report more interest, support and investment from OES boards in the security of networks and information systems since the introduction of the Regulations.[15] Correspondingly, 60% of OESs identify the

[13] 68% of OES who responded to the question took action in response to industry guidance compared to 50% of RDSPs who responded to the question. This is based on 113 OES and 18 RDSPs

[14] Feedback provided to the Department in submissions by Competent Authorities to the Review.

[15] Part of the barrier to investing in cyber risk mitigation lies with cyber security being viewed as an IT-specific issue and an objective in itself, rather than an enabler of business continuity and operational resilience. However, cyber security is an enabler of the everyday operations of most businesses today. Seen as such, cyber security becomes a business management challenge, which requires a strategic and whole-of-organisation approach. Boards and senior leaders therefore play a critical role in determining how cyber security is integrated across all business operations through informed decision making and better targeted investments. DCMS, Cyber Security Incentives and Regulation Review 2020: Call for Evidence

Regulations as responsible for increasing the prioritisation of security at a senior management level within their organisation.[16] One large OES reported that system security is now discussed as a distinct topic at a higher level within the business, while another OES referred to the Regulations as having 'brought cyber security to the fore at board level'.

- The majority of OESs report that they have introduced new [security] policies or processes (79%) or updated or strengthened existing policies or processes (69%).[17] Of those organisations that answered that they had not made any changes to their governance policies or processes as a result of the NIS Regulations, the main reason for OESs was that they already had appropriate measures in place so did not need to make further changes.

- 61% of OESs report strengthening processes and/or procedures for recovery from a security incident as a result of the NIS Regulations.[18] Of those OESs who did not report strengthening their processes, several reported that their processes already in place did not require strengthening as a result of the implementation of NIS.

- Of those OESs that use the Cyber Assessment Framework (CAF), 56% found the CAF extremely or very useful for managing risk to the security of their organisation's network and information systems.[19]

- The majority of OESs have made additional security investments into the security of their network and information systems for delivering their essential services, and 62% plan to make additional security investments.[20]

RDSPs

- A majority of the RDSPs who responded to the survey reported a positive impact on security standards within their organisations and understanding of key assets and critical systems as a result of applying the NIS security principles.[21]

- 47% of RDSPs reported they have updated or strengthened security governance processes, and 18% of RDSPs reported they intend to update or strengthen security governance processes as a result of the introduction of the Regulations.[22] Of those organisations that answered that they had not made any changes to their governance policies or processes as a result of the NIS Regulations, the main reason RDSPs

[16] A majority of OESs who responded to the survey. Base: 111 OESs
[17] Base: 67 OESs. Security policies that are fit for purpose and easy reporting processes will all help to mitigate cyber risks. NCSC, Cyber Security Toolkit for Boards: Helping board members to get to grips with cyber security.
[18] Base: 111 OESs
[19] Base: 81 OESs
[20] Base: 111 OESs
[21] Base: 14 RDSPs
[22] Base: 17 RDSPs

cited was that they already had appropriate measures in place so did not need to make further changes.

- Fewer RDSPs than OES reported improvements to senior level prioritisation as a result of the NIS Regulations, and fewer RDSPs than OES reported introducing new incident management processes, or strengthening existing processes. In qualitative responses, a popular reason given by RDSPs for the Regulations not having increased senior level prioritisation of security was that security was already a priority for other reasons.

A number of new measures and powers were included through these Regulations, including monitoring and enforcement powers, a penalty regime, and further guidance, which have likely supported this increased prioritisation of the security of network and information systems. One Competent Authority suggests that without the Regulations OESs may have chosen to defer security improvements, while others identify compliance as driving momentum and discussion of this area.[23]

Supporting organisations to implement the Regulations

In addition to looking at the key measurable outcomes to date, the Review assessed implementation, including looking at the effectiveness of key tools for supporting organisations in implementing the Regulations. The review looked at the effectiveness of the CAF; for those who use it, the CAF has been a useful tool for OES to identify areas that need attention and improvement. Of those OESs that do use the CAF, 56% found the CAF to be extremely or very useful, with one OES reporting that it helped them to prioritise workstreams.[24]

As OESs produce regular CAF returns showing progress against security metrics it should become a useful tool in which to track the security and resilience of an OES over time. This will be useful to the OESs themselves, their Competent Authority, and the NCSC. It has not yet been possible to track actual improvements in security through analysis of CAF returns in the short time that has elapsed since the Regulations have come into force, but future post implementation reviews could be informed by further data in this area.

Furthermore, guidance and support from Competent Authorities on implementing and complying with the Regulations may have helped OESs implement improvements to the security of their network and information systems. Almost all organisations who responded to the survey knew where to find guidance on NIS implementation and compliance (96% OESs and 94% RDSPs).[25] While this varied by sector, overall 60% of OESs and 71% of RDSPs felt that they had been given appropriate guidance and support from their Competent Authorities, with one OES describing the guidance as ‘clear and comprehensive’.[26] Other OESs suggest

[23] Feedback provided to the Department in submissions by Competent Authorities to the review (q.6 in CA Report template, which can be found at Annex C).
[24] Base: 81 OESs. All organisations in scope of the Regulations use the CAF except from those regulated by DHSC, Ofcom and the ICO.
[25] Base: 113 OESs and 18 RDSPs
[26] Base: 111 OESs and 17 RDSPs

that more defined guidance or more educational documentation - which could explain to managers or staff their responsibilities and the penalties for non compliance - would further assist with the implementation of the NIS Regulations.

Enforcement

As noted above, some Competent Authorities reported that in their view, general oversight and enforcement powers have helped ensure that the security of network and information systems has been prioritised and improved more than would otherwise have been the case. While this feedback suggests that the introduction of a regulatory framework is incentivising improvements, the survey also aimed to test whether the enforcement element of the Regulations was a specific driver of improvements. Only 38% of OESs and 27% of RDSPs reported that the enforcement regime has led them to make improvements to the resilience of their essential or digital services. A majority said that the enforcement regime had not driven improvements.[27] As other survey data indicates that security improvements are being made in many cases, this may mean that the existence of the enforcement regime within the Regulations is not the key factor driving change, although survey data does not provide additional insight to explain this result.

However, at this early stage in the implementation of the Regulations, it is important to underline that little enforcement action has been taken yet by Competent Authorities, and as such it is too early to assess the impact of the enforcement regime specifically. It would be useful for attitudes to the enforcement regime to be tested again in future PIRs. Previous experience of Competent Authorities as regulators (where applicable) as well as precedents have also been considered, and while the majority of Competent Authorities have indicated that overall, existing oversight and enforcement powers have helped prioritisation and some improvements, there is evidence that some Competent Authorities would be more confident if the NIS regulatory and compliance responsibilities were given a firmer statutory basis.

Despite not reporting the enforcement regime to be a key driver of improvements, a high proportion of OESs (81%) and RDSPs (86%) agree that the current enforcement regime is proportionate to the risk of disruption to essential and digital services in the event of an incident.[28] Among the OESs that disagreed with the question (19%), a number were unsure and felt that the enforcement regime was unclear. Sections ten and eleven contain further consideration of the effectiveness of the existing enforcement regime, alongside these high level findings.

Summary: Outcomes observed to date

The evidence gathered suggests that organisations in scope are taking measures to ensure the security of their networks and information systems as a result of the

[27] 57% of OESs and 73% of RDSPs said that it had not led to improvements. Base: 99 OES and 15 RDSPs

[28] Base: 98 OESs and 14 RDSPs.

introduction of the Regulations, in line with the objectives. As such, progress is being made towards achieving the intended outcome of the Regulations.

However, there is still room for further improvement. Initial assessments, submissions from Competent Authorities, and survey data suggest that in many sectors improvement is still required if the security and resilience of networks and information systems is to match the scale of the threat.

The full benefits of the Regulations are unlikely to have been felt in the short period of time since implementation in May 2018, but the evidence suggests that the Regulations are an effective vehicle in driving improvements at pace.

6) Assessment of the actual costs and benefits of the Regulations

a) Costs

The Impact Assessment (IA) identified the costs of implementing the Regulations as split between those falling on businesses and those falling on the government:

- Costs incurred by businesses include (a) familiarisation costs, (b) additional security spending, (c) costs of incidence reporting, (d) Competent Authority costs, including compliance costs, and (e) responding to enforcement activities.
- Costs to government include (a) setting up Computer Security Incident Response Team (CSIRT), single point of contact, and a cooperation group, and, (b) delivering enforcement activities, and international cooperation.

As part of the post implementation review, DCMS has reviewed whether the above costs were incurred, and thus whether the estimated costs were accurate.

Table 2: Summary of costs

Type of cost/benefit	Estimates in IA[29]	Estimate in PIR (average annual costs)	Drivers for change
Familiarisation costs (Year one only)	£406,018	£399,767	Decrease in the estimated hourly wage rates for IT directors.
Cost of incident reporting	£72,921	£2,246	The IA assumed that there would be 1,348 incidents per year. PIR estimates 39 per year.
Additional compliance costs	£237,080	£357,606	Increase in the estimated average number of hours for additional compliance for all OESs equal to those estimated to only be faced by large organisations in the IA.
Additional security costs	£40,605,550	£42,334,251	The PIR estimates used 2019 survey data which asked about NIS related security investment in three areas: internal staff, physical security and external costs.
Competent Authority costs	£4,104,035	£3,625,219	Updated estimates from Competent Authorities on their one off implementation costs, current annual costs and estimated future annual costs.

[29] DCMS, NIS Regulations: Impact Assessment (2018).

Where possible, we have updated cost data assumptions that were made in the IA. As such:

Consistent with the Impact Assessment, the median wage has been used to calculate costs as it is believed to be the most representative wage (it's less skewed by outliers). Overhead charges of 30% have been added to the wages, in accordance with the International Standard Cost Model Manual.[30] Where wage costs have been used to estimate total costs, this may lead to a slight underestimation of impacts, as other non-wage costs components of full labour costs are not taken into account.

For familiarisation costs, additional compliance costs and incident reporting costs, hourly wage rates used in the Impact Assessment have been updated using ONS ASHE revised data (2016-2018). The average annual nominal growth rate in median wages for different occupations has been estimated by taking the average of the difference between 2013 and 2018 ASHE wage data for legal professionals, IT professionals, managers and directors. This has then been used to estimate future wage growth when modelling future costs from 2019 onwards.

For internal staff security costs, which are a component of additional security costs, cost estimates were taken from data provided from survey responses, however this is in 2019 prices. These cost figures were adjusted using the growth rates of the median wage rate for all employees using ASHE revised data for 2016, 2017 and 2018 to estimate these costs in 2016, 2017 and 2018 prices. The future growth rate of wages was then calculated using the same process as described above by taking the average annual growth rate of all employee wages between 2013 and 2018 using revised ASHE figures.

For Competent Authority costs, it has been assumed that wage inflation is the same as the general inflation rate, as Competent Authorities are government departments, agencies, or public sector bodies.

Total costs have been deflated to 2016 prices and a discount rate of 3.5% applied to future costs to account for the time preference of money.

Table 3: Wage inflation

	Hourly wage 2018 ASHE (£)	Hourly wage 2013 ASHE (£)	5 year hourly wage growth rate (%)	Average annual hourly wage growth rate (%)
Legal profession	£26.07	£22.85	12.35%	2.47%
IT professional	£22.00	£20.06	8.82%	1.76%

[30] Standard Cost Model Network, Standard Cost Model Manual: Measuring and reducing administrative burdens for businesses

Corporate managers and directors	£22.58	£20.56	8.95%	1.79%
All employees	£12.71	£11.53	9.28%	1.86%

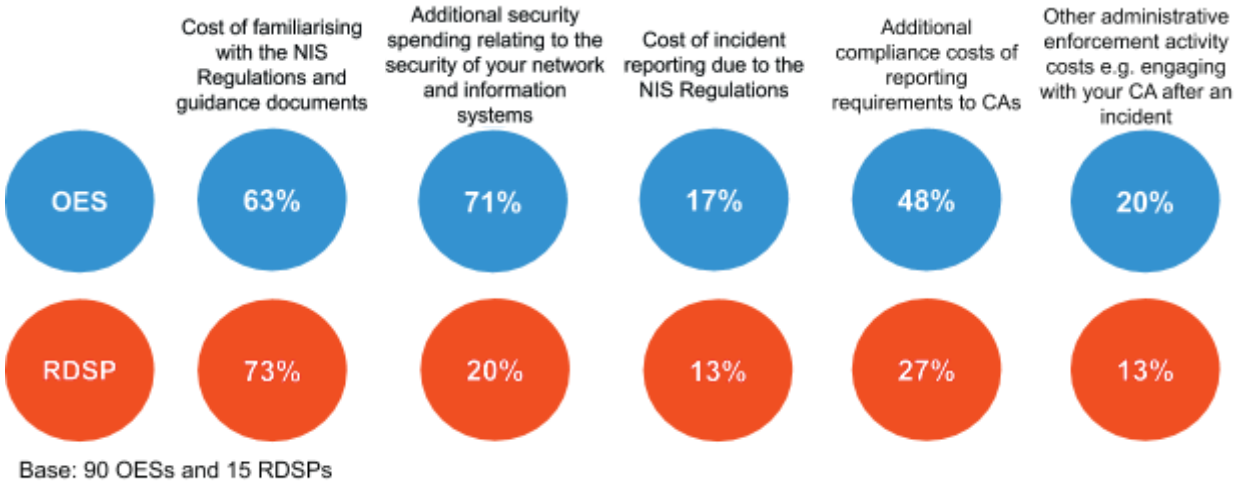
However, there have been some instances where it has not been possible to update the specific cost assumptions made in the Impact Assessment. Where this is the case, this has been indicated.

It is worth noting that many organisations in scope of the Regulations are public sector organisations, largely in the health sector. In view of this, much of the following refers to the impact and costs on 'organisations' - encompassing private and public sector - rather than businesses.

In calculating the direct cost to business, based on consultation with Competent Authorities, we have estimated that approximately 43% of organisations currently in scope of the Regulations are in the public sector. It should also be noted that while costs public sector organisations have incurred have been evaluated in the same way as costs to business throughout, these costs are ultimately borne by the government.

Not all organisations in scope of the Regulations reported incurring the costs as set out in the Impact Assessment, as can be seen in Figure 1, which sets out the percentages of organisations in scope who reported spend in each area.[31]

Figure 1: In the original NIS Impact Assessment, DCMS estimated expected costs to organisations associated with implementing the NIS Regulations. Which of the following costs, if any, has your organisation incurred as a result of the NIS regulations?



Base: 90 OESs and 15 RDSPs

[31] Percentages refer to the number of respondents reporting they had incurred each of the costs.

As set out in the diagram above, the majority of organisations reported incurring familiarisation costs, whereas far fewer reported incurring costs due to incident reporting or other administrative enforcement activity. To understand the costs incurred in more detail, the survey also asked organisations the amount they spent in comparison to the estimates set out in the Impact Assessment. In the Impact Assessment, the Department estimated that the following additional costs would be incurred by organisations in scope of the Regulations:

- **Cost of familiarisation** with the NIS Regulations and guidance documents (£660.19 per organisation);[32]
- **Additional compliance costs** of reporting requirements to Competent Authorities e.g. completing the CAF, or other type of assessment (£80 for a small organisation, £275 for a medium sized organisation, and £549 for a large organisation);[33]
- **Costs of incident reporting** due to the NIS Regulations (£54 per incident).[34]

Overall, only 11% of OESs and 17% of RDSPs agreed with this assessment and that the costs in the Impact Assessment were accurate for their organisations.[35] 21% of OESs and 28% of RDSPs did not agree that these costs were accurate.[36] The majority of organisations (68% of OESs and 56% of RDSPs) were unsure, responding that they did not know, even though organisations reported incurring these types of costs (figure 1).[37] This may be because organisations are unable to identify specific costs incurred as a result of the Regulations from their overall spending on security and compliance.

Of those that disagreed with the additional cost estimates, only 16 OESs and 1 RDSP provided any further information on the actual costs that they incurred as a result of the Regulations. As a result, DCMS has been unable to conduct robust analysis of these responses.

However, of those organisations that did not agree that the estimated costs were accurate and also provided additional information, most responses suggested that the estimates were too low.[38] There was also a wide range of costs reported, indicating that there are many factors (which may be specific to the organisation's needs) that affect additional costs to organisations of implementing the Regulations.

The Impact Assessment estimated that the **cost of familiarisation** with the NIS Regulations and guidance documents would be £660.19 per organisation, using eighteen hours of legal and senior management time.[39] Of those organisations who responded that estimated costs

[32] DCMS, NIS Regulations: Impact Assessment (2018), p.17
[33] Ibid, p.20
[34] Ibid, p.31
[35] Base: 107 OESs and 18 RDSPs
[36] Base: 107 OESs and 18 RDSPs
[37] Base: 107 OESs and 18 RDSPs
[38] Please note this was a qualitative question that asked respondents why they did not agree with the estimates hence why there is no number or percentage associated with the finding.
[39] DCMS, NIS Regulations: Impact Assessment (2018), p.17

were not accurate for their organisation, all but one of the 15 that provided actual costs reported that these were higher.[40]

One organisation reported familiarisation costs in excess of £100,000, requiring more than 100 hours on the process. Several organisations reported requiring over 100 hours for familiarisation, while a few reported requiring 10 hours or fewer.

Due to the small number of responses providing cost information and the wide range of costs reported, it is not possible to robustly assess the cost of familiarisation to organisations in scope. The results appear to suggest that there is a lot of variation in familiarisation costs, even within sectors and organisation size.

Table 4: Familiarisation costs, ONS ASHE 2016 revised figures

	Number of hours for familiarising with legislation	Number of hours for guidance documents	Hourly wage 2016 ASHE revised (£)	Total cost per organisation, incl. overhead charge (30%)
Legal profession	6	6	£25.17	£392.65
Information technology and telecommunication directors	3	3	£33.68	£262.70

Therefore, the estimated number of hours taken for organisations to familiarise with the legislation has remained unchanged. Updating the cost of hourly wages for IT director and legal professional, the one off cost of familiarisation per organisation is estimated to be £655.36 per organisation. It has been assumed that all organisations in scope faced familiarisation costs, despite only 63% and 73% of OESs and RDSPs that responded to this question reporting this cost. This conservative approach has been taken, as it is likely that all organisations faced some familiarisation costs, even if this was assumed to be business as usual. Overall, the total cost of familiarisation was estimated to be £399,767 in 2016 prices. The decrease in costs from the Impact Assessment's estimate is due to the decrease in estimated wage of IT directors from £34.30 per hour from provisional ASHE 2016 estimates to £33.68 per hour.

The Impact Assessment estimated that there would be a total annual **cost of incident reporting** of £2,110, calculated by estimating cost per incident (£54) and multiplying this by the estimated number of incidents likely to be in scope of the Regulations each year (39) on the basis of data provided by the NCSC. The Impact Assessment also estimated, using analysis of data from the 2017 Cyber Security Breaches Survey, a total cost of £71,921 from a maximum of 1348 incidents. The number of reported NIS level incidents has been lower

[40] There were 15 responses giving further information about familiarisation costs.

than expected since the Regulations came into force, which would imply a lower annual cost than estimated.

Of the relatively small number of OESs (8) that provided details on incident reporting costs, estimates varied from hundreds to the low thousands of pounds, with reported time taken from two hours to up to 25 hours. However, it was unclear whether the estimates provided were annual or per incident. It is therefore not possible to assess whether the estimated cost of reporting each incident (£54) was accurate or not, particularly as the number of reported incidents has been lower than expected since the Regulations came into force, which if this continued would affect the cost estimate. In the evidence-gathering process for this PIR, response rates to questions with banded options were better than open questions; future PIRs will use banded options in order to attain more informative data on the cost of incident reporting.

The NIS Regulations require organisations that have experienced an incident meeting the threshold to report this to their Competent Authority within 72 hours of its discovery by filling out an incident notification form. The information organisations are required to report varies by Competent Authority, however, most of this information would normally be gathered as part of a business as usual response to a security incident. Therefore, this estimate is based on the time taken to notify the Competent Authority that an incident has occurred. Any actions taken to respond to the incident have not been included, as this is assumed to be part of business as usual activity. Hence, the estimated time taken to report an incident has remained unchanged: 45 minutes of an IT professional's time to collect and present the information; 45 minutes for legal clearance; and 20 minutes for managers or senior directors to approve the notice.

Updating the incident reporting costs using revised wage rates (ASHE 2016-2018) gives a cost of £54.17 per incident in 2016 prices, which has been inflated annually from 2019 onwards using the wage inflation rates in table 3. The best (and low) estimate of the annual number of NIS incidents (39) has also remained unchanged, despite reported incidents being lower than expected since the introduction of the Regulations. This is because the average number of incidents is difficult to predict and is not dependent on previous year’s data. The best (and low) estimate of the total cost of incident reporting was estimated to be £22,462 over the 10 year appraisal period, in 2016 prices. However, if incident reporting thresholds are adjusted in the future, this may affect the number of incidents meeting the reporting threshold.

Sensitivity analysis was also conducted in line with HMT Green Book guidance using the proportion of organisations that reported having faced incident reporting costs since the introduction of the Regulations in May 2018 (17% of OESs and 13% of RDSPs, figure 1). This was to take into account uncertainty in the future average number of incidents that meet the reporting threshold per year. Assuming that one incident occurred per year, per organisation that reported facing incident reporting costs gives a total of 99 incidents per year. However, it is important to note that some organisations have voluntarily reported incidents to NCSC and their Competent Authority that fall below the reporting threshold, while organisations in some sectors are required to report all incidents as part of other

regulations. Overall, the total high estimate of incident reporting costs due to the introduction of the NIS Regulations is £57,019 over 10 years.

The IA also estimated **additional compliance costs** of reporting requirements to Competent Authorities - such as completing the Cyber Assessment Framework or another type of assessment - as £80 for a small organisation, £275 for a medium sized organisation, and £549 for a large organisation.[41] Of the 11 organisations who reported that estimated costs were not accurate for their organisation and provided further detail of this cost, all reported costs well in excess of the original estimates.[42] It would be useful for this to be further tested and explored in the future.

As initial evidence suggests that additional compliance costs exceeded those estimated in the Impact Assessment, it has been assumed that the average number of hours taken for additional reporting by all OESs is the same as those estimated to be faced only by large OESs in the Impact Assessment.

Similarly to the cost of incident reporting, ONS ASHE data was used for hourly wages between 2016 and 2018, with wage growth rates in table 3 used to estimate wage inflation rates from 2019 onwards.

Table 5: Additional annual compliance costs, ONS ASHE 2016 revised figures

	Hours	Hourly wage 2016 ASHE (£)	Total annual cost per organisation, incl. overhead charge (30%)
Legal profession	10	£25.17	£251.70
Corporate managers and directors	14	£21.30	£298.20

Results of the survey show that 48% of OESs and 27% of RDSPs reported facing additional compliance costs as a result of the introduction of the Regulations (figure 1). Hence, the best estimate has assumed that, in years one and two of the 10 year appraisal period, these proportions of OESs and RDSPs have faced the annual costs, which are detailed in Table 5. However, from year 3 onwards, it has been assumed that all OESs will face this cost due to having to regularly complete the Cyber Assessment Framework (CAF) or similar assessment, while these 27% of RDSPs will continue to face this cost (RDSPs are not required to complete the CAF). This leads to a best cost estimate for additional compliance reporting of £3,576,058 over the 10 year appraisal period, in 2016 prices.

The high estimate of additional reporting costs of £4,653,420 has assumed that all organisations in scope of the Regulations have incurred this cost from year one. This is because not all Competent Authorities use the CAF framework, but instead have

[41] DCMS, NIS Regulations: Impact Assessment (2018), p.20
[42] There were 11 responses giving further information about compliance costs.

incorporated additional reporting requirements into existing reporting tools, which may lead to underreporting of costs. On the other hand, the low estimate of £3,309,059 has assumed that 48% of OESs and 27% of RDSPs incurred these costs in years one and two, but in subsequent years, 100% of OESs and no RDSPs faced these costs.

The Impact Assessment also attempted to estimate the **costs of additional security spending** that would be incurred by organisations due to the introduction of the Regulations, based on responses to the consultation. As the Impact Assessment stated, any additional security spending by individual organisations will vary by the existing measures and technical controls they have in place, and the extent to which they judge additional spending to be appropriate. Nonetheless, the Impact Assessment provided high and low estimates of cyber security spending based on the consultation responses, with additional spending envisaged on measures such as increasing staffing, investing in IT software, additional risk assessments and audits, staff training and testing and monitoring systems.[43] The additional security spending estimated in the Impact Assessment, is shown in the table below.

Table 6: Estimated additional cyber security spending estimates by size and type of organisation[44]

	Small OESs	**Medium OESs**	**Large OESs**	**Medium/Large DSPs**
High estimated additional costs per business	£1,400	£75,000	£200,000	£50,000
Low estimated additional costs per business	£500	£50,000	£100,000	£5,000

In the online surveys, OESs and RDSPs were asked to report on their additional security spending. In order to help respondents answer the question more easily and maximise the response rate, the question divided spending into three categories: internal staff costs; physical security; and external costs. Response options were also banded, due to the commercially sensitive nature of the information, and the probability that organisations were unlikely to know the exact figure.

[43] DCMS, NIS Regulations: Impact Assessment (2018), , p.25
[44] Ibid, p.25

Figure 2: Which areas have you invested in, or plan to invest in, relating to the security of your network and information systems for providing your essential/ digital service(s)?

Base: 111 OESs and 17 RDSPs, respondents could select multiple options

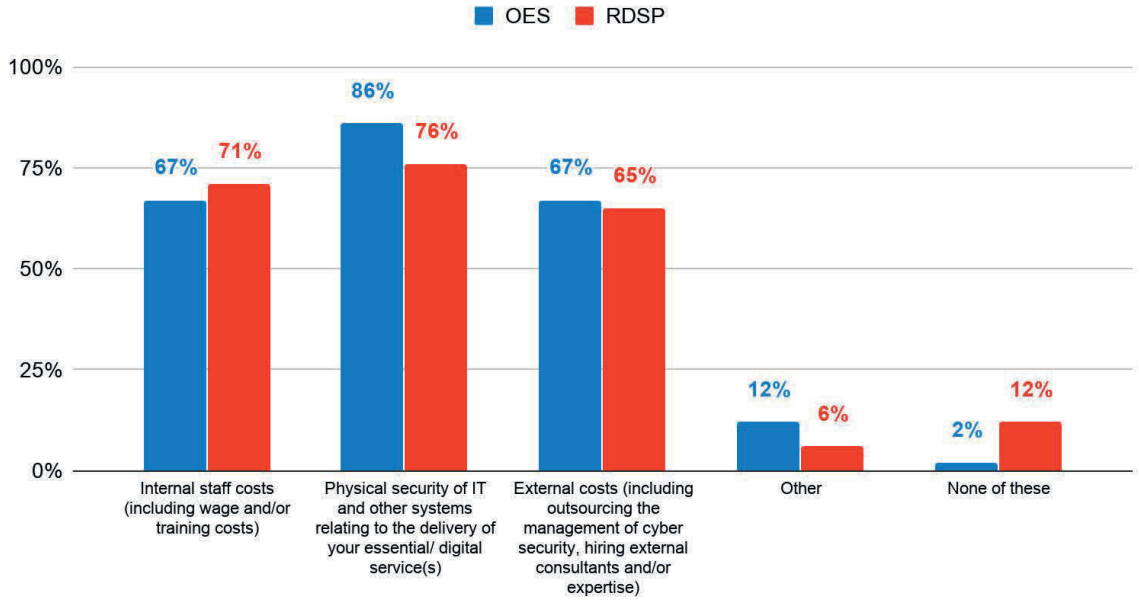


Figure 3: OESs: How much have you invested in the last 12 months, or do you plan to invest in the next 12 months as a result of the introduction of the NIS regulations in additional security measures in the following areas relating to your network and information systems for providing your essential service(s)?

Base: Internal staff costs and Physical security costs: 104 OESs, External costs: 101 OESs

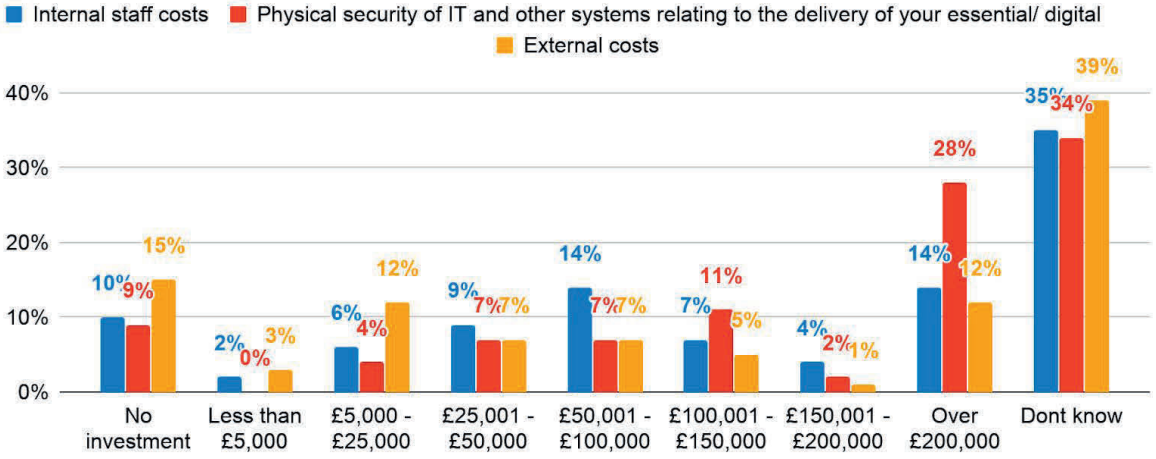
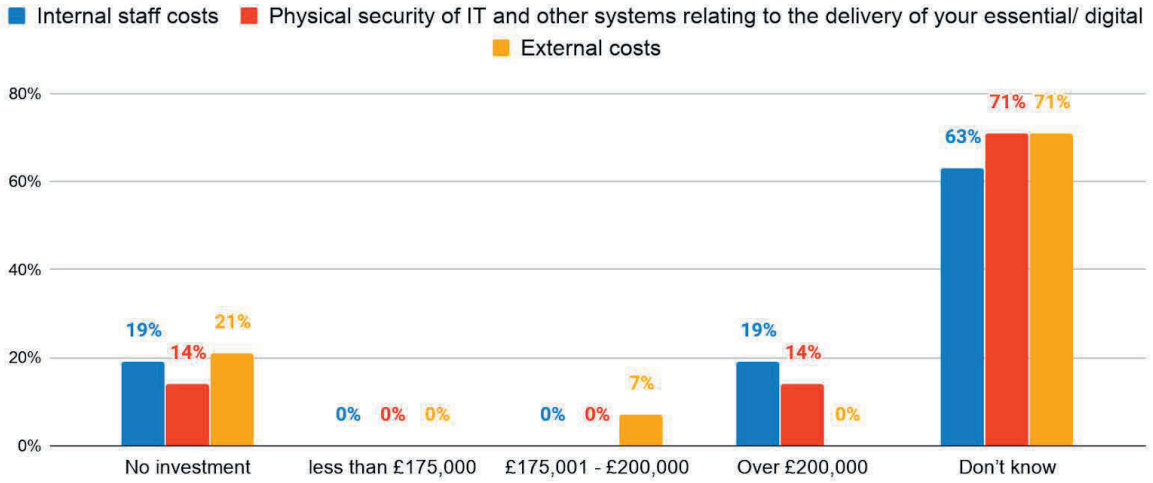


Figure 4: RDSPs: How much have you invested in the last 12 months, or do you plan to invest in the next 12 months as a result of the introduction of the NIS regulations in additional security measures in the following areas relating to your network and information systems for providing your digital service

Base: Internal staff costs: 16 RDSPs, Physical security and External costs: 14 RDSPs



This set of questions has produced some useful and important data on where and how organisations are focusing their security spending, but it also makes it possible to state that a minimum of 39% of large OESs who responded to the survey spent more than the high estimated additional costs per business (£200,000).[45] A minimum of 27% of large RDSPs who responded spent more than the high estimated additional costs per business (£50,000). [46] This was calculated by combining the lower bound of each of the cost brackets that organisations selected for each of the three cost categories.

An estimate of additional security costs has been calculated using the data provided in the survey. Low, middle and high estimates were calculated by taking the low, middle and high values in each of the cost brackets and applied to the proportion of OESs and RDSPs that reported investing in, or planning to invest in, each of the three cost areas (figures 3 and 4). It has been assumed that the distribution of investment reported in the survey is the same across organisations that did not respond to the survey or responded with 'don't know' to this question. Cost distributions were calculated and applied separately for OESs and RDSPs before being aggregated to give a total cost estimate.

It has further been assumed that physical costs are one off costs, while internal staff costs and external costs are ongoing annual costs. This is because it is unlikely that organisations will continue their physical capital investment at a steady annual rate. Internal staff costs have also been adjusted using average wage inflation rates of all employees from 2016-2018 ASHE revised data to deflate the 2019 reported cost figures from the online surveys. The five-year average wage growth rate for all employees was then used to inflate these annual

[45] Base: 97 OESs that responded to the question
[46] Base: 11 RDSPs that responded to the question

internal staff costs from 2019 to the end of the appraisal period. External costs have been assumed to remain constant every year.

The total cost of security investments for OESs and RDSPs over the 10 year appraisal period has been estimated at £423,342,513 in 2016 prices, with high and low estimates of £448,246,281 and £398,440,499 respectively.

Overall, the evidence suggests that there are a wide range of costs incurred as additional security spending across different organisations in scope of the Regulations; as much is clear in figures 2, 3 and 4. As the Impact Assessment points out, any additional security spending by individual organisations will vary by the existing measures and technical controls they have in place, and the extent to which they judge additional spending to be appropriate. While additional expenditure on security measures does not automatically lead to improved security, as it is important to also ensure the investment is targeted in the correct way, it is encouraging that organisations in scope appear to be making significant investments to protect the security of their network and information systems, and expenditure in this area should be viewed as a positive investment.

Although we might expect those organisations who had spent the most on security before the Regulations came into force to have subsequently spent relatively less on additional security - and vice versa - it has not been possible to substantiate this hypothesis with the data we have gathered, as many of these projects or plans for improvement would be delivered over a longer period of time (e.g. installation of a control system), which is longer than this review period. It would be useful for this hypothesis to be tested in future reviews.

The Impact Assessment also identifies **additional administrative costs resulting from enforcement activity** as a possible cost to businesses. Given the uncertainty and lack of detail at this stage about what this activity might have entailed for organisations it was not possible to quantify or monetise the burden to organisations in the Impact Assessment. The PIR has been unable to identify specific costs in relation to enforcement activity as there have been minimal enforcement measures carried out by Competent Authorities during this initial phase of the Regulations. As most Competent Authorities, at the time of writing, are at assessment stage with their OESs and have not pursued a significant amount of enforcement action, it is difficult to make an informed assessment of the levels of enforcement that will be taking place; this question will be best answered in subsequent reviews.

In addition to testing the assumptions and estimates given in the Impact Assessment, the review team also tested whether there were any **unexpected costs** incurred by organisations that were not addressed in the IA. Just 8% of OESs and 14% of RDSPs who responded to the survey reported incurring unexpected costs that were not covered in the original IA.[47] Unexpected costs which organisations incurred included higher implementation costs than were stated in the IA and time invested in attending meetings with Competent Authorities and agencies. Some OESs reported fees from Competent Authorities as an

[47] Base: 97 OESs and 14 RDSPs

unexpected cost, but these costs were clearly stated in the IA (and are addressed more fully below).[48]

In response to the original IA, the Regulatory Policy Committee outlined **other possible costs** that may be incurred by business,[49] which are addressed here in turn:

- Costly interaction between the NIS directive, General Data Protection Regulation (GDPR) and the e-privacy directive. Whilst some OES and RDSPs have cited the GDPR as an additional driver for investment in the security of their network and information systems, no OES or RDSP raised concerns about the cost of interaction between the NIS Regulations in this Review period.

- Establishment costs for regulators. By utilising the experience of existing sectoral regulators where possible to implement regulatory oversight of NIS, this reduced 'establishment costs for sectoral-competent authorities',[50] certainly in comparison with the costs that would be incurred in establishing a new regulator and then passing these costs on to business.

- Increase in revenue of digital service providers from providing security services to essential service providers. There is no specific evidence that there has been an 'increase in revenue of digital service providers from providing security services to essential service providers,' although 67% of OESs have invested in, or plan to invest in external resources in order to secure their network and information systems.[51] This response category included outsourcing the management of cyber security, and hiring external consultants and/or expertise. It is not clear that there is an overlap between this category of external resource and the digital service providers in scope of the Regulations, namely online marketplaces, online search engines, cloud computing services

- Potential disproportionate impact on small businesses. There is no direct evidence that new measures under the NIS Regulations have had a disproportionate impact on small businesses, but there is further work to be done to ensure small businesses are not brought into scope of the Regulations unnecessarily. The IA estimated that there would be just one small or micro business designated as an OES, and small and micro businesses were specifically excluded from being designated as RDSPs. The evidence suggests that this was an underestimation, although due to the nature of the industries in scope it is still considered unlikely that many small businesses have been brought into scope. It is not clear what the overall size of the small business population brought into scope of the Regulations is, but two small organisations completed an online survey as part of the review process. One Competent Authority is also suggesting that designation thresholds should be changed to avoid bringing small businesses into scope. Subsequent sections of the PIR set out how DCMS will address this issue.

[48] DCMS, NIS Regulations: Impact Assessment (2018), p.18.
[49] Ibid, pp.4-5.
[50] Ibid, p.5
[51] Base: 111 OESs

Costs incurred by Competent Authorities

Costs to the government for enforcement activity - the **costs of operating Competent Authorities** - are in some cases being passed on to organisations. The IA included high-level estimates of the (annual) costs of operating Competent Authorities. Where it has been possible to gather equivalent costs actually incurred by Competent Authorities, this has been indicated in Table 5. The figures suggest that in most cases the estimates in the IA were too high.

Competent Authorities also reported on whether they expected their **future costs of operating** to increase. Most Competent Authorities foresee operating costs to increase in the future, as some expect to increase staff capacity and to increase engagement with the organisations they regulate. One Competent Authority notes that as the Regulations and cyber incidents are better understood, there will be improved visibility of the sector, and as a result, may encourage additional incident reporting. This in turn may create additional investigative workstreams (and thus, cost). Where a Competent Authority is passing on operating costs to organisations, increased operating costs will likely lead to increased costs to organisations.

Proposed amendments to cost recovery powers may also increase future costs incurred by organisations. Why these changes are necessary, and how the Department intends to take action to make these changes, is explained in sections ten and eleven of this review.

In addition to operating costs, most Competent Authorities have indicated that they incurred significant **one-off implementation costs.** Only Defra and the ICO previously indicated estimated one-off set up costs of £998,000 and £100,000, respectively in the IA. The ICO have reported that the initial implementation cost was higher, at approximately £103,953, although the Department of Finance Northern Ireland found that their initial implementation cost was lower than their estimates.

Implementing the Regulations has led to **other costs for government:**

- In implementing the NIS Directive the UK was required to designate a single point of contact to act as a liaison on NIS matters within the EU and between different national competent authorities. The single point of contact's core tasks include preparing a summary report of incident notifications and forwarding cross-border incidents to the single points of contact in other Member States. The NCSC is the UK's single point of contact. These requirements will no longer apply following the end of the Transition Period, and the SPOC will have much more flexibility over what it must share internationally whilst remaining the core point of contact for the UK.

- As the UK's national technical authority for cyber security, NCSC incurs costs in providing technical cyber security support to Competent Authorities. This includes continued development and maintenance of the Cyber Assessment Framework and associated guidance.

- As lead government departments, BEIS, DfT, DHSC, Defra, and DCMS incur staffing costs in the day-to-day management of the NIS Regulations, and in broader policy

and review work. The Cabinet Office also has responsibility for managing and coordinating the National Cyber Security Strategy, of which the Regulations are a part.

The cost of **operating Competent Authorities** was calculated using the estimates provided by the Competent Authorities in table 5. Where full time equivalent roles were provided rather than actual wages, the mid-point of the relevant DCMS 2019/20 pay bands were used. In year 1, the cost was assumed to be the one off implementation cost plus the annual cost reported. Year 2 costs were equal to annual reported costs and year 3 costs equal to future costs. Where future costs were not provided, it is assumed that the annual costs will remain constant for the remainder of the appraisal period. It has further been assumed here that wage inflation will be equal to the general inflation rate, as Competent Authorities are government departments, agencies, or public sector bodies.

The total one off implementation cost of setting up Competent Authorities has been estimated as £1,353,955, while the total ongoing costs have been estimated as £34,898,231, in 2016 prices. It has been assumed that Competent Authorities did not pass their initial implementation costs onto businesses, whilst it has also been assumed that the operating costs of the public sector regulators have not been passed on to their public sector OESs. These are therefore costs to the government.

Table 7: Estimated and reported Competent Authority annual costs, 2019 prices

Competent Authority sector	Competent Authorities	Cost of staff estimated in Impact Assessment	Total costs estimated in Impact Assessment [52]	Reported one-off implementation costs	Reported annual costs	Forecast future annual costs
Transport (maritime, road, rail)	Department for Transport,	£954,647		DfT: £8,000	£472,500	£504,500
(aviation)	Civil Aviation Authority,			CAA:[53]	£274,000	£272,000
Energy (electricity, oil, gas)	BEIS and Ofgem (joint Competent Authority[54])	£415,054		BEIS, Ofgem and HSE: £1,083,864	£1,137,419	£1,453,431
Digital infrastructure	Ofcom	£219,124			£45,000	£45,000*
Health	Department of Health & Social Care	£57,956		£36,031	£44,997	£44,997*
Drinking water supply and distribution	Defra & Drinking Water Inspectorate	£646,154		DWI: £85,000[55]	£352,000[56]	£442,000
Digital service providers	ICO (UK wide)		£461,252 (plus £100,000 upfront costs)	£103,953	£495,283	£510,883
Devolved Administrations (aggregated across sectors)						
Scotland	Scottish Government, Drinking Water Quality Regulator (Scotland)	£358,161		Health: £190,000	£279,200	£232,300
				Water: Included in annual cost	£27,000	£30,000
Wales	Welsh Government		£480,000			
Northern Ireland	Department of Finance (Northern Ireland)	£411,687		£15,100	£224,080	£246,067

* Where no future cost data was provided, it has been assumed that future costs will be equal to current annual costs

[52] Where staff resources have not been provided.
[53] Not possible to separate one-off implementation costs from other cyber regulatory activity.
[54] BEIS and Ofgem are the joint Competent Authority for the downstream gas and electricity subsectors.
[55] This will be incurred in the financial year 2020-21 (year three of the appraisal period).
[56] For the devolved elements of the Regulations in relation to the water industry, the Welsh government has assigned Competent Authority duties over to the Drinking Water Inspectorate.

The total cost of operating Competent Authorities has been estimated over the 10 year appraisal period to be £36,252,186 in 2016 prices. Sensitivity analysis has also been conducted to account for uncertainty in future costs by varying total costs by 20%. This gives low and high estimates of £30,084,913 and £43,502,623 respectively.

The IA indicated that the Regulations may have an upward impact on prices of essential services due to familiarisation and administrative costs incurred by businesses, which may be passed on as additional **costs to consumers.**[57] The IA did not estimate what impact the introduction of the Regulations would have on prices, as there was a scarcity of both primary and secondary-level data to model an accurate impact on consumer's prices as a result of implementation. Evidence from the surveys conducted as part of the PIR suggests that there has been a small but limited upward pressure on prices of essential and digital services: only 1% of OESs and 6% of RDSPs reported having passed on costs incurred as a result of the Regulations to their consumers.[58]

b) Benefits

The key benefit of the Regulations outlined in the IA was the expected improvement in security which would lead to a reduction in the risks posed to essential services relying on networks and information systems. This in turn would benefit the UK's economic prosperity as we rely on these services to support economic output and societal wellbeing. It was expected that these benefits would derive from both: a reduction in the number of incidents that have significant disruptive effects due to improved protective measures; and a reduction in the impact due to appropriate incident response plans being put in place.

Incident reduction

The Regulations require notification of serious incidents to the relevant national authorities. This is an important part of incident response, and ensures that where necessary the NCSC can help OESs and RDSPs respond or react to a cyber incident.

While it has not been possible to look at longer term incident reporting trends, the review has looked at how organisations in scope have responded to the incident reporting requirements in the Regulations. Evidence from the survey of OESs and RDSPs indicates that most organisations are aware of the thresholds for reporting incidents,[59] and that they believe these thresholds are appropriate for their sector,[60] although as set out above, some Competent Authorities have highlighted a need to keep them under review and assess whether they remain appropriate. Although it would be preferable that all organisations in scope of the Regulations are aware of the thresholds, at this early stage of implementation this is nonetheless a positive indication.

There is some indication that the number of incidents that have significant disruptive effects is lower than anticipated. The IA estimated the number of incidents likely to be in scope of the Regulations each year (39) by annualising data provided by the NCSC for 1st October

[57] DCMS, NIS Regulations: Impact Assessment (2018), p.4
[58] Base: 110 OESs and 17 RDSPs.
[59] 91% of OESs and 82% of RDSPs. Base: 110 OESs and 17 RDSPs.
[60] 71% of OESs and 76% of RDSPs. Base: 111 OESs and 17 RDSPs.

2016 and 31st January 2017. The annual and annualised numbers of reported incidents has been lower than 39 since the Regulations came into force. While data collected for the review cannot show why this is the case, some Competent Authorities have suggested that incident reporting thresholds may currently be set too high for the NIS Regulations, both in the existing guidance for OES or in legislation for RDSPs. This is an area of implementation that will be reviewed (see sections 10 and 11), and should incident reporting thresholds[61] be set lower by any sectors, the number of reported incidents may increase.

At this stage in the implementation, insufficient data is available to look for any trend in reportable incidents decreasing over time. However, even in future years when trends in incident reporting will be possible to observe, given the nature of cyber breaches and the complex factors involved, it will not be possible to attribute incidents as having been prevented by measures taken under the Regulations. It is also not possible to quantify whether there has been a reduced impact of incidents where appropriate incident response plans have been put in place.

Quantifying the benefits of avoided losses through better security and risk management approaches is an extremely difficult task due to the breadth of impact cyber incidents can have across an organisation and its operations. To this end, the Government has commissioned work to better define the full extent of long and short-term costs of a cyber attack or breach, the results of which will be available later this year. These difficulties pose barriers to undertaking a robust cost benefit analysis, however, the argument made in the Impact Assessment - that benefits are likely to be substantial where even just one significant incident is prevented - remains sound.[62] In addition to the broader social benefit of avoiding disruption of critical services, the financial benefits of reduced incidents to organisations themselves can be significant.

For example, the Department of Health and Social Care estimated the direct costs to the NHS of lost output and IT support of the May 2017 WannaCry cyber attack to be £92 million. [63] This alone is more than the direct cost to business per year calculated for this PIR (£26.9m), and suggests that if one WannaCry-type incident is prevented, the benefits of the Regulations far outweigh the costs. Similarly, large impacts of cyber incidents have been felt in the transport sector in recent years. The Danish shipping container conglomerate AP Moller-Maersk's IT system was crippled by a cyber attack in 2017, and the company estimated the overall cost of the incident at $200m-$300m.[64]

Furthermore, the evidence suggests that the wider impact on the economy of disruption to essential services - disruption which could be caused by the types of incidents that the Regulations are designed to reduce - could in some cases be significantly greater than the likely direct cost to organisation which is the source of disruption. Research referenced in the Impact Assessment modelled the economic costs for a sophisticated cyber attack on the

[61] Referring both to the thresholds set out in guidance by Competent Authorities on what constitutes a 'significant impact on the continuity of the essential service', as per Regulation 11, as well as the provisions in Regulation 12 for RDSPs, referring to EU Regulation 2018/151.
[62] DCMS, NIS Regulations: Impact Assessment (2018), p.36.
[63] DHSC, Securing cyber resilience in health and care: Progress update October 2018
[64] Richard Milne, Moller-Maersk puts cost of cyber attack at up to $300m, Financial Times, (16/08/17).

electricity distribution network in the South East of the UK. The modelled scenarios show a loss of electricity supply from an attack affecting between 9 million and 13 million electricity customers. The knock on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.[65]

The economic losses to sectors were modelled to be in the range of £11.6 billion to £85.5 billion in the different variants of the scenario. The overall GDP impact of the attack amounts to a loss between £49 billion to £442 billion across the UK economy in the five years following the outage, when compared against baseline estimates for economic growth.[66]

More recent research models the impact of a cyber-physical attack - of the type which affected the Ukrainian power grid in 2017 - taking place on the electricity distribution network serving London, and surrounding regions in the southeast of England. Impacts are modelled on the basis of a 24-hour blackout, directly affecting between 0.25 to 1.45 million people in different scenarios, reflecting between 0.4% and 2.2% of the total U.K. population. Even with these limited assumptions, the economic consequences are modelled to be severe, with GDP loss ranging from £20.6 million in a four substation event with a 50% cumulative probability, up to £111.4 million for a 14-substation event with a 1% cumulative probability.[67]

Overall, although it has not been possible to monetise the benefits of the Regulations to date, the evidence suggests that the benefits of preventing just a small number of the types of incidents outlined above would far outweigh the costs of regulatory compliance.

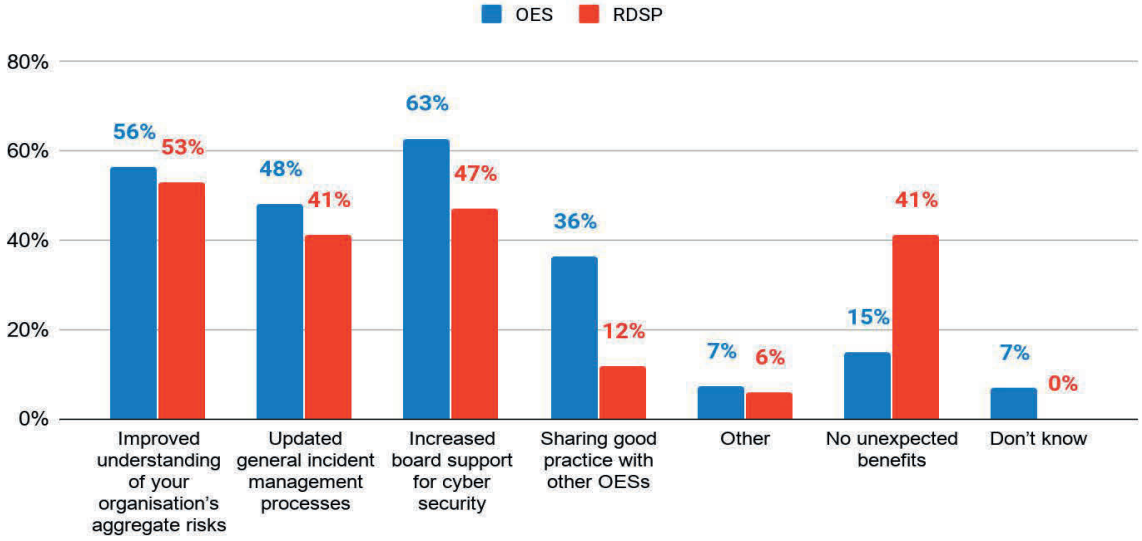
Other reported benefits

At an organisational level, many OESs and RDSPs responded that they had experienced some benefits as a result of implementing the NIS Regulations (Figure 5). The majority of organisations that answered this question felt that they had an improved understanding of their organisation's aggregate risk (56% of OESs and 53% of RDSPs), and 63% of OESs responded that NIS had increased board support for cyber security in their organisation.[68]

[65] Cambridge Centre for Risk Studies, Integrated infrastructure: cyber resilience in society (2016); DCMS, NIS Regulations: Impact Assessment (2018), p.33.
[66] Cambridge Centre for Risk Studies, Integrated infrastructure: cyber resilience in society (2016), DCMS, NIS Regulations: Impact Assessment (2018), p.34.
[67] Edward J. Oughton et al, Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks; *Risk Analysis* (Vol. 39, No. 9, 2019).
[68] Base: 110 OESs and 17 RDSPs

Figure 5: Have you incurred any of the following benefits as a result of implementing the NIS regulations?

Base: 110 OESs and 17 RDSPs, respondents could select multiple options



It is also worth noting that additional security spending by organisations, discussed above as a cost to organisations, can also be viewed as a benefit. Although there is no automatic link between additional spending on security measures and improved security outcomes, it can be viewed as much as a business investment as a cost, improving operational resilience and continuity of service.

The evidence base developed by DCMS has shown limited indications that there have been unintended benefits resulting from the Regulations at this early stage in the implementation. For example, this included increased collaboration between regulatory authorities and the sharing of best practice. Future post implementation reviews will look again at unexpected effects to understand whether other unexpected costs or benefits are observed over a longer time frame.

c) Aggregated costs and benefits

There were limitations to the cost figures used in calculating aggregate costs and benefits. Respondents were not forced to answer questions on costs in the survey, and the most popular response to many of the cost questions was that organisations did not know the answer, meaning there is limited new data to base revised estimates on. Where there have been gaps in data, many of the assumptions and estimates from the Impact Assessment have been updated and used again. Not all Competent Authorities were able to provide full data to calculate each Competent Authority's implementation, annual and projected future costs. Details of economic assumptions made can be found in the Competent Authority cost section.

The total net present value was calculated by aggregating the total quantified costs over the 10 year appraisal period, deflating to 2016 prices and discounting at a rate of 3.5%. Costs incurred by Competent Authorities of regulating private sector organisations have been

assumed to have been passed on to business, although costs may not have been transferred by all Competent Authorities, and certain costs cannot currently be transferred due to limitations on cost recovery powers (see section 10). Consistent with the IA, the benefits have not been quantified for the reasons examined above. Estimated figures from the Impact Assessment and calculations for this PIR are presented below:

Table 8: Total costs and benefits

	Total net present value	Business net present value	Net direct cost to business per year
Estimated in IA (EANDCB: 2014 prices; 2015 present value)	Low/Best: -£402.59 m High: -£215.98 m	-£202.54m	£20.4m
PIR Estimates (2016 prices, 2017 present value)	Low: -£434.1m Best: -£405.2m High: -£377.1m	-£232.4m	£27.0m

As set out in the table above, the analysis indicates a small increase in the net direct cost to business, which is predominantly due to the cost of additional security spending being higher than originally estimated. This may be due to organisations in scope needing to invest more initially in security improvements; it should also be noted that while the Impact Assessment set out business costs including spending on cyber security spending, the PIR gathered evidence on broader categories of security spending - including physical security - which more accurately reflects the scope of the Regulations; this may also have had an impact on the variance between the 2016 and 2019 calculations on net direct costs to businesses.

Despite representing an additional cost to organisations in scope, additional security spending should be seen as an investment in improved security, resilience and organisational capability; where this investment is properly targeted, it should lead to a reduction in the risk of a security incident which could require significant resources to remedy. In DCMS's view, the additional expenditure on security is an indication that organisations in scope are positively engaging with the requirements of the Regulations.

7) Is government intervention still required?

As set out in the summary, the rationale for government intervention remains compelling, and the regulatory objectives remain appropriate; we all rely on energy networks to power and heat our homes, transport networks to travel to work and school, and healthcare networks and information systems to allow medical professionals to do their jobs. Digital infrastructure and digital service providers are increasingly important to our economy. The failure or

compromise of networks and information systems in these sectors is a systemic threat to the availability of the services they provide.

Society relies on these OESs and RDSPs, but as set out in the IA, the potential cost of disruption to society may not be taken into account when organisations consider how much to invest in resilience and security measures and practices. The external factors cited in the IA are still relevant today. It is challenging for organisations to estimate the benefit of additional investment in their security, as this is the benefit of costs avoided due to preventing incidents that would have otherwise have occurred. Therefore, it is difficult for organisations to justify investing in these measures at the level required to meet the national interest. As a result, Government intervention is still required in order to ensure the security and resilience of networks and information systems in these sectors. Initial returns from organisations who use the CAF show that many organisations found it to be a useful process which helped identify areas where further intervention and investment are needed.

8) Is the existing form of government regulation still the most appropriate approach?

The National Cyber Security Strategy 2016-2021 committed to putting measures in place to intervene where necessary to drive improvements that are in the national interest.[69] The evidence outlined in previous sections indicates that the Regulations are effective in driving improvements at a quicker pace than would otherwise be the case; for the reasons set out above and in light of the evidence gathered through the review, in our view non-statutory measures would not achieve the same benefits. In view of societal reliance on the sectors in scope of the Regulations, and the substantial cyber threats posed to these sectors, proportionate regulatory intervention is still required to ensure the pace of change is not slowed down.

While in our view there is a strong case that regulation in this area is required, the Government has worked to minimise the compliance burden to organisations in scope wherever possible. The regulatory framework has been set up to support and encourage organisations towards compliance, rather than taking a punitive approach which uses enforcement action as the primary tool. The framework allows organisations to draw on the support and expertise of Competent Authorities and the NCSC in order to drive improvements, with enforcement action as a last resort. It is not possible to fully assess how effective the enforcement mechanism has been, since there has been very limited enforcement activity in the short time in which the Regulations have been in force. However, Competent Authorities have advised that the current enforcement regime would benefit from being placed on a more statutory footing, using existing judicial structures, which would make enforcement more robust and transparent for OESs and RDSPs.

The Regulations are also outcome-focussed, and they therefore allow organisations to develop bespoke and innovative approaches to compliance which suit them. By avoiding a prescriptive set of compliance requirements, the regulatory framework is innovation-friendly

[69] National Cyber Security Strategy 2016-2021, p.41.

and does not need continual revision and reformulation in order to keep pace with a digital environment which is fast-moving and changeable.

The Regulations are also proportionate and targeted with regard to the organisations brought into scope; section 11 indicates some next steps in ensuring the regulatory framework continues to be proportionate and brings organisations into scope only where necessary.

While some areas for improvement are set out in section 11, the Government views the current regulatory framework is the most appropriate approach. However, if the behaviour of organisations in scope of the Regulations towards the security of their network and information systems changes significantly in the future, or the nature or scale of the threat substantially alters, a different regulatory approach may need to be developed.

9) EU-derived regulations

This section outlines how the implementation of the NIS Directive in the UK compares with implementation in EU member states, especially considering the impacts on UK based businesses relative to other European competitors and whether there are opportunities to improve UK transposition in comparison.

A common list of OES sectors to be brought into scope of regulation were identified in the original NIS Directive: energy, transport, banking, financial market infrastructures, health, drinking water and digital infrastructure. UK implementation brought all but the finance sector into scope of the Regulations. The UK omitted the finance (banking and financial market infrastructures) sector from the scope of the NIS Regulations, as relevant 'sector-specific Union legal acts' applying to the finance sector were deemed 'at least equivalent in effect to the obligations' of the NIS directive.[70]

As the Regulations were transposed from an EU Directive, there are differences in the national implementation of NIS in each of the EU's Member States; each Member State therefore had flexibility over the measures that were to form the overall regulatory framework for NIS, whilst still maintaining its overall principles. For example, there is a requirement in the UK for DSPs to register with the ICO, but this is not the case across Europe. The UK is also the only country which included a reporting period deadline of 72 hours for NIS incidents for all OESs and RDSPs.

For the sectors that the UK has included, there are fewer OES in scope than some Member States, which could have a bearing on the number of incidents reported. Across all other countries which have implemented the Directive, through international cooperation and information sharing mechanisms, it has been evidenced that there are strong discrepancies between countries in relation to both incident reports received and the essential services (and OES) in scope of the Directive.

The European Commission, pursuant of Article 23(1) of the Directive, carried out an EU-wide assessment of the consistency of approaches taken by Member States in identifying OESs

[70] UK Transposition Table, NIS Directive.

and DCMS developed an Explanatory Memorandum which was subsequently presented to Parliament on this topic.[71] The report concluded in broad terms that there is some fragmentation and a wide range of differing approaches across all EU Member States, and broke down the differences into a number of categories: (1) differences in identifying essential services, (2) use of thresholds, (3) degree of centralisation for NIS implementation, (4) different authorities in charge of identification of OES, and (5) Member State assessment of network and information systems dependence.

Its analysis suggested that this is likely a consequence of the fact that the legislation comes from a directive and discretion was given to Member States in interpreting and transposing the Directive into national legislation. The Commission made recommendations to address this issue, focusing mostly on the value of the NIS Cooperation Group and the need for further close cooperation and information sharing; the Commission also committed to reviewing existing guidelines and documentation available to all EU Member States.

Regarding the scope of the Regulations, some Member States, for instance, have chosen to include additional sectors in scope of their implementation of the Directive, above and beyond the common list of sectors specified. For example, Slovakia and Lithuania have included the civil nuclear and nuclear sectors in their regulations, while France and Germany include the insurance sector. France in particular has implemented the Directive broadly, including many additional sectors - such as space, research and innovation - in addition to the common list required by the Directive.

By bringing a limited number of sectors into scope of the Regulations compared with many other EU member states, the UK has reduced the burden of the Regulations on UK organisations compared with most EU member states. This accords with the Government's aim that regulation is proportionate and targeted.[72]

Currently, information gathered as part of this Review did not conclusively indicate whether there is a need for a broader sectoral approach. Evidence from this PIR will inform wider consideration of what is appropriate and proportionate cyber security regulation for other sectors in the UK, as part of the forthcoming Incentives and Regulation Review and the development of future strategic objectives and priorities for cyber security.

The UK implementation of the Directive also diverges from Member States in its approach to the penalty regime. The maximum penalty which can be imposed on OESs and RDSPs in the UK is £17 million, which is reserved for actions that have caused, or could cause incidents that result in an immediate threat to life or significant adverse impact on the United Kingdom economy. This maximum penalty is designed to be partly aligned with the General

[71] European Commission, Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (2019); DCMS, Explanatory Memorandum: Report of the Commission on the consistency of Member State approaches to identifying operators of essential services under the NIS Directive (2019).
[72] BEIS, White Paper: Regulation for the Fourth Industrial Revolution (2019), p.8.

Data Protection Regulation's penalty regime, although for the NIS Regulations there is no 'percentage of turnover' element.[73]

Member states have a varied and diverse approach to constructing penalty regimes. In addition to financial penalties that can be imposed on organisations, some member states such as Cyprus and Belgium include personal liability as a deterrent and penalty, some going as far as prosecuting for criminal offences. Most member states have a maximum financial penalty which is significantly lower than the maximum figure in the UK, with the exception of Romania and Austria in certain circumstances.[74]

The strength of the UK penalty regime reflects the seriousness with which the Government considers cyber security and the risks it poses to society and the economy, and the government is committed to ensuring that the penalty regime remains proportionate to cyber security threats and risks. Concerns from industry on the penalty regime were raised during the original public consultation process, and amendments were made to the Government's original proposals as a result. However, there remains the potential for the relatively robust penalty regime in the Regulations to have a greater impact on UK based businesses compared with businesses in member states in scope of different implementations of the Directive. There is no evidence that this has occurred since UK implementation in May 2018, as no penalty notices have yet been issued. Furthermore, penalty notices would only be issued as a measure of last resort, and therefore would only affect organisations which are non-compliant.

Following the departure of the UK from the EU on 31 January 2020 and the end of the transition period on 31 December 2020, the NIS Regulations (which implement the NIS Directive) will remain part of UK law but the UK will not be required to implement any changes made to the NIS DIrective by the EU. The UK will be able to amend the NIS Regulations as it sees fit; amendments within scope of the NIS Directive can be made by secondary legislation, but amendments beyond the scope of the NIS Directive must be made by primary legislation. This has been incorporated into our assessment of areas for potential improvements in the following section.

[73] Under the General Data Protection Regulation (GDPR) the maximum penalty that can be imposed by the ICO is £17 million, or 4% of annual global turnover, whichever is higher. A proposal to match this provision in the NIS Regulations was rejected following public consultation in 2018, with the percentage turnover element removed from the penalty regime.

[74] In the event of repeated breaches, Romanian regulators can impose a maximum penalty of up to 5% of a company's turnover. Austria has imposed a cumulative approach to imposing fines, issuing a penalty for each specific instance of non-compliance.

10) What are the areas for improvement?

As well as looking at the outcomes that have been reported to date and the costs and benefits to organisations, DCMS has also looked at elements of the implementation of the Regulations, and the framework of non-regulatory processes and activities which have been put in place to support organisations. Reviewing the implementation in this way is vital to ensuring that both organisations in scope and Competent Authorities are able to implement the Regulations in the most effective and efficient way. This section outlines areas for potential improvement which have been highlighted during the review process. Section 11 - 'Next Steps' - sets out where and how the Department intends to act to make improvements to the Regulations.

The Department is committed to ensuring that Competent Authorities are equipped to effectively support and secure compliance with the Regulations. In order for the Competent Authorities to be in a position to regulate more effectively, improvements could be made in the following areas set out below.

Cost Recovery:
The current cost recovery framework under the NIS Regulations is enshrined in Regulation 21 (Fees). The Regulations allow Competent Authorities to recover reasonable costs incurred in the discharge of their duties in implementing the Regulations, with the notable exceptions of functions carried out under Regulations 17(1) - 17(4), 18, 19, and 20. This means that cost recovery powers available to Competent Authorities include costs up to, but not including, any form of enforcement.

This creates challenges for some Competent Authorities and risks creating inconsistencies across NIS implementation in the UK; It also puts more pressure on funding from public sources (i.e. central government), as Competent Authorities are reliant on funding streams from government departments to support their enforcement regimes. Addressing this challenge is an important area for improvement in order to achieve regulatory objectives in an effective and proportionate way.

Appeals Mechanism:
Improvements to the operation of the mechanism by which OESs and RDSPs appeal enforcement and designation decisions made by Competent Authorities have been identified. A number of Competent Authorities and LGDs have suggested that the existing mechanism for appealing decisions made by Competent Authorities can be improved to reduce the burden on the Competent Authorities to appoint the independent reviewer where, per Regulation 19, OESs or RDSPs request a review of a specific designation or penalty notice. Competent Authorities have identified that amending Regulation 19 could help Competent Authorities and operators to resolve any potential disputes in a more efficient, transparent and timely manner. Amending Regulation 19 would also provide an opportunity to specify procedures which an appeal should take to ensure consistency amongst the Competent Authorities when making decisions whilst also expanding the scope of appealable decisions that are currently excluded from the Regulations.

Support for OESs and RDSPs from Competent Authorities:
60% of OESs and 71% of RDSPs feel they have been given appropriate guidance and support by their Competent Authorities.[75] This varies by sector, with more organisations in some sectors reporting not receiving appropriate guidance and support. The quality of guidance and support is therefore an area for improvement, especially when considering that initial returns from organisations who use the CAF show that there is still more to be done to ensure organisations in scope can fully implement the standards recommended by the NCSC to ensure security and resilience in these sectors.

Support for Competent Authorities:
Competent Authorities were asked what further support from DCMS would be helpful in supporting them to effectively regulate the NIS Regulations. Most of the Competent Authorities would like to see further support from the Government in the following areas: further guidance on implementation; a work programme to support capability building and sharing; and working with the NCSC to develop a more consistent skills and training framework for compliance teams.

Designation Thresholds for OESs:
Schedule 2 of the Regulations specifies the criteria (thresholds) for designating which organisations in a given sector are in scope of the Regulations, and designated as an OES or RDSP.

While some Competent Authorities reported their designation thresholds to be broadly correct, some Competent Authorities have indicated that they believe that the designation thresholds for their sector or region could be improved upon to ensure all relevant organisations are in scope. Some Competent Authorities have highlighted potential issues with designation thresholds, for example that designation thresholds could be set too low and are bringing too many small businesses into scope of the Regulations, or that the thresholds as they are currently defined may not be covering all organisations critical to the provision of essential services. Addressing concerns about designation thresholds is an important area for improvement in order to achieve regulatory objectives in an effective and proportionate way.

Wider enforcement regime:
As mentioned earlier in this Review, evidence submitted from Competent Authorities suggests that there is a need to further develop and refine the wider enforcement regime[76], which may include, but is not limited to, improvements to the enforcement and information notices, clarification in respect to civil liabilities, and further amendments to simplify and improve the legislation. Within this category, and going beyond the recommendations made on designation thresholds, there is also a need to review and reconsider the wording in the legislation to improve clarity.

[75] Base: 111 OESs and 17 RDSPs
[76] In this section, the word 'enforcement' refers to various provisions in the NIS Regulations that have an impact upon wider enforcement and compliance efforts, and is not limited to its definition in the legislation.

Several Competent Authorities, based on their collective experience, also raised the need to provide further tweaks and improvement to the wording in the penalty bandings, to ensure that the Regulations are effective, clear, and provide stability and a clear expectation to organisations that are regulated by the Competent Authorities. Overall, based on the evidence and assessments submitted, there is a strong case to reinforce and improve the overall enforcement regime, as there are concerns that the current framework does not provide sufficient clarity and certainty to Competent Authorities, OES or RDSPs.

Supply chain:
A supply chain attack is a cyber attack that seeks to damage an organisation by targeting less secure companies in the organisation's supply network. In practice this means that the functioning of one company is increasingly dependent on the cyber resilience of a number of other companies, their networks, systems, processes and infrastructure. The complexity and interconnectivity of today's digital environment means that organisations have limited understanding of vulnerabilities and interdependencies that they and their supply chains are subject to.

Effective supply chain risk management is essential to having appropriate and proportionate security measures in place to protect network and information systems, as required by the Regulations. Government treats supplier risks as one of the priority focus areas due to the growing number of attacks targeted at the weak link within supply chains and the scale of damages these attacks continue to pose to the wider economy and society.

Supply chain risk management was highlighted as an issue by both Competent Authorities and organisations in scope. The Government is actively looking at what more can be done to support organisations to manage the risks arising from their supply chain effectively; further details of the next steps in this area are set out in section 11.

Incident thresholds:
Incident reporting thresholds for OES are set in guidance by Competent Authorities. Some Competent Authorities reported a need to consider whether incident reporting thresholds are set at the appropriate level, in particular in light of the small number of incidents below the original estimates that have so far been reported, and as a result this will be considered as a potential area for improvement.

For RDSPs, these thresholds for what constitutes a 'substantial impact of an incident' are set in legislation, under Regulation (EU) 2018/151, and are currently implemented at EU-level, due to the framing and the nature of the NIS Directive.[77] As this legislation will become EU-retained law by virtue of the UK's departure from the EU through the Withdrawal Act, it is necessary to amend the thresholds to reflect this change, as it is not appropriate for these to be set at EU-level now that the UK is no longer a Member State.

[77] Official Journal of the European Union, Commission implementing Regulation (EU) 2018/151 (2018). This sets rules for application of Directive (EU) 2016/1148 [etc.], which will be retained following the Transition Period.

Review period:
As mentioned previously in this Review, DCMS's assessment is that this two year model of review is preferred at the present time, as it allows the Government to monitor implementation closely in the initial phases of implementation. This period, however, should be reviewed to allow for a more comprehensive report to be developed in the long-term. Therefore, the Department recommends, pending consultations and further policy development, that the review time be lengthened to the more standard and widely used 5-year cycle, to ensure that future Reviews have more data to draw on and do not become a burden on business or Government. The regular use of the Cyber Assessment Framework and other tools by Competent Authorities would allow regulatory authorities to monitor and evaluate progress between reviews.

11) Next steps

Recommendation:
Taking account of the evidence as set out above, DCMS recommends **retaining** the Regulations, but making **amendments** in order to address the areas for improvement identified in section ten.

DCMS intends to consult, as soon as is reasonably practicable, on options to improve the effectiveness of the implementation of the Regulations, likely covering the following issues:

Cost Recovery:
DCMS will need to conduct further analysis of this issue, and may intervene in order to ensure that Competent Authorities have cost recovery powers which allow them to effectively conduct regulatory activity. This would require primary legislation and any powers must be proportionate and not place an undue burden on regulated organisations. DCMS will explore cost recovery models which operate successfully in other pieces of regulation as a starting point, such as Regulation 28 of COMAH (Control of Major Accident Hazards) Regulations 2015. Addressing this challenge and others is an important area for improvement in order to achieve regulatory objectives in an effective and proportionate way.

Appeals Mechanism:
DCMS intends to amend the current review mechanism in Regulation 19, to create a long-term solution which reduces risk borne by Competent Authorities, gives them the confidence and legal safeguards necessary for them to effectively conduct regulatory activity, and provides OESs and RDSPs with a more robust appeals mechanism. DCMS aims to lay a statutory instrument, as soon as is reasonably practicable, making such amendments.

Designation Thresholds:
DCMS will consider whether designation thresholds are set at the right level. Amending the designation thresholds set out in Schedule 2 of the Regulations where necessary, is possible by secondary legislation and will be incorporated into the SI which addresses the appeals mechanism (see above).

Wider enforcement regime:
DCMS will consider amendments, pending further policy development and formal consultation, to a number of aspects that affect the wider enforcement regime, to provide further clarity to both Competent Authorities and to regulated organisations (OES and RDSPs), particularly in relation to improvements for enforcement and information notices, provisions around information sharing, and the need for further clarification around penalties to avoid any issues arising from the cross-sectoral interpretation of the bandings. This Review also recommends that further attention is given to a review of the inspection and investigation powers, to ensure that the Regulations are effective in maintaining the UK's critical infrastructure, wider security and long-term prosperity.

Incident thresholds:
DCMS will need to make amendments to the incident thresholds for RDSPs as the current thresholds are set at an EU-wide level. The regulatory authorities and DCMS will also be assessing the incident thresholds for OESs following this review, to ensure they remain relevant and effective. Incident thresholds for OESs are set in guidance by Competent Authorities, and DCMS will play a coordinating role to ensure that regulatory authorities are reviewing and setting their thresholds consistently.

Supply Chain:
The issue of supply chain risk management affects organisations across the entire economy, and solutions need to be developed which will have a broader impact than purely supporting those organisations in scope of NIS. As this is a wider policy concern, the forthcoming Cyber Security Incentives & Regulation Review will consider the support Government can provide to procurers, such as standard contractual clauses or supplier questionnaires, as well as the role of Government in reducing these risks at scale.

Whilst not directly specified in the NIS Regulations, in recognition of its integral importance to the continuity of services, a number of supply chain risk management outcomes have been integrated into the CAF. Accordingly and akin to all organisations across the UK, OES are responsible for the management of their own supplier-related risks. For those in scope of the NIS Regulations, the Government is looking at ensuring there is effective support to manage these supply chain risks. Where there continue to be barriers that cannot be addressed by guidance and advice alone, the Government will consider the potential appropriateness of regulatory action to achieving security at scale. We will look to engage industry further on this issue in due course.

Delegated Powers:
It is important that the government maintains the powers to amend the Regulations, in order to adapt them to better suit the needs of industry and the Government in the future. The Government is also ambitious to ensure that the NIS regulatory regime is tailored to the needs of the UK and that the Government is able to go beyond the limits imposed by the Directive it stems from if there is a need to do so, in line with the Government's aspirations of being a global leader in cyber security. Authority to amend the Regulations currently derives from Section 2(2) of the European Communities Act and will expire at the end of 2020 when the transition period concludes. Policy options to develop legislative powers are needed, particularly to replicate the flexibility present in Section 2(2) of the European Communities

Act 1972, especially focusing on aspects that are likely to be amended in order to keep pace with the speed of technology advances (e.g. designation thresholds, both numerical and procedural aspects, the wider penalty regime, security requirements, etc.). These policy options must be developed with the aim of maintaining the relevance and efficacy of the NIS Regulations in securing operators of essential services to the UK and key digital service providers.

Review period:
This Review recommends that the Government consider amending the legal requirement for review of the Regulations from 2 to 5 years.

Scope of the Regulations within existing sectors:
There may be a need in future to amend the scope of the Regulations (beyond tweaks to designation thresholds) to adapt the regulatory regime in response to major technological changes and to include new market players that gain importance in the sectors currently in scope. DCMS and regulatory authorities will continue to monitor the landscape, and will seek to adapt the scope of the regulatory regime where necessary - subject to appropriate consultations - to ensure that the Regulations meet their objectives effectively and proportionately.

Support for OESs and RDSPs from Competent Authorities and support for Competent Authorities from DCMS:
DCMS will continue to provide opportunities for Competent Authorities to share best practice and improve their abilities to support the organisations they regulate, in conjunction with the expert advice provided by the NCSC. In addition to regular Competent Authority meetings hosted by DCMS, deep dives and work groups will continue to be held in order to support Competent Authorities in their regulatory activity.

ANNEXES

Annex A: Questionnaire used to survey OESs

Introduction

In May 2018, the UK government introduced the Network and Information Systems (NIS) Regulations. These regulations were designed to improve the cyber and physical resilience of network and information systems for the provision of essential services and digital services. These regulations apply to operators of essential services (OESs) in the water, transport, energy, health and digital infrastructure sectors, as well as relevant digital service providers (RDSPs), which provide online marketplaces, online search engines and cloud computing services. Section 25(1) of the NIS Regulations requires the Secretary of State to carry out a review of the regulatory provision contained in the NIS Regulations and publish a report setting out its conclusions.

Purpose of the survey

A post-implementation review seeks to establish whether the regulations have achieved their original objectives and remain appropriate. In order to inform our assessment of the impact of the NIS Regulations, we are conducting a survey of organisations that are covered by the regulations. The information you provide as part of this survey will inform future policy making with regard to the NIS Regulations.

How your data will be used

Full information on how your personal data will be stored and used for this survey is contained in your Competent Authority privacy notice. Survey responses will be collected and stored securely by DCMS (as the Department responsible for the NIS Regulations), and will not be shared beyond the team responsible for managing this survey at DCMS, unless you give us permission to share your response with your Competent Authority and/or the NCSC, in order for them to understand how the implementation of the NIS Regulations can be improved. While we cannot guarantee full anonymity, as the number of OESs in some sectors is small, we will not ask for the name of your organisation and we will ensure that the final post implementation review report, which will be published, does not make public information which could identify any individual organisation.

You do not have to answer all of the questions, and you can skip any questions you cannot or would prefer not to answer, beyond the first four opening questions. Your Competent Authority may contact you again to ask if you would like to take part in further research to inform the post implementation review.

Freedom of Information

Under the FOIA (Freedom of Information Act (2000), there is a statutory Code of Practice with which public authorities must comply and which deals, among other things, with obligations of confidence. In view of this, if you would like the information you provide in the survey to remain confidential, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. FOI exemptions may be applied to this data. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

How to answer the survey

The purpose of this survey is to evaluate the effectiveness of the NIS Regulations. Therefore, we would like you to answer the questions throughout the survey with specific regard to the NIS Regulations and your organisation's network and information systems resilience relating to the provision of your essential service(s), unless clearly specified otherwise. Please also bear in mind when completing the survey that the purpose of the survey is to understand your experience of implementing the NIS Regulations at your organisation; we do not require any information on any security vulnerabilities as the survey is not designed to test security resilience. Please do not provide information in your answers that you would classify as sensitive and/or contains personal data.

If you have any questions, please get in touch with your Competent Authority or the DCMS survey and policy team at nis@culture.gov.uk.

Please confirm below that you have read and understood this statement, about how your personal data will be collected and used, and agree with its terms. Please note that you have to answer this question before you are allowed to proceed with the survey.

- ❑ I confirm that I have read and understood this statement

DCMS will be collecting partial responses to the survey. If, during completion of the survey you decide to withdraw your response, you will need to contact DCMS Data Protection Team at dcmsdataprotection@culture.gov.uk asking that your response be deleted, please use the email subject heading 'Cyber Security NIS PIR review'. Please note we may require you to provide us with some of your answers to the survey in order to identify and thus delete your response.

Once you have submitted your response to the survey, you will not be able to withdraw your answers from the analysis stage.

If you need any further information related to the processing of your personal data please contact us: DCMS Data Protection Team at dcmsdataprotection@culture.gov.uk and specify which survey you have concerns about.

If you need any further information about the survey please contact your Competent Authority or the DCMS survey and policy team at nis@culture.gov.uk.

Please confirm that you have read the information above and you are happy to participate and continue with the survey.

- ❏ I have read the above information and am happy to participate in the survey

Are you content for your answers to be shared with the National Cyber Security Centre?

- ❏ Yes
- ❏ No

Are you content for your answers to be shared with your Competent Authority?

- ❏ Yes
- ❏ No

Background demographic

1. What sector do you provide your essential service(s) to?
    - ❏ Health
    - ❏ Energy
    - ❏ Transport
    - ❏ Digital Infrastructure
    - ❏ Water

2. Are you a parent company?
    - ❏ Yes
    - ❏ No

    If q.2 = yes go to q.3
    If q.2 = no go to q.4

3. What size is your organisation? Please select the option for which 2 or more of the following requirements have to be met by the group for which your organisation is the parent company in the current and previous financial year
    - ❏ Small: (not more than 50 employees, aggregate turnover <£10.2m net/£12.2m gross, aggregate balance sheet total <£5.1m net/£6.1m gross)
    - ❏ Medium: (not more than 250 employees, aggregate turnover <£36m net/£43.2m gross, aggregate balance sheet total <£18m net/£21.6m gross)
    - ❏ Large: (more than 250 employees, aggregate turnover >£36m net/£43.2m gross, aggregate balance sheet total >£18m net/£21.6m gross)

4. What size is your organisation? Please select the option for which 2 or more of the following requirements have to be met by your organisation in the current and previous financial year
    - ❏ Small: (not more than 50 employees, turnover <£10.2m, balance sheet total <£5.1m)
    - ❏ Medium: (not more than 250 employees, turnover <£36m, balance sheet total <£18m)
    - ❏ Large: (more than 250 employees, turnover >£36m net, balance sheet total >£18m)

5. Who is your Competent Authority?
    - ❏ Department for Business, Energy and Industrial Strategy (BEIS)
    - ❏ Department for Business, Energy and Industrial Strategy (BEIS) and Office of Gas and Electricity Markets (Ofgem)
    - ❏ Department for Transport (DfT)
    - ❏ Department for Transport (DfT) and Civil Aviation Authority (CAA)
    - ❏ Office of Communications (Ofcom)
    - ❏ Department for the Environment, Food and Rural Affairs (Defra)
    - ❏ Department for Health and Social Care (DHSC)
    - ❏ Drinking Water Quality Regulator for Scotland (8)
    - ❏ Department for Finance (Northern Ireland)
    - ❏ Scottish Government
    - ❏ Welsh Government
    - ❏ Don't know

6. To the best of your understanding, or as agreed with your Competent Authority, how many systems do you use that are considered 'critical' within the scope of the NIS regulations?
    - ❏ 1 to 5
    - ❏ 6 to 10
    - ❏ 11 to 15
    - ❏ 16 to 20
    - ❏ 21+
    - ❏ Don't know

7. How long has your organisation been designated as an OES?
    - ❏ less than 6 months
    - ❏ 6-12 months
    - ❏ over 12 months
    - ❏ Do not know

Impacts of the NIS Regulations

8. Prior to the NIS regulations, did you take any action to improve the security of your Network and Information Systems specifically relating to providing your essential service?

- ❑ Yes
- ❑ No
- ❑ Don't know

9. Prior to the legal obligation of the NIS regulations, what other reasons have caused you to implement changes to the security of your Network and Information Systems relating to the provision of your essential service(s) in the past?
   - ❑ Previously experienced a breach or attack
   - ❑ Media coverage of other organisations experiencing a breach or attack
   - ❑ To protect critical systems
   - ❑ To protect customer data
   - ❑ To protect intellectual property/trade secrets
   - ❑ To maintain business continuity
   - ❑ To avoid financial loss
   - ❑ To avoid reputational damage
   - ❑ To comply with requirements imposed by other businesses e.g. customer/ supplier standards
   - ❑ To respond to industry guidance (e.g. from NCSC or trade bodies)
   - ❑ To comply with data protection law (Data Protection Act 2018 and the GDPR)
   - ❑ To comply with other non-NIS regulations (excl. GDPR), please specify……..
   - ❑ To comply with other industry initiatives
   - ❑ Other, please specify……..
   - ❑ Don't know

Guidance

10. Do you know where to find guidance on NIS implementation and compliance?
    - ❑ Yes
    - ❑ No

    Display q.11 if q.10 = yes

11. Is this guidance easy to access?
    - ❑ Yes
    - ❑ No

12. Have you received appropriate guidance and support from your Competent Authority to implement the NIS regulations effectively?
    - ❑ Yes
    - ❑ No
    - ❑ If no, please explain……

13. What additional support or guidance from your Competent Authority or other sources would further assist you with the implementation of the NIS regulations?
    - ❑ Hold industry events
    - ❑ Provide information exchanges

- ❑ Provide updates to the businesses
- ❑ Other, please suggest here……

Security Risk Management

14. Prior to the NIS regulations, did you have any governance policies and/or processes to manage security risk of your Network and Information Systems?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

15. Have you made any changes to or strengthened your governance policies and/or processes to manage security risk as a result of the NIS regulations?
    - ❑ Introduced new policies/processes
    - ❑ Updated/strengthened existing policies/processes
    - ❑ No, but we intend to update/strengthen our policies/processes
    - ❑ No change, please specify why……..

16. Have the NIS regulations increased the prioritisation of security at a senior management level?
    - ❑ Yes
    - ❑ No

17. Please explain your answer……...

18. Do you feel there are any challenges to your organisation's ability to implement the NIS regulations?
    - ❑ Yes
    - ❑ No
    - ❑ If yes, please explain what these are……

Skills

19. Within your organisation, do you feel you have the in-house skills and capacity to deliver your obligations under the NIS Regulations?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

20. Did you take any of the following actions with regard to resourcing to support your implementation of the NIS regulations when they were introduced? Please select all options that apply.
    - ❑ Hired additional staff
    - ❑ Outsourced to specialist security consultants
    - ❑ Provided training for existing staff

- ❑ Other, please specify……...
- ❑ No external means used

21. As a result of the NIS regulations, have you retrained/up-skilled any existing staff or hired any new staff to manage security risks to your Network and Information Systems?
    - ❑ Yes
    - ❑ No, outsourced instead
    - ❑ No
    - ❑ Don't know

22. Are there any barriers that prevent you from conducting effective risk management of your suppliers (and your wider supply chain e.g. supplier's suppliers)?
    - ❑ Yes
    - ❑ No
    - ❑ If yes, please explain why……...

23. Do you feel you have the resources to manage risks to the security of your Network and Information Systems arising from your suppliers (and your wider supply chain e.g. supplier's suppliers)?
    - ❑ Yes, we have the resources to manage the risk from our direct suppliers and our wider supply chain
    - ❑ Yes, we have the resources to manage the risk from our direct suppliers but not from the wider supply chain
    - ❑ No, managing supplier risk is not a priority
    - ❑ No, we are unsure how to manage risk from our direct suppliers and our wider supply chain
    - ❑ No, we do not have the resources
    - ❑ Other, please specify……...

Incidents and incident reporting

24. Prior to the NIS regulations, did you have any processes and/or procedures in place for recovery from a security incident relating to the Network and Information Systems used for the provision of your essential service(s)?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

25. Have you introduced or strengthened existing processes and/or procedures for recovery from a security incident as a result of the NIS regulations?
    - ❑ Introduced new processes/procedures
    - ❑ Strengthened existing processes/procedures
    - ❑ No, but we intend to introduce/strengthen our processes/procedures
    - ❑ None of the above

26. Which of the following areas have you taken action as a result of the NIS regulations with regard to incident response? Please select all that apply
    - ❑ Risk assessment that takes account of your essential service
    - ❑ Up to date incident response plan
    - ❑ Understand the resource requirements required to enact your incident response plan
    - ❑ Carry out regular exercises to test your incident response plan
    - ❑ Other, please specify…….
    - ❑ No action taken

27. Are you aware of the incident reporting thresholds for your sector?
    - ❑ Yes
    - ❑ No

28. Is the current deadline of 72 hours from discovery of an incident which meets the reporting threshold sufficient time to report an incident to your Competent Authority?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know
    - ❑ If no, please explain why: ……..

29. Do you think the incident identification thresholds for reporting NIS incidents are appropriate for your sector?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know
    - ❑ If no, please explain why: ……..

30. Since the implementation of the NIS regulations, how has your attitude towards voluntary reporting of an incident that is under the reporting threshold changed towards
    a) your Competent Authority?
    b) Your lead Government Department
    c) the NCSC?

    - ❑ More likely to voluntarily report
    - ❑ Less likely to voluntarily report
    - ❑ Stayed the same
    - ❑ Do not have a voluntary reporting process

31. Please explain your answer…….

Lessons learned

32. The operators of essential services that are in scope of the NIS regulations are those that meet the designation thresholds set out in schedule two of the regulations. Did your organisation find the designation thresholds which apply to you clear?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

33. To what extent has applying the NIS security principles impacted positively on the following with regard to the provision of your essential service(s) in your organisation? (-2= extremely negative, -1 = somewhat negative, 0= neither positive nor negative, 1= somewhat positive, 2= extremely positive)
    - ❏ Awareness of security amongst employees
    - ❏ Security standards within your organisation
    - ❏ Understanding of key assets and critical systems
    - ❏ Processes to respond to security breaches and attacks
    - ❏ Security guidance you produce within your organisation
    - ❏ Security training for staff
    - ❏ Understanding of your responsibilities in managing your security risks
    - ❏ Confidence in understanding your organisations' security risks

Cyber Assessment Framework

34. Do you use the Cyber Assessment Framework?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

Display q.35 if q.34 = yes

35. To what extent did you find the Cyber Assessment Framework useful for managing risk to the security of your organisation's Network and Information Systems?
    - ❏ Extremely useful
    - ❏ Very useful
    - ❏ Moderately useful
    - ❏ Slightly useful
    - ❏ Not at all useful

Display q.36 if q.34 = yes

36. How could the Cyber Assessment Framework be improved?.....

Enforcement Regime

37. Are you aware that there is an enforcement regime associated with the NIS Regulations?
    - ❏ Yes

❏ No

Display q.38 if q.37 = yes

38. Has the enforcement regime (meaning the enforcement actions a Competent Authority can take, such as issuing an information notice, enforcement notice or penalty notice) led you to implement any improvements to the resilience of your essential service(s)?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

Display q.39 if q.37 = yes

39. Do you feel the current enforcement regime is proportionate to the risk of disruption to essential services in the event of an incident?
    - ❏ Yes
    - ❏ No
    - ❏ If no, please explain why not……...

Costs and Benefits

40. Before the introduction of the NIS regulations, how much on average did you invest annually in each of the following areas relating to the **security** of your Network and Information Systems for providing your essential service(s)?
    a. Internal staff costs (including wages and training)
    b. Physical security of IT and other systems relating to the delivery of your essential service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
    c. External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise)
    - ❏ No investment in this area
    - ❏ Less than £5,000
    - ❏ £5,0001 - £25,000
    - ❏ £25,001 - £50,000
    - ❏ £50,001 - £75,000
    - ❏ £75,001 - £100,000
    - ❏ £100,001 - £125,000
    - ❏ £150,001 - £175,000
    - ❏ £175,001 - £200,000
    - ❏ Over £200,000
    - ❏ Don't know

41. In the original NIS Impact Assessment, DCMS estimated expected costs to organisations associated with implementing the NIS regulations. Which of the

following costs, if any, has your organisation incurred as a result of the NIS regulations? Please select all that apply

- ❏ Cost of familiarising with the NIS Regulations and guidance documents
- ❏ Additional security spending relating to the security of your network and information systems
- ❏ Cost of incident reporting due to the NIS Regulations
- ❏ Additional compliance costs of reporting requirements to Competent Authorities e.g. completing the Cyber Assessment Framework, or other type of assessment
- ❏ Other administrative costs from enforcement activity e.g. engaging with your Competent Authority after an incident

42. Did you incur any unexpected costs that were not covered in the original NIS Impact Assessment (see Q41)?
    - ❏ Yes, please specify……..
    - ❏ No

43. In the original NIS Impact Assessment, DCMS estimated that following additional costs would be incurred by in-scope organisations as a result of the NIS regulations:
    - Costs of incident reporting due to the NIS Regulations *(£54 per incident - p.31 of the NIS impact assessment)*
    - Additional compliance costs of reporting requirements to Competent Authorities e.g. completing the Cyber Assessment Framework, or other type of assessment *(£80 for a small organisation, £275 for a medium sized organisation, and £549 for a large organisation - p.20 of the NIS impact assessment)*
    - Cost of familiarising with the NIS regulations and guidance documents *(£660.19 per organisation - p.17 of the NIS impact assessment)*

    Were these estimates accurate for your organisation
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

    Display q.44 if q.43 = no

44. If no, please clarify the number of hours, who was involved, how much this cost?

	Number of hours	Who was involved	Total cost (£)
Costs of incident reporting due to the NIS Regulations			
Additional compliance costs of reporting requirements to Competent Authorities			

e.g. completing the Cyber Assessment Framework, or other type of assessment

Cost of familiarising with the NIS regulations and guidance documents

45. As a result of the NIS Regulations, have you made or do you plan to make any additional security investments relating to your Network and Information Systems for providing your essential service(s)? Please select all that apply
    - ❏ We have made additional security investments relating to our network and information systems for providing our essential service(s)
    - ❏ We plan to make additional security investments relating to our network and information systems for providing our essential service(s)
    - ❏ No
    - ❏ Don't know

46. Which areas have you invested in, or plan to invest in, relating to the security of your Network and Information Systems for providing your essential service(s)?
    - ❏ Internal staff costs (including wages and/or training costs)
    - ❏ Physical security of IT and other systems relating to the delivery of your essential service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
    - ❏ External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise)
    - ❏ Other, please specify…
    - ❏ None of these

47. How much have you invested, or plan to invest in additional security measures in the following areas relating to your Network and Information Systems for providing your essential service(s)?
    a. Internal staff costs (including wages and training)
    b. Physical security of IT and other systems relating to the delivery of you essential service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
    c. External costs (including outsourcing the management of cyber security, hiring external consultants and expertise)
    - ❏ No investment in this area
    - ❏ Less than £5,000
    - ❏ £5,0001 - £25,000
    - ❏ £25,001 - £50,000
    - ❏ £50,001 - £75,000

- ❏ £75,001 - £100,000
- ❏ £100,001 - £125,000
- ❏ £150,001 - £175,000
- ❏ £175,001 - £200,000
- ❏ Over £200,000
- ❏ Don’t know

48. Have you passed any costs incurred as a result of the introduction of the NIS regulations on to consumers?
    - ❏ Yes
    - ❏ No
    - ❏ Not applicable - we do not charge for our services/do not control the prices we charge to our customers.
    - ❏ Don’t know

    Display q.49 if q.48 = yes

49. If yes, can you quantify these costs?.....

50. Have you incurred any of the following benefits as a result of implementing the NIS regulations? Please select all that apply
    - ❏ Improved understanding of your organisation’s aggregate risks
    - ❏ Updated general incident management processes
    - ❏ Increased board support for security
    - ❏ Sharing good practice with other RDSPs
    - ❏ Other, please specify……..
    - ❏ No unexpected benefits
    - ❏ Don’t know

Annex B: Questionnaire used to survey RDSPs

Introduction

In May 2018, the UK government introduced the Network and Information Systems (NIS) Regulations. These regulations were designed to improve the cyber and physical resilience of network and information systems for the provision of essential services and digital services. These regulations apply to operators of essential services (OESs) in the water, transport, energy, health and digital infrastructure sectors, as well as relevant digital service providers (RDSPs), which provide online marketplaces, online search engines and cloud computing services. Section 25(1) of the NIS Regulations requires the Secretary of State to carry out a review of the regulatory provision contained in the NIS Regulations and publish a report setting out its conclusions.

Purpose of the survey

A post-implementation review seeks to establish whether the regulations have achieved their original objectives and remain appropriate. In order to inform our assessment of the impact of the NIS Regulations, we are conducting a survey of organisations that are covered by the regulations. The information you provide as part of this survey will inform future policy making with regard to the NIS Regulations.

How your data will be used

Full information on how your personal data will be stored and used for this survey is contained in your Competent Authority privacy notice. Survey responses will be collected and stored securely by DCMS (as the Department responsible for the NIS Regulations), and will not be shared beyond the team responsible for managing this survey at DCMS, unless you give us permission to share your response with your Competent Authority and/or the NCSC, in order for them to understand how the implementation of the NIS Regulations can be improved. While we cannot guarantee full anonymity, as the number of OESs in some sectors is small, we will not ask for the name of your organisation and we will ensure that the final post implementation review report, which will be published, does not make public information which could identify any individual organisation.

You do not have to answer all of the questions, and you can skip any questions you cannot or would prefer not to answer, beyond the first four opening questions. Your Competent Authority may contact you again to ask if you would like to take part in further research to inform the post implementation review.

Freedom of Information

Under the FOIA (Freedom of Information Act (2000), there is a statutory Code of Practice with which public authorities must comply and which deals, among other things, with

obligations of confidence. In view of this, if you would like the information you provide in the survey to remain confidential, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. FOI exemptions may be applied to this data. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

How to answer the survey

The purpose of this survey is to evaluate the effectiveness of the NIS Regulations. Therefore, we would like you to answer the questions throughout the survey with specific regard to the NIS Regulations and your organisation's network and information systems resilience relating to the provision of your digital service(s), unless clearly specified otherwise. Please also bear in mind when completing the survey that the purpose of the survey is to understand your experience of implementing the NIS Regulations at your organisation; we do not require any information on any security vulnerabilities as the survey is not designed to test security resilience. Please do not provide information in your answers that you would classify as sensitive and/or contains personal data.

If you have any questions, please get in touch with your Competent Authority or the DCMS survey and policy team at nis@culture.gov.uk.

Please confirm below that you have read and understood this statement, about how your personal data will be collected and used, and agree with its terms. Please note that you have to answer this question before you are allowed to proceed with the survey.

- ❑ I confirm that I have read and understood this statement

DCMS will be collecting partial responses to the survey. If, during completion of the survey you decide to withdraw your response, you will need to contact DCMS Data Protection Team at dcmsdataprotection@culture.gov.uk asking that your response be deleted, please use the email subject heading 'Cyber Security NIS PIR review'. Please note we may require you to provide us with some of your answers to the survey in order to identify and thus delete your response.

Once you have submitted your response to the survey, you will not be able to withdraw your answers from the analysis stage.

If you need any further information related to the processing of your personal data please contact us: DCMS Data Protection Team at dcmsdataprotection@culture.gov.uk and specify which survey you have concerns about.

If you need any further information about the survey please contact your Competent Authority or the DCMS survey and policy team at nis@culture.gov.uk.

Please confirm that you have read the information above and you are happy to participate and continue with the survey.

- ❏ I have read the above information and am happy to participate in the survey

Are you content for your answers to be shared with the National Cyber Security Centre?

- ❏ Yes
- ❏ No

Are you content for your answers to be shared with your Competent Authority (the ICO)?

- ❏ Yes
- ❏ No

Background demographic

1. As a Relevant Digital Service Provider (RDSP), are you a:
    - ❏ Online marketplace
    - ❏ Online search engine
    - ❏ Cloud computing service
    - ❏ Other

2. What size is your organisation? Please note that small and micro sized organisations do not fall within the scope of the NIS Regulations for RDSPs
    - ❏ Medium (50-249 employees)
    - ❏ Large (250+ employees)

3. How long has your organisation been registered with the ICO as an RDSP?
    - ❏ less than 6 months
    - ❏ 6-12 months
    - ❏ over 12 months
    - ❏ Do not know

Impacts of the NIS Regulations

4. Prior to the NIS regulations, did you take any action to improve the security of your Network and Information Systems specifically relating to providing your digital service?
    - ❏ Yes
    - ❏ No
    - ❏ Don’t know

5. Prior to the legal obligation of the NIS regulations, what other reasons have caused you to implement changes to the security of your Network and Information Systems relating to the provision of your digital service(s) in the past?
    - ❑ Previously experienced a breach or attack
    - ❑ Media coverage of other organisations experiencing a breach or attack
    - ❑ To protect critical systems
    - ❑ To protect customer data
    - ❑ To protect intellectual property/trade secrets
    - ❑ To maintain business continuity
    - ❑ To avoid financial loss
    - ❑ To avoid reputational damage
    - ❑ To comply with requirements imposed by other businesses e.g. customer/ supplier standards
    - ❑ To respond to industry guidance (e.g. from NCSC or trade bodies)
    - ❑ To comply with data protection law (Data Protection Act 2018 and the GDPR)
    - ❑ To comply with other non-NIS regulations (excl. GDPR), please specify……..
    - ❑ To comply with other industry initiatives
    - ❑ Other, please specify……..
    - ❑ Don't know

Guidance

6. Do you know where to find guidance on NIS implementation and compliance?
    - ❑ Yes
    - ❑ No

    Display q.7 if q.6 = yes

7. Is this guidance easy to access?
    - ❑ Yes
    - ❑ No

8. Have you received appropriate guidance and support from your Competent Authority to implement the NIS regulations effectively?
    - ❑ Yes
    - ❑ No
    - ❑ If no, please explain……

9. What additional support or guidance from your Competent Authority or other sources would further assist you with the implementation of the NIS regulations?
    - ❑ Hold industry events
    - ❑ Provide information exchanges
    - ❑ Provide updates to the businesses
    - ❑ Other, please suggest here……

Security Risk Management

10. Prior to the NIS regulations, did you have any governance policies and/or processes to manage security risk of your Network and Information Systems?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

11. Have you made any changes to or strengthened your governance policies and/or processes to manage security risk as a result of the NIS regulations?
    - ❑ Introduced new policies/processes
    - ❑ Updated/strengthened existing policies/processes
    - ❑ No, but we intend to update/strengthen our policies/processes
    - ❑ No change, please specify why……..

12. Have the NIS regulations increased the prioritisation of security at a senior management level?
    - ❑ Yes
    - ❑ No

13. Please explain your answer……...

14. Do you feel there are any challenges to your organisation's ability to implement the NIS regulations?
    - ❑ Yes
    - ❑ No
    - ❑ If yes, please explain what these are……

Skills

15. Within your organisation, do you feel you have the in-house skills and capacity to deliver your obligations under the NIS Regulations?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

16. Did you take any of the following actions with regard to resourcing to support your implementation of the NIS regulations when they were introduced? Please select all options that apply.
    - ❑ Hired additional staff
    - ❑ Outsourced to specialist security consultants
    - ❑ Provided training for existing staff
    - ❑ Other, please specify……...
    - ❑ No external means used

17. As a result of the NIS regulations, have you retrained/up-skilled any existing staff or hired any new staff to manage security risks to your Network and Information Systems?
    - ❏ Yes
    - ❏ No, outsourced instead
    - ❏ No
    - ❏ Don't know

18. Are there any barriers that prevent you from conducting effective risk management of your suppliers (and your wider supply chain e.g. supplier's suppliers)?
    - ❏ Yes
    - ❏ No
    - ❏ If yes, please explain why……...

19. Do you feel you have the resources to manage risks to the security of your Network and Information Systems arising from your suppliers (and your wider supply chain e.g. supplier's suppliers)?
    - ❏ Yes, we have the resources to manage the risk from our direct suppliers and our wider supply chain
    - ❏ Yes, we have the resources to manage the risk from our direct suppliers but not from the wider supply chain
    - ❏ No, managing supplier risk is not a priority
    - ❏ No, we are unsure how to manage risk from our direct suppliers and our wider supply chain
    - ❏ No, we do not have the resources
    - ❏ Other, please specify……...

Incidents and incident reporting

20. Prior to the NIS regulations, did you have any processes and/or procedures in place for recovery from a security incident relating to the Network and Information Systems used for the provision of your digital service(s)?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

21. Have you introduced or strengthened existing processes and/or procedures for recovery from a security incident as a result of the NIS regulations?
    - ❏ Introduced new processes/procedures
    - ❏ Strengthened existing processes/procedures
    - ❏ No, but we intend to introduce/strengthen our processes/procedures
    - ❏ None of the above

Display q.22 only:

If Q21 = Introduced new processes/procedures

And Q21 = Strengthened existing processes/procedures

22. Were these new processes influenced or affected by the GDPR?
    - ❑ Yes
    - ❑ No

23. Which of the following areas have you taken action as a result of the NIS regulations with regard to incident response? Please select all that apply
    - ❑ Risk assessment that takes account of your digital service
    - ❑ Up to date incident response plan
    - ❑ Understand the resource requirements required to enact your incident response plan
    - ❑ Carry out regular exercises to test your incident response plan
    - ❑ Other, please specify…….
    - ❑ No action taken

24. Are you aware of the incident reporting thresholds for your sector?
    - ❑ Yes
    - ❑ No

25. Is the current deadline of 72 hours from discovery of an incident which meets the reporting threshold sufficient time to report an incident to your Competent Authority?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know
    - ❑ If no, please explain why: ……..

26. Do you think the incident identification thresholds for reporting NIS incidents are appropriate for your sector?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know
    - ❑ If no, please explain why: ……..

27. Since the implementation of the NIS regulations, how has your attitude towards voluntary reporting of an incident that is under the reporting threshold changed towards
    a) your Competent Authority?
    b) the NCSC?

    - ❑ More likely to voluntarily report
    - ❑ Less likely to voluntarily report
    - ❑ Stayed the same
    - ❑ Do not have a voluntary reporting process

28. Please explain your answer…….

Lessons learned

29. Did your organisation find it easy to identify yourself as in scope of the NIS Regulations?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

30. To what extent has applying the NIS security principles impacted positively on the following with regard to the provision of your digital service(s) in your organisation? (-2= extremely negative, -1 = somewhat negative, 0= neither positive nor negative, 1= somewhat positive, 2= extremely positive)
    - ❏ Awareness of security amongst employees
    - ❏ Security standards within your organisation
    - ❏ Understanding of key assets and critical systems
    - ❏ Processes to respond to security breaches and attacks
    - ❏ Security guidance you produce within your organisation
    - ❏ Security training for staff
    - ❏ Understanding of your responsibilities in managing your security risks
    - ❏ Confidence in understanding your organisations' security risks

31. Are you aware that there is an enforcement regime associated with the NIS Regulations?
    - ❏ Yes
    - ❏ No

    Display q.32 if q.31 = yes

32. Has the enforcement regime (meaning the enforcement actions a Competent Authority can take, such as issuing an information notice, enforcement notice or penalty notice) led you to implement any improvements to the resilience of your digital service(s)?
    - ❏ Yes
    - ❏ No
    - ❏ Don't know

    Display q.33 if q.31 = yes

33. Do you feel the current enforcement regime is proportionate to the risk of disruption to Relevant Digital Service Providers if there is an incident?
    - ❏ Yes
    - ❏ No
    - ❏ If no, please explain why not……...

Costs and Benefits

34. Before the introduction of the NIS regulations, how much on average did you invest annually in each of the following areas relating to the **security** of your Network and Information Systems for providing your digital service(s)?
    a. Internal staff costs (including wages and training)
    b. Physical security of IT and other systems relating to the delivery of your digital service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
    c. External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise)

    ❏ No investment in this area
    ❏ Less than £5,000
    ❏ £5,0001 - £25,000
    ❏ £25,001 - £50,000
    ❏ £50,001 - £75,000
    ❏ £75,001 - £100,000
    ❏ £100,001 - £125,000
    ❏ £150,001 - £175,000
    ❏ £175,001 - £200,000
    ❏ Over £200,000
    ❏ Don't know

35. In the original NIS Impact Assessment, DCMS estimated expected costs to organisations associated with implementing the NIS regulations. Which of the following costs, if any, has your organisation incurred as a result of the NIS regulations? Please select all that apply
    ❏ Cost of familiarising with the NIS Regulations and guidance documents
    ❏ Additional security spending relating to the security of your network and information systems
    ❏ Cost of incident reporting due to the NIS Regulations
    ❏ Additional compliance costs of reporting requirements to Competent Authorities e.g. completing the Cyber Assessment Framework, or other type of assessment
    ❏ Other administrative costs from enforcement activity e.g. engaging with your Competent Authority after an incident

36. Did you incur any unexpected costs that were not covered in the original NIS Impact Assessment (see Q35)?
    ❏ Yes, please specify……..
    ❏ No

37. In the original NIS Impact Assessment, DCMS estimated that following additional costs would be incurred by in-scope organisations as a result of the NIS regulations:
    - Costs of incident reporting due to the NIS Regulations *(£54 per incident - p.31 of the NIS impact assessment)*

- Additional compliance costs of reporting requirements to Competent Authorities e.g. completing the Cyber Assessment Framework, or other type of assessment *(£80 for a small organisation, £275 for a medium sized organisation, and £549 for a large organisation - p.20 of the NIS impact assessment)*
- Cost of familiarising with the NIS regulations and guidance documents *(£660.19 per organisation - p.17 of the NIS impact assessment)*

Were these estimates accurate for your organisation

- ❏ Yes
- ❏ No
- ❏ Don't know

Display q.38 if q.37 = no

38. If no, please clarify number of hours, who was involved, how much this cost?

	Number of hours	Who was involved	Total cost (£)
Costs of incident reporting due to the NIS Regulations			
Additional compliance costs of reporting requirements to Competent Authorities e.g. completing the Cyber Assessment Framework, or other type of assessment			
Cost of familiarising with the NIS regulations and guidance documents			

39. As a result of the NIS Regulations, have you made or do you plan to make any additional security investments relating to your Network and Information Systems for providing your digital service(s)? Please select all that apply
    - ❏ We have made additional security investments relating to our network and information systems for providing our digital service(s)
    - ❏ We plan to make additional security investments relating to our network and information systems for providing our digital service(s)
    - ❏ No
    - ❏ Don't know

40. Which areas have you invested in, or plan to invest in, relating to the security of your Network and Information Systems for providing your digital service(s)?
    - ❏ Internal staff costs (including wages and/or training costs)

- ❏ Physical security of IT and other systems relating to the delivery of your digital service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
- ❏ External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise)
- ❏ Other, please specify…

41. How much have you invested, or plan to invest in additional security measures in the following areas relating to your Network and Information Systems for providing your digital service(s)?
    a. Internal staff costs (including wages and training)
    b. Physical security of IT and other systems relating to the delivery of you essential service(s) (including purchasing new/updating existing hardware and/or software, physical security measures)
    c. External costs (including outsourcing the management of cyber security, hiring external consultants and expertise)
    - ❏ No investment in this area
    - ❏ Less than £5,000
    - ❏ £5,0001 - £25,000
    - ❏ £25,001 - £50,000
    - ❏ £50,001 - £75,000
    - ❏ £75,001 - £100,000
    - ❏ £100,001 - £125,000
    - ❏ £150,001 - £175,000
    - ❏ £175,001 - £200,000
    - ❏ Over £200,000
    - ❏ Don’t know

42. The Data Protection Act 2018 (DPA), and General Data Protection Regulation (GDPR), set out the legal framework relating to the protection of individuals’ personal data. Were any of the NIS related investments in your organisation closely linked to measures taken by your organisation to comply with the DPA 2018 and the GDPR?
    - ❏ Yes
    - ❏ No
    - ❏ Don’t know

43. Have you passed any costs incurred as a result of the introduction of the NIS regulations on to consumers?
    - ❏ Yes
    - ❏ No
    - ❏ Don’t know

Display q.44 if q.43 = yes

44. If yes, can you quantify these costs?.....

45. Have you incurred any of the following benefits as a result of implementing the NIS regulations? Please select all that apply
    - ❑ Improved understanding of your organisation's aggregate risks
    - ❑ Updated general incident management processes
    - ❑ Increased board support for security
    - ❑ Sharing good practice with other RDSPs
    - ❑ Other, please specify……..
    - ❑ No unexpected benefits
    - ❑ Don't know

Member State Considerations

46. Do you operate in any EU member states other than the UK?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

47. Has the cost of implementing the NIS regulations in your organisation in the UK differed from the implementation costs in other EU member states in which you operate?
    - ❑ Yes
    - ❑ No
    - ❑ Don't know

    Display q.48 if q.47 = yes

48. Please explain your answer…….

49. Have the actions taken to implement the NIS regulations in your organisation in the UK differed from those taken to comply in other EU member states in which you operate?
    - ❑ Yes, please specify…….
    - ❑ No

Annex C: Competent Authority Report

Purpose of the report

As previously outlined in the NIS Review scope and governance document, two key workstreams will feed into the NIS Statutory Review:

1. **Workstream One** looking at the effectiveness, costs and benefits of the NIS regulations, and

2. **Workstream Two** which looks at implementation and whether changes should be made to the regulations to enable Competent Authorities to implement NIS as effectively as possible.

Your responses to this report will form a crucial part of the official data we are collecting to inform the review.

Reports completed and returned by Competent Authorities (CAs), which may include Co-Competent Authorities with a Lead Government Department, will be stored securely by DCMS. You do not have to answer all of the questions; you can leave any questions you cannot or would prefer not to answer blank.

Responses will be handled at OFFICIAL-SENSITIVE level of data classification. Therefore please do not disclose any information which might be classified as 'SECRET'.

Freedom of Information

Under the FOIA (Freedom of Information Act 2000), there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, if you would like the information you provide in the survey to remain confidential, it would be helpful if you could explain to us why you regard the information you have provided as confidential.

If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. FOI exemptions may be applied to this data. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

Please confirm that you are happy to participate in the research and answer the following report questions below.

I confirm that I have read the above information and I am happy to participate in the CA/LGD report research [Yes/No]

1. Name of Competent Authority

Please include name here.

.

2. Which geography do you cover?
    - ❏ UK wide
    - ❏ Scotland
    - ❏ England
    - ❏ Wales
    - ❏ Northern Ireland

3. How many OES or RDSPs do you regulate?

Please add number here.

Impact to date

4. Were you working with the organisations in scope of NIS in your sector / region regarding security of network and information systems before the NIS Regulations came into force in May 2018?
    - ❏ Yes
    - ❏ No

    [IF YES] Please explain the previous level of engagement with them regarding network and information systems security relating to the delivery of their essential/digital service.

Please give further details here:

5. Have you observed any improvement in the levels of security of network and information systems at your OES/RDSPs relating to the delivery of their essential/digital service(s) since NIS came into force?
    - ❏ Yes
    - ❏ No

[IF NO] If you have not observed improvements in the organisations you regulate, do you have any views regarding why this could be (for example, cost issues, lack of capacity or understanding of how to improve, lack of prioritisation of cyber security, lack of availability of cyber security expertise on the market)?

Please give further details here:

[IF YES] If you have observed improvements, in which key areas have improvements been made, and what do you think were the key drivers behind these improvements?

Please give further details here:

6. In your view, if the NIS Regulations no longer existed, would improvement in the security of network and information systems among OES & RDSPs continue, and at the same pace?
    - ❏ Yes
    - ❏ Yes, but at a slower pace
    - ❏ No

    [If Yes], please explain your answer:

Please give further details here:

[If Yes, but at a slower pace] please explain your answer:

Please give further details here:

[If No] please explain your answer:

Please give further details here:

Costs & benefits incurred by you as a result of the implementation of NIS

7. Please estimate the initial one-off implementation costs incurred by your organisation as a result of becoming a Competent Authority under the NIS regulations?

Please give further details here:

8. Please estimate below your annual costs to date incurred as a result of the implementation of the NIS Regulations.

Please give further details here:

9. Please estimate the ongoing costs you expect to incur per annum in the future as a result of becoming a Competent Authority under the NIS Regulations.

Please give further details here:

Costs & benefits for the organisations you regulate

10. Do you expect the costs of complying with the NIS regulations to increase in the future for the organisations you regulate?
    - ❑ YES
    - ❑ NO

Please explain why here:

11. In your view, are there any ways that the current cost burden of compliance for organisations regulated under NIS could be reduced?

Please give further details here:

12. Do you have any small businesses in scope of NIS in your sector / region?
    - ❏ Yes
    - ❏ No

    IF YES, have you observed a cost impact on small businesses you regulate which has had a disproportionate impact on these businesses as opposed to the larger businesses you regulate?

    - ❏ Yes
    - ❏ No

If YES, please give further details here:

13. Please indicate whether you believe the following benefits have been realised as a result of the implementation of NIS to date (please select all that apply):
    - ❏ OES/RDSPs you regulate taking action to improve the security of their network and information systems
    - ❏ OES/RDSPs you regulate have improved governance processes in relation to the security of their network and information systems
    - ❏ Improved incident management processes at the organisations you regulate
    - ❏ Increased prioritisation of security of network and information systems at board level in the organisations you regulate
    - ❏ Greater information sharing on threats and incidents through the NIS Cooperation Group with each EU member state represented
    - ❏ Increased investment in security of network and information systems of the organisations you regulate, both staff and in IT/OT/ICT
    - ❏ A closer working relationship between OES/RDSP and Competent Authorities
    - ❏ Other (please specify in the box below)

OTHER: Please give further details here.

14. What reasons, in your opinion, have prevented any of the above benefits from being realised in your sector/region?

    - ❏ The regulations have not been in place for long enough to realise all of the benefits
    - ❏ The regulations do not reach the right organisations
    - ❏ The regulations have not sufficiently motivated / provided the right incentives for organisations to make the expected improvements to their security
    - ❏ Organisations in scope do not understand how to properly implement the regulations
    - ❏ Information sharing with other member states has not been possible or has not been helpful
    - ❏ The regulations do not offer an appropriate enforcement regime for these measures
    - ❏ There is a lack of relevant skills and/or expertise in the organisations you regulate
    - ❏ The regulations are not ambitious enough or do not cover enough aspects to adequately address the security threats in your sector / region
    - ❏ Other (please specify in the box below)

OTHER: Please give further details here.

15. In your view, have there been any unexpected positive consequences as a result of the implementation of the NIS Regulations?

Please give further details here:

16. In your view, have there been any unexpected negative consequences as a result of the implementation of the NIS Regulations?

Please give further details here:

Specific policy questions

17. Do you have the right tools to implement the regulations effectively?
    - ❑ Yes
    - ❑ No

If NO, please give further details here:

18. Do you believe that all of the right organisations can be designated within the current framework of thresholds?
    - ❑ Yes
    - ❑ No

If NO, please give further details here:

19. Are you confident that all organisations which fall within the scope of the current regulations for your sector / region have been designated?
    - ❑ Yes
    - ❑ No

If NO, please give further details here:

20. What are your views on the current **incident reporting** thresholds for your sector / region? Are they set at an appropriate level?

Please give further details here:

21. Do you believe that the regulations adequately offer information-sharing provisions to allow effective domestic collaboration between NIS Competent Authorities?
    - ❑ Yes

❏ No

If NO, please give further details here:

Capacity & capability

22. Do you feel you have all of the skills & expertise required internally to be able to effectively regulate your sector / region under NIS?
    ❏ Yes
    ❏ No

If NO, please explain here:

23. Do you feel you have the capacity internally to be able to effectively regulate your sector / region under NIS?
    ❏ Yes
    ❏ No

If NO, please explain here:

24. What further guidance and support from DCMS would be helpful in supporting you to effectively regulate NIS? Some examples are included below:

    ❏ Further guidance on NIS implementation across all sectors in the UK;

    ❏ Developing a NIS work programme to further support capability building and sharing;

    ❏ Working with NCSC to develop a more consistent skills / training framework for NIS compliance teams;

    ❏ Other (please specify in the box below)

OTHER: Please give further details here.

25. Is there anything else you would like to highlight to feed into the NIS Statutory Review, which has not already been covered?

Please give further details here.

Annex D: Assumptions Log

Assumption	Description of assumption
Number of organisations in scope of NIS	We have estimated the number of OESs and RDSPs in scope of the NIS regulations based on evidence provided by Competent Authorities (CAs). It has been assumed that this number will remain constant over the appraisal period, however this number could change, as new organisations could be designated if they reach the thresholds, and any potential amendments to designation thresholds could also have an impact. Costs to public sector OESs will fall on the government.
Proportion of OESs that are public sector organisations	The proportion of OESs that are in the public sector has been estimated based on evidence provided by CAs. It has also been assumed that this proportion will remain constant over the appraisal period.
Wage inflation	ASHE revised estimates have been used to calculate wage costs for the years 2016, 2017 and 2018. The average annual nominal growth rate in median wages for different occupations from 2019 until the end of the appraisal period has been estimated by taking the average of the difference between 2013 and 2018 ASHE wage data for legal professionals, IT professionals, managers and directors, and all employees.
Wage overheads	Overhead charges of 30% have been added to the wages, in accordance with the International Standard Cost Model Manual.
Discount rate	Total costs have been deflated to 2016 prices and a discount rate of 3.5% applied to future costs to account for the time preference of money, in line with HMT Green Book guidance.
Physical security costs	It has been assumed that physical security costs would have been a one off investment cost at the start of the appraisal period.
Other additional security costs	It has been assumed that internal and external security costs will be an annual cost incurred by OESs and RDSPs. Survey data (from OES and RDSPs) has been used to estimate the proportion of OESs and RDSPs that invest in each of the cost categories and the value of this investment. It has been assumed that the distribution of those organisations that invest and the value of this investment will be the same across organisations that said that they did not know or did not respond to the survey, as those that did. Sensitivity analysis has been conducted in line with HMT Green Book guidance to account for the cost bands reported in the survey, using the high middle and low cost figures for each

	band.
Incident reporting costs	The average number of incidents has been assumed to be 39 per year over the appraisal period. Sensitivity analysis in line with HMT Green Book guidance was conducted using the survey results to give a high estimate of 99 incidents per year to account for uncertainty in the future number of incidents occurring on average per year.
Additional reporting costs	It has been assumed in all scenarios that all OESs will complete the CAF or similar assessment after year 2 of the appraisal period. Assessments take place regularly, and it has been assumed for the purposes of the analysis presented in the PIR that this is annual. However, it is up to individual CAs to decide how regularly this takes place.
CA wage inflation	It has been assumed that CA wage inflation will be equal to the general inflation rate, as Competent Authorities are government departments, agencies, or public sector bodies.
CA wage costs	Where only job roles were provided by CAs for setting up/operating costs, the mid point of DCMS 2019/20 pay bands were used to estimate the cost. Sensitivity analysis has been conducted in line with HMT Green Book guidance to account for changes in the future costs faced by CAs by varying costs by 20%.
Future CA costs	Where future costs of operating CAs were not provided, it has been assumed that the current annual reported cost will remain constant for the remainder of the appraisal period. Sensitivity analysis has been conducted in line with HMT Green Book guidance to account for changes in the future costs faced by CAs by varying costs by 20%.

CCS0320329850

978-1-5286-1939-4