2nd Post Implementation Review of the Network and Information Systems Regulations 2018

Summary

Introduction

The Network and Information Systems (NIS) Regulations 2018 are a set of regulations that were originally derived from an EU Directive[1]. The Regulations are in place to help ensure that the UK economy is resilient against cyber attacks by raising the level of security of providers of essential services that citizens and businesses rely on. The outcome-based nature of the Regulations allow aspects of the regulations to change and adapt in a rapidly evolving environment.

This Post-Implementation Review is the second review on the NIS Regulations. The review aims to build on the evidence set out in the 2020 Post-Implementation Review in assessing how effective the Regulations have been in achieving the original objectives to date and whether those objectives remain appropriate for the UK, four years after the implementation of the Regulations domestically.

This review will also set out what the costs and benefits of the Regulations have been to date, as well as setting out the limitations in what can be realistically assessed This review comes after the government has published and is consulting on a set of proposals to amend the NIS Regulations. The evidence base for these changes is based on the 2020 Post-Implementation Review, as well as early findings from this review. Having set the evidence and findings, this document will also discuss whether we should retain this EU-derived legislation following the UK's exit from the EU, highlight areas of improvement, next steps, and how the proposed measures contribute to the objectives of the Regulations.

Background

The overarching objective of the NIS Regulations, which came into force on 10 May 2018, is to improve the security of those network and information systems that are critical to the provision of essential services and certain digital services. The Regulations set out legal measures required to boost the overall level of security of network and information systems of organisations in scope. The Impact Assessment of the NIS Regulations highlights the rationale for intervention, in addition to the objectives, costs and benefits.

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. In this sense, the Finance and banking sectors were excluded from the UK transposition of the NIS Directive.

The Regulations apply to Operators of Essential Services in the transport, energy, water, health, and digital infrastructure sectors as well as to relevant Digital Service Providers. The Regulations specify that - if falling within the designation thresholds - an operator of essential service or relevant digital service provider 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.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

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 (NCSC).

Key findings and conclusions

The Regulations are largely working successfully in achieving the objectives that were set out in the 2018 Impact Assessment "to prevent (where possible) and improve the levels of protection against network and information systems incidents". It is recommended that the legislation be retained. The Regulations are a vital framework in raising the wider UK resilience against network and information systems security threats, and are actively contributing to the ambitions of the National Cyber Strategy. Following our exit from the EU, the UK has the opportunity to ensure that the Regulations are tailor-made to its own needs, in line with UK national objectives and ambitions set out in the National Cyber Strategy and the Integrated Review.

It has not been possible to assess how the NIS Regulations have impacted the number of incidents faced by these critical firms, as it is not possible to build a good counter-factual position as to the number of incidents that would have occurred without the Regulations. Competent authorities have nevertheless improved the cyber resilience of some critical organisations through improvement plans, suggesting that without the regulations there would be more vulnerabilities in these organisations that could be exploited and bring harm to the economy.

Findings suggest that the current form of the Regulations is the most appropriate form of government intervention. Furthermore, the Regulations are proportionate and targeted and not overburdensome. Finally, cyber risks to these relevant organisations still exist, so the Regulations are very much needed to ensure that the UK can continue to increase resilience to the cyber threats it faces.

However, this Review still finds room for improvement:

- Further work is required to ensure that the guidance makes it easy to identify whether firms are in or out of scope of the Regulations and to ensure that organisations that need to be included in the regulations are designated.

- There should be more done to secure the supply chains of operators of essential services, where the supplier is critical to the provision of that essential service.

- Competent authorities also need more resources to carry out what they deem to be an effective job of enforcing the Regulations.

- The Regulations are not effective at capturing the right cyber incidents that occur in the sectors regulated, work needs to be done to ensure that the right incidents are captured.

- DCMS needs to conduct work to assess why the enforcement regime is not being utilised where it is merited.

- Finally, greater consistency in regulatory implementation across sectors is required, alongside the creation of performance metrics so that we can better measure the impact and effectiveness of the Regulations.

Next steps

DCMS is currently in the process of consulting on a number of legislative changes that intended to improve the effectiveness of the Regulations in meeting its objectives. The consultation measures will address some of the issues outlined in this Review. Whilst the early evidence from this Review fed into the policy development at the consultation stage, the full findings will help further shape the policy measures as the policies develop.

DCMS should take steps to become a more effective coordinating authority in the implementation of the NIS Regulations. New guidance will be issued to provide further clarity where gaps currently exist, and stakeholder engagement will continue with the competent authorities, to facilitate a more consistent approach across different sectors to the NIS Regulations, as well as ensuring that the regime delivers against national objectives, such as the 2022 National Cyber Strategy. Whilst the next Post-Implementation Review is not scheduled until 2027, DCMS will remain in regular contact with regulators and their lead government departments to ensure that the NIS Regulations are continually developed in line with the emerging threat picture.

Title: The Network and Information Systems Regulations 2018	Post Implementation Review
PIR No:	**Date:** 25/03/2022
Original IA/RPC No: RPC-4066(2)-DCMS	**Type of regulation: EU**
Lead department or agency: Department for Digital, Culture, Media & Sport (DCMS)	**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**
Contact for enquiries: The NIS Policy Team (NIS@DCMS.gov.uk)	**Recommendation: Amend** **RPC Opinion:** Fit for purpose

1. What were the policy objectives of the measure? (Maximum 5 lines)

The Network and Information Systems Regulations 2018 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? (Maximum 5 lines)

DCMS conducted online surveys of the organisations in scope of the Regulations and all organisations in scope were contacted via their respective regulatory authorities. Participation was voluntary. There were 82 responses, or a response rate of 14% across both operators of essential services and relevant digital service providers, 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? (Maximum 5 lines)

DCMS evidence shows that there have been improvements in the cyber security of the sectors regulated by the NIS Regulations, and that the regulations have been successful in driving these changes, but there is more that could be done. The attempts to reduce the asymmetry of information between firms and the NCSC has only been partially achieved, this is due to the definition of a NIS incident not covering all cyber incidents, so the NCSC are working on limited information. Firms are addressing their cyber resilience by increasing their spending and introducing or improving policies to deal with cyber risks. 61 (14% of designated operators of essential services) operators have confirmed that they have put improvement plans in place to reduce vulnerabilities, with the longer term aim of reducing their, and subsequently the UK economy's, exposure to cyber risk.

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: Mark WIngham (delegated by Chief Economist) Date: 14/03/2022
Signed: Julia Lopez, MP Date: 25/03/2022

Further information sheet

Please provide additional evidence in subsequent sheets, as required.

4. What were the original assumptions?(Maximum 5 lines)

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? (Maximum 5 lines)

There is little evidence to suggest that there have been any significant unintended consequences. There has been an indication that the original cost assumptions were too low. In addition, there is an indication that organisations in scope may be reluctant to report incidents for fear of financial penalties; the reporting of such an incident is not, in itself, a reason for a penalty. It is expected that better guidance and information-sharing will tackle this issue.

6. Has the evidence identified any opportunities for reducing the burden on business? (Maximum 5 lines)

Better collaboration between regulated bodies such as the sharing of policies and good practices and other shared industry initiatives could lead to efficiencies. i.e. common supplier procurement frameworks. Streamlining regulatory processes such as Cyber Assessment Framework assessments would also reduce the burden on businesses. More proactive work on the behalf of competent authorities to identify common areas for improvement across sectors that could be supported by more targeted guidance. A more consistent cross-sector approach would be required (led by DCMS or lead government departments) to support competent authorities' actions and provide better read-across between how different regulators implement the regulations in different sectors. Cost savings on delivering specialised cyber training for all regulators rather than each competent authority negotiating their own NIS training programmes will also contribute to lower costs across competent authorities.

7. How does the UK approach compare with the implementation of similar measures internationally, including how EU member states implemented EU requirements that are comparable or now form part of retained EU law, or how other countries have implemented international agreements? (Maximum 5 lines)

Member States transposed the Directive differently. The UK's approach was to minimise costs to businesses where possible whilst remaining within the confines of the Directive. This meant that each proposed sector was assessed to make sure that it was not already subject to equivalent or more stringent regulatory requirements.

This translated into relatively fewer sectors in scope of NIS in the UK (the banking and finance sectors already had equivalent legislation in place). Most Member States implemented a sole competent authority for NIS approach, although some others did go with multiple competent authorities like the UK. Having a single competent authority allows for greater focus and clarity on cyber security advice and guidance in some instances, but the UK approach of having multiple competent authorities for some sectors allows them to have a better breadth of knowledge in the sectors which they are responsible for.

Full Report

Post Implementation Review of the Network and Information Systems Regulations 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. 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 underlying obligation (in this case the EU NIS Directive 2016) is being implemented in other countries which are subject to it.

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

This PIR will follow the guidance set out in ‘Producing post-implementation reviews: principles of best practice’ produced by the Department for Business, Energy, and Industrial Strategy (BEIS) Better Regulation Executive (BRE). This review will aim to answer the following 4 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.
    a. **If this regulation is still required,** what refinements could be made? (What scope is there for simplification and/or improvements?)
    b. **If this regulation is not required,** but government intervention in some form is, what other regulation or alternatives to regulation would be appropriate?

c) The policy cycle

To date there have been several pieces of analysis carried out on the NIS Regulations. The following documents have all been produced by DCMS:

- The final impact assessment, carried out in 2018;
- The 1st Post Implementation Review of the Network and Information Systems Regulations (2018), dated May 2020; and
- The pre-consultation impact assessment on legislative proposals to improve the UK's cyber resilience, carried out in 2021.

The pre-consultation impact assessment on legislative proposals to improve the UK's cyber resilience looks at 7 policy measures to amend the NIS Regulations. The document uses evidence from the first post-implementation review and preliminary outcomes from this review, in addition to other sources, to produce a rationale for change. As the department continues development of these policy options after the consultation, DCMS will ensure that the findings of this review are fully incorporated into the final impact assessment.

The seven amendments that have been put forward in the January 2022 consultation are:

- expanding the scope of 'digital services ' to include 'managed services';
- applying a two-tier supervisory regime for all digital service providers: a new proactive supervision tier for the most critical providers, alongside the existing reactive supervision tier for everyone else;
- creating new delegated powers to enable the government to update the regulations, both in terms of framework but also scope, with appropriate safeguards;
- creating a new power to bring certain organisations, ones that entities already in scope are critically dependent on, within the remit of the NIS Regulations;
- strengthening existing incident reporting duties, currently limited to incidents that impact on service, to also include other significant incidents; and
- extending the existing cost recovery provisions to allow regulators (for example, Ofcom, Ofgem, and the ICO) to recover the entirety of reasonable implementation costs from the companies that they regulate.

More information can be found about these amendments in either the consultation or the cyber measures impact assessment.

The research for this post-implementation review was carried out at a stage where it could be used to help develop the legislative proposals above. Evidence from the review was used to test the assertions made in the proposed amendments and in some cases found evidence that further supported the case for some of the amendments. Where the recommendation of this review is to amend the legislation, it will be stated whether this will be done by the proposed cyber security measures or whether further or different amendments are required.

d) Previous RPC feedback

This review will also look to build on the weaker sections of evidence that the Regulatory Policy Committee has highlighted in previous impact assessments and reviews focused on the NIS Regulations 2018. The feedback that is relevant to this review can be seen detailed below:

1) **Whether the Directive affects the price of essential services and the number of workers employed by essential service providers.** This PIR collected evidence in the surveys to determine how many of the organisations have passed on the costs of these regulations to the end user through higher costs of services. This evidence has been demonstrated in the costs section of this Post-Implementation Review (Section 6, p. 41). For some organisations this question is not relevant as they don't have a price of their goods and services, as like the health organisations, a lot of these are free at the point of service. The Review has found that more people have likely been employed by the NIS regulated organisations as a result of the NIS Regulations.

2) **Whether the measures will have a disproportionate impact on small businesses.** This review looked to collect the responses from all the organisations that are regulated by the NIS Regulations, including any small firms. The review also asked the regulators how many small organisations that are regulated in their sector or region are small. This review has found that there are no known small businesses regulated by these regulations so there is no direct impact to small businesses. Further analysis on this impact can be found in Section 6 (p. 41-42)

3) **Whether costs will differ among essential service providers from different sectors (e.g. energy, transport, and health care).** This review will identify if there are any differences between sectors. The questionnaires asked what sectors the regulated firms operated in to enable the analysis team to present any sector-specific analysis; this will be covered in the costs section of this document. This can be found in Section 6 (p. 42).

4) **More details about implementation of the Directive (e.g. how non-EU firms in the UK will be bound by the regulation, and why banking and financial sectors are exempt from the regulations).** The NIS Regulations are designed to ensure that the UK's essential services are resilient. Where sectors already have a strong and effective regulatory regime there is no need to bring them within the scope of the NIS Regulations. The banking and financial services sectors are heavily regulated, with a strong focus on cyber security and based on this assessment their inclusion within the NIS Framework was not required. Something that has been identified by the last post-implementation review was that there is a need for the government to be able to amend the regulations to counter emerging threats and protect the UK economy. The recent consultation therefore includes a measure to enable the government to amend the NIS Regulations via secondary legislation. Organisations based outside of the UK, but offering services that would otherwise be covered by the regulations to UK citizens and businesses, are required to uphold their duties under these regulations and designate representatives in the UK for this purpose.

5) **Whether the impact assessment has considered all the potential costs and benefits (e.g. the costly interaction between the NIS Directive, UK General Data Protection Regulation and the DPA 2018 and the ePrivacy Directive, establishment costs for sectoral-competent authorities, and the increase in revenue of digital service providers from providing security services to essential service providers).** This review identifies the overlaps with the other regulations that impact the same firms. The main regulatory overlap is with the UK General Data Protection Regulation and Data Protection Act 2018. The impact of this is further addressed in Section 6 (p.42-43) .

6) **Response rate - whilst the Department has done well to gather the data from 14% of those surveyed (page 14), the review would have benefited from outlining future plans to improve and increase the response rates to future surveys. The Department should further explore how best to ensure that results at the next review point are more representative of the population of relevant stakeholders and how they will achieve fuller results.** The lack of a pre-election period during this review, as opposed to the 2020 Post-Implementation Review, allowed the use of reminder emails to try and encourage firms to take part in the review. Several reminders were sent out during the survey period via competent authorities, but unfortunately survey participation was lower than in the last review. The impacts of the covid-19 pandemic cannot be ignored as a potential reason for lower response rate. Additionally, as the regulations have been in force for 4 years, there could be less interest in the implementation of the regulations.

7) **Costs - the PIR states that *"overall, only 11% of OESs and 17% of relevant digital service providers agreed with the assessment and that the costs in the Impact assessment were accurate for their organisations.",* and that *"68% of OESs and 56% of relevant digital service providers were unsure, responding that they did not know, even though organisations reported incurring these types of costs*" (page 26). The Department should therefore discuss how they intend to receive further data from the impacted parties in the future review. The PIR would also benefit from discussing how an updated monitoring and evaluation plan would improve the response rate from stakeholders.** The 2020 Post-Implementation Review did not consider the responses of those firms that said they did not agree with the impact assessment costs as from the responses it was not clear whether they responded on an annual or other time period basis (e.g. per incident report). For this review, the questions were clearly signposted to show that it is referring to annual cost. All responses were incorporated and costs outlined in the Impact Assessment were estimated using a weighted average of responses from the respondents that agreed and those that didn't. A full explanation can be found in the costs section of this review (Section 6, p.31-34).

8) **Familiarisation costs - the Department concedes that "*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.*" Whilst the RPC commends the Department in attempting to assess these costs via their survey and consultation, again the PIR would benefit from a clearer explanation of why the Department has been unable to provide further information.** This PIR collected evidence in the surveys to determine the familiarisation costs that organisations incurred in implementing the NIS Regulations. This evidence has been taken into account in the estimates provided and is addressed in the cost section of this PIR (Section 6, p. 32).

e) 2020 Post-Implementation Review Errors

DCMS ensures that there is quality assurance of all the documents it publishes, as it did with this Review and the 2020 Post-Implementation Review. Whilst conducting the analysis for this review, analysts also reviewed the previous work as part of the 2020 Post-Implementation Review, to see what improvements could be made to the previous modelling. During the review of the previous work, analysts found 2 errors in the previous calculations that caused a miscalculation in the 2020 Post-Implementation Review. Approaches to the estimation of the costs and benefits were appraised and improvements to the methodology were made. These changes will be highlighted in the costs and benefits section of this document.

2) The objectives and intended outcomes of the Regulations

Policy background: implementation of the NIS Regulations

The Network and Information Systems Regulations 2018 (NIS Regulations) came into force on 10 May 2018 and are aimed at improving the level of security of organisations that provide essential services to the UK, as well as some digital services. The NIS Regulations apply to operators of essential services in the transport, energy, water, health, and digital infrastructure services as well as to online marketplaces, online search engines, and cloud computing services (as digital service providers).

As required by the NIS Regulations, the government has established a NIS national strategy, which has been embedded within the 2022 National Cyber Strategy, and which strongly influences the Regulations' policy implementation.

Authorities involved in implementation

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. The Department has a responsibility to ensure that the NIS Regulations are underpinned by a wider strategic direction, to conduct post-implementation reviews of the NIS regulations and to put forward improvements (either legislative or non-legislative) for the regulations.

Competent authorities are responsible for the implementation of the regulations in their sector, by assuring themselves that the regulated bodies have appropriate and proportionate measures in place, developing guidance, providing support, and responding to incident reports. In addition, competent authorities are responsible for designating any organisations that do not already qualify as NIS regulated organisations. Competent authorities are designated in the NIS Regulations under Schedule 1 and their duties and responsibilities are clearly set out in regulation 3.

The competent authorities' implementation and enforcement of the NIS Regulations, is further supported by the UK's national technical authority, the National Cyber Security Centre (NCSC).

Under the Regulations, the NCSC plays two different roles. Firstly, they are the UK's Single Point of Contact (SPOC) for incident reporting. This means that they act as the contact point for engagement with the EU member states on NIS, where appropriate. Secondly, NCSC acts as the Cyber Security Incident Response Team (CSIRT). Once an operator has alerted their competent authority of an incident they believe to be reportable under NIS, the operator may also contact NCSC. NCSC in their role as CSIRT will provide advice and support as appropriate. In addition to these two duties set out in the legislation, the NCSC supports the wider development of cyber security policy in their role as the technical authority on cyber security. The NCSC also acts as a source of technical cyber security expertise for operators and competent authorities.

Identifying organisations in scope

The NIS Regulations cover the energy, transport, health, drinking water supply and distribution, and digital infrastructure sectors. These are further broken down into subsectors, details of which can be found in Schedule 1 of the NIS Regulations. Schedule 2 sets out the further sector-specific designation thresholds that operators of essential services must meet in order to qualify as a NIS organisation.

Regulation 12(1) provides the definition of what is to be considered a digital service provider: organisations who provide online marketplaces, online search engines, and cloud computing services.

Operators of essential services are designated *de jure* at the moment when they fulfil the thresholds, and must register themselves with their competent authority. As mentioned above, competent authorities may also specifically designate organisations that are not captured by the thresholds, but that do provide an essential service within the scope of the Regulations as described in the legislation.[2] Digital service providers are also designated *de jure* and must register with their competent authority. The NIS Regulations do not apply to digital service providers that qualify as small or micro enterprises.

The 2018 Impact Assessment estimated that 611 organisations would be brought into scope of the Regulations: 432 operators of essential services and 179 relevant digital service providers.

Competent authority submissions to DCMS for the Review indicated that a total of 605 organisations had been designated: 436 operators of essential services and 169 relevant digital service providers. The number of organisations designated under the NIS Regulations was estimated using information provided by competent authorities on the number of organisations they regulate. Where a Competent Authority did not provide this information figures were taken from NCSC figures, which were previously provided by competent authorities (2020).

It is worth noting that recent assessments carried out by the Information Commissioner's Office estimate that there may be up to 1,200 digital service providers that qualify for designation under the regulations and that should be registered with the Information Commissioner.

Responsibilities of operators of essential services, relevant digital service providers, and Competent Authorities

Operators of essential services and relevant digital service providers are required by the NIS Regulations to take appropriate and proportionate measures to ensure the security of the network and information systems used to provide their essential services. Such measures may include, but are not limited to, implementing policies and procedures to tackle incident response, designating board-level responsibility for organisations, ensuring that organisations have a good understanding of their network and information system assets, and many others. These measures are established by the relevant competent authority, and the guidance issued by them sets out what is appropriate and proportionate in this context.

The NCSC has developed the Cyber Assessment Framework to assist competent authorities set target levels of cyber security in their sectors, and assess the levels of cyber security achieved by operators of essential services. The Cyber Assessment Framework is both sector-agnostic and outcome-based, and was designed to accommodate the use of a range of recognised cyber security standards. Most NIS competent authorities have chosen to use the Cyber Assessment Framework, which is now also being employed outside the NIS Regulations to improve the cyber security of a wide range of organisations that play a vital role in the day-to-day life of the UK.

Incidents

Operators of essential services and relevant digital service providers have a duty to notify their designated competent authority about any incident which has a significant impact on the continuity of the network and information systems used to provide their essential services, according to criteria set out in the Regulations and incident reporting thresholds. These are set by each competent authority in

[2] Regulation 8(3)

guidance.[3] Any incident that meets or exceeds these thresholds must be reported to the relevant competent authority no later than 72 hours after the incident was identified.

Enforcement measures

Competent authorities may take action against operators of essential services and relevant digital service providers. Enforcement measures include information notices (require an organisation to provide the competent authority with relevant information), inspections, enforcement notices (specifying steps that must be taken to rectify alleged failures), and penalties.

Penalties are meant to be used as a last resort, in the face of significant breaches of duty or persistent refusals to comply with interventions from the competent authority. Competent authorities must serve a notice of intention to impose a penalty before issuing the final penalty, and the relevant organisation will have an opportunity to provide representations and discuss the intention of the regulator before a final penalty decision is served. There are three levels of fine bandings that can be applied. Contraventions which were not material may go up to £1 million. Material contraventions may go up to £8.5 million. And finally up to £17 million for the most severe material contraventions which the enforcement authority determines have or could have created a significant risk or impact to the regulated body's service provision.

Regulated bodies have the right to appeal to the First-tier Tribunal against designation, revocation, enforcement or penalty notice decisions made by the competent authority.[4]

Amendments to the NIS Regulations since the last PIR

Based on the recommendations of the last PIR, in 2020 the government put forward legislative amendments to the NIS Regulations, to implement the review's recommendations. A public Call for Views on the proposed changes was published in September 2020, with the Government's Response published in November 2020 and the changes implemented by secondary legislation via Statutory Instrument SI 2020/1245, which came into force on 31st December 2020. A Supply Chain Call for Views and its government response were published in May 2021 and November 2021 respectively.

This statutory instrument made changes in the following areas, linked to the recommendations of the last Post-Implementation Review:

The introduction of an independent appeals mechanism

The last Review identified the need to improve the appeal mechanism. Previously, competent authorities were responsible for appointing an independent reviewer at the request of an operator of essential services or relevant digital service provider to review its designation decisions or penalty notices. Following the Review's recommendation, the government introduced a statutory appeals process, with appeals heard by the General Regulatory Chamber of the First-tier Tribunal, adding significantly more consistency across all sectors, relying on established judicial processes and which is expected to lead to much lower costs for operators and competent authorities.

Changes to regulatory enforcement powers

[3] This includes RDSPs, since the coming into force of SI 2021/1461.
[4] Regulation 19A.

The enforcement regime was broadly identified as needing refinement, with a particular focus on enforcement and information notices, clarifications in respect to civil liabilities, and a broader need to make the legislation clearer. The following amendments were introduced:

- **A more effective enforcement regime**: Information notices were amended to allow their use in identifying whether cyber incidents affected the security of networks and information systems, in addition to their previous use. Powers of inspection were also broadened to allow for a wider variety of actions, including testing, and safeguards were implemented to ensure appropriate and proportionate use. Alternatives to penalties were also introduced, in the form of civil proceedings, allowing regulators a more varied toolset to drive behaviours, and important changes to the use of enforcement notices were included to provide better safeguards for operators.

- **Revised penalty notice bands and process**: Changes were made so that competent authorities can better tailor penalties to their specific sector and to the seriousness of the breach. Issuing penalties now gives regulatory authorities more freedom to levy financial penalties as deterrents, as authorities no longer have to be bound to first issuing an enforcement notice. To ensure that their use is proportionate, safeguards were also included in the form of a more comprehensive two-step process for levying penalties, allowing for more engagement with operators and providing further opportunities to make representations or take steps to rectify their breach of duty.

- **Better information-sharing provisions**: The amendments further allowed competent authorities to share information, where necessary and proportionate, with each other and with law enforcement authorities for regulatory and national security purposes, and for the purpose of criminal proceedings and investigations.

Making sure the right organisations are in scope

The 2020 Review found that designation thresholds for certain sectors needed to be changed to make sure that the right organisations were in the scope of NIS. Consequently, amendments were made to Schedule 2 thresholds in the energy, the digital infrastructure, and the Scottish health sector thresholds.

Supply chain security

The 2020 Post-Implementation Review stated that ‘effective supply chain risk management is essential to having appropriate and proportionate measures in place to protect network and information systems’ and that this risk has been flagged by both regulators and regulated entities alike. Since then, the government has continued work on developing options to better tackle the security risks arising from supply chains, keeping in mind that any measure must be targeted and proportionate so as to not create undue burdens, limit innovation, or create challenges for organisations in scope.

DCMS issued a Call for Views in 2021[5], which sought the public’s thoughts on how to improve cyber security in supply chains more broadly and in managed service providers more specifically. Following this, DCMS has been developing legislative solutions to reduce supply chain risk and is currently consulting on measures which propose to identify certain third party providers critical to NIS operators, as well as bringing a specific type of third party provider through which many major supply chain attacks had been conducted: Managed Service Providers.

Incident reporting thresholds

[5] Call for views on supply chain security, 17 May 2021
https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security

The last Review found that thresholds for relevant digital service providers and operators of essential services needed to be amended. Relevant digital service providers' incident thresholds were previously set to an EU-market level (i.e. number of users impacted were based on the total of the EU's population). Since the publication of the Review's findings, the Government chose to bring thresholds to a more UK-appropriate level through secondary legislation (SI 2021/1461). Some Competent Authorities began work to review the incident thresholds they had set in guidance. DCMS also undertook policy work to investigate whether the definition of incident in the Regulations should be reviewed. This policy work is further explored in the "Areas of improvement" section of this Review.

Review period

Following the findings of the last Post Implementation Review, the legal requirements for its review timings were changed. After 2022, Post-Implementation Reviews will take place no later than every 5 years, instead of every 2 years.

EU Exit

A further SI (2021/1461) was put forward in 2021 in order to resolve certain EU-Exit deficiencies in Commission Implementing Regulation 2018/151, which governs additional rules to be taken into account in relation to the network and information systems security provisions and incident reporting thresholds for digital service providers. This statutory instrument did not make any policy changes; rather, it provided much needed amendments to the incident reporting thresholds for digital service providers in scope of the NIS Regulations, by removing defective EU reporting requirements and requiring relevant digital service to have regard to relevant statutory guidance issued by the Information Commissioner.

National Cyber Strategy

In December 2021 the government published the National Cyber Strategy. This strategy consists of five pillars. The Network and Information Systems Regulations contribute primarily to the 2nd pillar of the strategy, the resilience pillar. The resilience pillar of the strategy has three objectives:

1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience.
2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens.
3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.

The new strategy was published after the last Post-Implementation Review, but shows that the government still sees cyber resilience as a priority for the UK. These Regulations are working to address all 3 of these objectives and contribute towards the national objectives. They do this by ensuring critical organisations have good cyber hygiene and reduce their exposure to cyber risk and therefore reduce the likelihood of essential services being compromised.

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 post-implementation review. Similarly to the 2020 Post-Implementation Review the 2020 Post-Implementation Review, a medium resource approach was identified as being proportionate to the scale of the policy and the likely information we would be able to understand given the 3 years the policy has been active. DCMS opted to conduct surveys to gather bespoke evidence to assess the outcomes, costs and benefits both over the last 2 years since the last post-implementation review and any that occurred since the inception of the policy.

The analysis had to cover both research questions set out by Regulation 25 and the post-implementation review guidance detailed above. This document will build on the 2020 Post-Implementation Review and fully assess the implementation of the regulations. The analysis for this post-implementation review was carried out by in-house analysts at DCMS. All organisations, both operators of essential services and relevant digital service providers, that are in scope of the NIS Regulations were invited to take part in the surveys that informed our evaluation. To ensure that this review was not overburdensome on these organisations, they were informed that the survey and questions were all optional.

As the regulations had only been in force for 3 years at the time of the surveys, the surveys focussed on the experiences of organisations and how they have implemented the regulations. The views of the competent authorities were also collected to assess how the regulators have been implementing the regulations. The aim of the regulations is to reduce the cyber risk that critical firms pose to the UK economy. The review therefore focused on the cyber security improvements that firms have implemented because of the regulations.

The views of the NCSC were collected in order to assess if they believe the cyber risks posed to the economy from these firms have reduced. It is not possible to quantify a reduction in incidents as a counterfactual is impossible to prove, and also a reduction in incidents may be flawed. A reduction in incidents may mean that just less incidents are being detected. There was also no baselining of incidents before the regulations came into place, as there was no ability to enforce firms to report incidents to a central body that would be brought under the NIS Regulations.

To assess whether there has been an improvement in the outcomes due to the regulations, we will compare the results of these surveys to the previous post-implementation review to see if there has been any change.

In the last post-implementation review, DCMS committed to running a more qualitative stage of research. To ensure that our research was not overburdensome on the firms especially during the Covid-19 pandemic and given the short period since the last Review, DCMS opted to add more qualitative questions into the survey to reduce the amount of burden from different research projects. This approach allowed us to directly ask firms about the quantitative results they provided us with allowing for more detailed analysis and therefore more informed policy making.

4) Evidence collection and methodology

DCMS conducted primary research with 4 key groups of stakeholders: operators of essential services; relevant digital service providers; the competent authorities; and NCSC. Each survey was different and asked questions that were relevant to each stakeholder. As the secure-online surveys worked well for the 2020 post-implementation review, DCMS decided that it would be the most appropriate tool to conduct the primary research.

DCMS scoped out the surveys with other government departments, competent authorities and NCSC. These stakeholders shared their thoughts to improve the data collected as part of this review. The reason operators of essential services and relevant digital service providers had separate surveys was to ensure we only asked questions that relate to the policy areas that were outlined in the original Impact Assessment.

Just as in the last Post-Implementation Review, a combination of quantitative and qualitative questions were included. As previously mentioned, it was identified in the last review that there was a benefit to carrying out more qualitative research. DCMS has achieved this by adding more qualitative questions included in this review, as opposed to running a standalone project. This was judged as being the less burdensome approach to completing the proposed research in the last Post-Implementation Review. Annexes A and B show the surveys that were sent to operators of essential services and relevant digital service providers, respectively. Additional questions were included in the surveys to capture the impact of the regulations on innovation, as DCMS is a trial department on including the impacts of regulations on innovation in impact assessments.

The surveys were distributed to the competent authorities who then shared them with the operator of essential services or relevant digital service providers that belong to their sector. All operators of essential services and relevant digital service providers had the opportunity to respond to the survey. Participation in the survey was voluntary and operators of essential services and relevant digital service providers were given six weeks to respond. The exception was the Department for Transport, due to a distribution list error the initial survey links were not distributed to the competent authority and the survey was opened at a later date with a shorter period of 10 days. The Department for Transport still received a response rate of 26% which was higher than the survey average. Contact information was provided in case they had any queries. After reviewing the data, the team noticed no differences in the quality of responses between those of the Department for Transport and other sectors. Their responses did not alter any trends or policy recommendations, and their respondents tended to agree with other operators of essential services. The differences that are observed between the answers, for example on cyber security spending, often differ between sectors and are not as a result of a shortened response period. Reminders were sent out via competent authorities during the six weeks in which the survey was live to encourage participation. Only the team directly working on the Post-Implementation Review could see the individual responses to the survey that were submitted.

The responses to surveys were lower than those that we received in the last Post-Implementation Review, this could be due to firms being busy due to the COVID-19 pandemic or less interest in completing the surveys as this is the second of such reviews. As the last Post-Implementation Review fell within a pre-election period DCMS could not send reminder emails to organisations to encourage them to complete the survey. During this Post-Implementation Review, DCMS sent reminder emails whilst the surveys were open to try and encourage participation, this did not improve the response rate from the last Review. To improve participation for the next Post-Implementation Review, DCMS recommends working more closely with individual competent authorities to target sectors or regions that have a lower response rate. The surveys captured the views of 68 operators of essential services, down from 117 in the last review. The 68 respondents make up 16%[6] of the total population of operators of essential services covered by the NIS Regulations. The surveys also received 14 responses from digital service providers covered by the NIS Regulations, down from 21 in the last review, representing 8%[7] of the population of relevant digital service providers. Whilst DCMS cannot guarantee that this sample is representative, the survey was open to all organisations that are regulated by the NIS Regulations to complete, so DCMS believes it is a robust basis to evaluate the NIS Regulations. Due to the low number of relevant digital service provider responses and the number of “Don’t know” responses on some questions, DCMS has been unable to update some assumptions from the previous review. Where this is the case, it will be made clear to the reader where the assumption originates.

Responses cover both medium and large organisations, as no small organisations were identified as being regulated under the NIS Regulations by competent authorities in this review. Replies were received across the different sectors and regions to give a good sample spanning the NIS Regulations, however it should be noted that there were very few medium operators of essential services. Operators of essential services and relevant digital service providers have the regulations applied differently, so it is worth noting that when comparing the results and costs of the regulations.

Table 1: Number of responses by size of organisation

Size	Operators of essential services		Relevant digital service providers	
	Number of respondents	% of respondents	Number of respondents	% of respondents
Medium	3	4%	9	64%
Large	65	96%	5	36%
Total	68	100%	14	100%

Analysts in DCMS undertook quantitative and qualitative analysis on the survey questions. For the qualitative work, a coding framework was designed for each open ended question and separate key themes were identified for operators of essential services and relevant digital service providers depending on the questionnaire. Closed questions were analysed using descriptive statistics which enabled findings to be displayed simply whilst allowing for conclusions to be drawn. All the analysis completed was quality assured by other analysts to ensure that departmental policies were followed and that the results are accurate.

As part of the analysis, the analysts also compared the results to the previous Post-Implementation Review. The questionnaires were designed so that the results could be compared by ensuring consistency where the results in the last survey were meaningful. Where there is a change that DCMS feels is worth noting, this will be pointed out throughout the review.

The surveys with competent authorities and the National Cyber Security Centre received a good response rate with all surveyed organisations providing feedback. The responses that were received also formed part of the evidence that is reviewed in this document, as it is important to understand the perspective of the regulators and the experts. Competent authorities also have other channels to provide feedback on the NIS Regulations, as DCMS hosts monthly meetings where issues can be raised and

[6] Rounded to the nearest 1% and taken from a base of 436 operators of essential services that are regulated out of a total 605 organisations regulated under NIS.

[7] Rounded to the nearest 1% and taken from a base of 169 relevant digital service providers that are regulated out of a total 605 organisations regulated under NIS.

discussed. The findings of the review were discussed with both the regulators and the policy teams of other government departments. DCMS also undertook desk research to further the understanding of how the NIS Regulations interact with other regulations such as the General Data Protection Regulations (GDPR). This was to address the feedback received from the Regulatory Policy Committee (RPC) that the previous review had not assessed the impact of the combined cost of the regulations.

Monitoring and evaluation

Whilst DCMS has highlighted the problems with baselining the number of incidents to prove a benefit of fewer incidents as a result of the Regulations, it wants to improve the ability to evaluate in the next Post-Implementation Review. DCMS will aim to collect annual data from the competent authorities on data that will help to assess the Regulations and also the National Cyber Security Strategy. This data could include:

- The number of incidents per year.
- The number of independent audits of the Cyber Assessment Framework.
- The number of improvement plans as a result of the Cyber Assessment Framework.
- The number of information notices issued by the competent authorities.
- The number and nature of enforcement notices issued by competent authorities.
- The number of organisations regulated by sector and also the number of SMEs regulated by sector.

Work will be carried out to make sure that the competent authorities collect the data required and that they can utilise it for their own monitoring purposes. DCMS does not want to increase the regulatory burden of the NIS Regulations, so organisations regulated by the NIS Regulations will not be contacted on an annual basis. DCMS will work to estimate the potential economic cost of a cyber incident in the NIS sectors to better demonstrate the benefits of avoiding such incidents. If the data above is collected, analysts may be able to utilise methods such as Bayesian Networks[8] to assess what the security changes as a result of the Regulations have done to the risk profile of these organisations. DCMS will work with NCSC, as they are the technical authority, to try and understand the trends in attacks by sector, to fully highlight where the Regulations may be helping and where they could be more helpful.

Whilst this will not fully overcome the issue of not having a baseline to assess the number of incidents. It should allow us to estimate the risk reduction from the improvements that the Regulations have generated on cyber security.

[8] Bayesian networks are just one example of the methodologies that might be appropriate for this problem. Bayesian Networks would allow DCMS analysts to quantify the risk posed by cyber as can be seen in this paper by Hossain et al on Modelling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem.

5) Are the Regulations working?

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

The policy objectives set out in the 2018 Impact Assessment of the NIS Regulations are "to prevent (where possible) and improve the levels of protection against network and information systems incidents"[9], as well as to "ensure that there is a culture of security across sectors which are vital for our economy and society".[10] Overall, although there is evidence indicating that the overarching policy objectives have largely been met, there nonetheless remain a number of opportunities to improve the NIS Regulations' implementation.

With regards to assessing the effectiveness of the NIS Regulations in preventing NIS incidents, as it is not possible to estimate a counterfactual number of NIS incidents that would occur had the Regulations not been in place, it is not possible to assess whether the NIS Regulations have reduced the number of NIS incidents. Overall, in 2019 a total number of thirteen NIS incidents were recorded. This number decreased to twelve incidents in 2020, indicating a slight decrease in the number of incidents recorded, however these may not be cyber-related. There have been issues and concerns surrounding what classifies as a NIS incident, as the current definition of a NIS incident only captures a small percentage of all incidents that threaten essential services.

This suggests that the current NIS Regulations reporting requirements do not capture all important incidents.An issue which is evidenced by the stark contrast between the average number of incidents informally reported to the NCSC by organisations in NIS essential service sectors, versus the very low number reported officially by NIS firms to their responsible competent authorities, and the number of incidents reported in the press. Some estimates suggest that the number of incidents impacting these sectors could be significantly larger. The main concern with regards to this is whether despite not currently meeting the threshold for reporting a NIS incident set out in the Regulations and guidance, these incidents have the potential to disrupt essential services in the long run (e.g. ransomware attacks). If they were reportable, regulators could seek regulatory intervention and by suggesting improvement plans or intelligence sharing, improve the levels of protection of that essential service against future incidents, thus meeting the NIS Regulations' objectives. Suggestions on how to capture important incidents are outlined in section 10 of this document.

Although it is difficult to assess whether the Regulations have reduced incidents given the issues surrounding incident reporting under NIS, the findings of the Post Implementation Review do suggest that NIS has improved levels of protection by accelerating the development of a security culture across essential service sectors. How this culture of security has manifested itself is detailed in the outcomes section below.

Regulatory outcomes

The main projected benefits to the UK economy outlined in the 2018 Impact Assessment include the improved protection of the network and information systems that underpin the UK's essential services; and reducing the likelihood and impact of security incidents affecting those networks and information systems and the corresponding impact on economic prosperity. It is also pointed out that businesses also may benefit from reducing the impact of breaches or attacks that are below the NIS Directive thresholds, as the improvements in cyber security and handling of incidents will not just apply to NIS

[9] DCMS, NIS Regulations: Impact Assessment (2018), p.1
[10] Ibid, p.6

incidents. Moreover, international cooperation and information sharing is also expected to improve advice and incident response for firms.[11]

NIS has accelerated the improvement of essential services' protection of their network and information systems. The surveys conducted as part of this review showed that 28% of operators of essential services reported having introduced new policies and processes since the inception of the Regulations, while 51% have updated or strengthened existing policies and processes, and 7% intend to update or strengthen these processes as a consequence of the NIS Regulations.[12] This highlights a direct correlation between regulated bodies' improved cyber security behaviours and the NIS Regulations. Moreover, the proportion of organisations that reported having introduced or updated policies and processes is significantly higher relative to the findings of the 2021 Cyber Breaches Survey, which found that only 33% of businesses had a formal policy or policies covering cyber security risks.[13]

In addition, 71% of operators of essential services respondents reported an increase in board support for cyber security.[14] This was corroborated by the competent authorities' responses, who reported greater buy-in and understanding of cyber security from their regulated bodies at board level since the implementation of the NIS Regulations.

62% of operators of essential services also reported having updated general incident management processes, and 49% reported having improved their understanding of their organisations' aggregate risks.[15] The incident response plans that NIS organisations have in place, as well as the improved speed at which organisations mitigate vulnerabilities when alerted by regulators, will improve resilience to incidents, and could potentially stop non-NIS incidents turning into NIS incidents. Additional NIS protection outcomes reported by operators of essential services included improving the way that they assess their supply chain.

With regards to unexpected benefits of the NIS Regulations for relevant digital service providers, the respondents to the post-implementation review survey also indicated that they have improved their understanding of their organisations' aggregate risks (31%), increased board support for cyber security (31%), and updating general incident management processes (23%) as a result of implementing the NIS Regulations. 46% of respondents reported that they have not experienced any unintended benefits as a result of the Regulations. [16]

Overall, these findings confirm that both operators of essential services and relevant digital service providers are improving their security culture in response to duties imposed on them by the NIS Regulations, in the context of an increasing focus on cyber resilience across the economy. This is further supported by the competent authorities' responses to the Post-Implementation Review, as it was noted by regulators that despite the financial difficulties in the context of COVID-19 pandemic, there had been an increase in spending among organisations in the form of hiring additional staff and increasing projects related to cyber security. Reports from competent authorities have also indicated that firms are updating their legacy systems, which are likely to provide better mitigations and risk management against threats, raising the level of resilience of the essential services.

Competent authorities also noted fundamental improvements to risk and incident management processes as one of the key improvements in their sectors. This is in stark contrast to the 2021 Cyber Breaches Survey, which provides evidence of information risk management regimes being the area in

[11] Ibid, p.3
[12] Base: 68 OESs.
[13] DCMS, Cyber Security Breaches Survey (2021), p. 33
[14] Base: 68 OESs.
[15] Base: 68 OESs.
[16] Base: 13 RDSPs.

which the least amount of companies had undertaken any action (30% of organisations, a decrease from the previous 39% captured in the 2017 Cyber Breaches Survey). This provides an indication that the NIS Regulations have provided an incentive for companies under its scope to focus on specific improvements such as these, in contrast to unregulated companies in the wider economy. This data indicates that the NIS Regulations have had a positive and beneficial impact on those organisations in scope, raising their levels of resilience compared to those organisations that are covered by the regulations.

As mentioned above, there are indications that the current definition of a reportable NIS incident may mean that regulated organisations are not reporting important incidents . We therefore lack robust data to assess the number of cyber incidents on firms that provide essential services. However, we have data that confirms that there has been a marginal reduction in NIS reported incidents: from 13 in 2019, to 12 in 2020, however these aren't necessarily cyber incidents.

Due to a lack of primary and secondary data collection on the cost of a NIS incident to organisations, this review is not able to assess the economic impact of a possible incident reduction as a result of the Regulations.

Similarly, we do not have data on whether businesses have benefitted from reduced breaches/attacks below thresholds, however it can be inferred from the numbers supplied to us by NCSC on informally reported incidents, which show a decrease in overall incidents between 2019 and 2020 in sectors classed as essential by NIS.[17]

Finally, with regards to international cooperation and information sharing leading to improved advice and incident response for organisations, this review notes that notwithstanding the UK's departure from the European Union on 31 January 2020, Part 4 of the Trade and Cooperation Agreement (TCA) contains provisions that would allow the UK to cooperate with the EU on cyber security. This includes taking part in some of the activities of NIS related action groups: the EU NIS Cooperation Group, the EU Agency for Cybersecurity (ENISA), as well as cooperation with the EU's Computer Emergency Response Team Network (CERT-EU).[18]

Security practices prior to the NIS Regulations

Data from both Post-Implementation Reviews suggests over the past 4 years that the NIS Regulations are acting as an accelerator for improvements across sectors that fall under the NIS Regulations. Competent authorities, when queried, in the context of both the 2022 and 2020 Post-Implementation Reviews, reported that in their view without the regulations, improvements in security would continue, albeit at a much slower pace.

DCMS intended to collect baselining data again from the organisations that are regulated by NIS. This was due to two main reasons: firstly, organisations may have been designated under the regulations since the last review and; secondly, to ensure that any difference in conclusion of this Post-Implementation Review was not down to a difference in sample. Similarly to the last review, the vast majority of operators of essential services and relevant digital service providers (85% and 93%), indicated having made improvements to the security of their network and information systems prior to the introduction of the Regulations.[19] Moreover, 88% of operators of essential services and 100% of relevant

[17] This data cannot be disclosed due to its sensitive nature.
[18] The UK-EU Trade and Cooperation Agreement: Summary and Implementation (2020), p. 29.
[19] Base: 68 OESs and 13 RDSPs.

digital service providers had governance policies and/or processes to manage security risks to the network and information systems prior to the NIS Regulations.[20]

As identified in both the 2018 NIS Regulations Impact Assessment and the 2020 review of the NIS Regulations, the firms covered by the NIS Regulations will be subject to other regulations and requirements. The sample collected from this review found that other regulations or standards mentioned as drivers for improvements in cyber security included: UK General Data Protection Regulations (GDPR) (86% of relevant digital service providers and 78% of operators of essential services)[21]; ISO27001 (28% of operators of essential services); Cyber Essentials and Cyber Essentials Plus (11% of operators of essential services); as well as other industry standards (33% of operators of essential services).[22]

As shown in Figure 1, further non-regulatory drivers of change prior to the NIS Regulations included maintaining business continuity (93% relevant digital service providers, 94% operators of essential services), protecting critical systems (86% relevant digital service providers, 94% operators of essential services), avoiding financial loss (71% relevant digital service providers, 82% operators of essential services), and avoiding reputational damage (86% relevant digital service providers, 82% operators of essential services).[23]

Figure 1: Reasons for implementing changes to the security of network and information systems prior to the NIS Regulations

[20] Base: 68 OESs and 13 RDSPs.

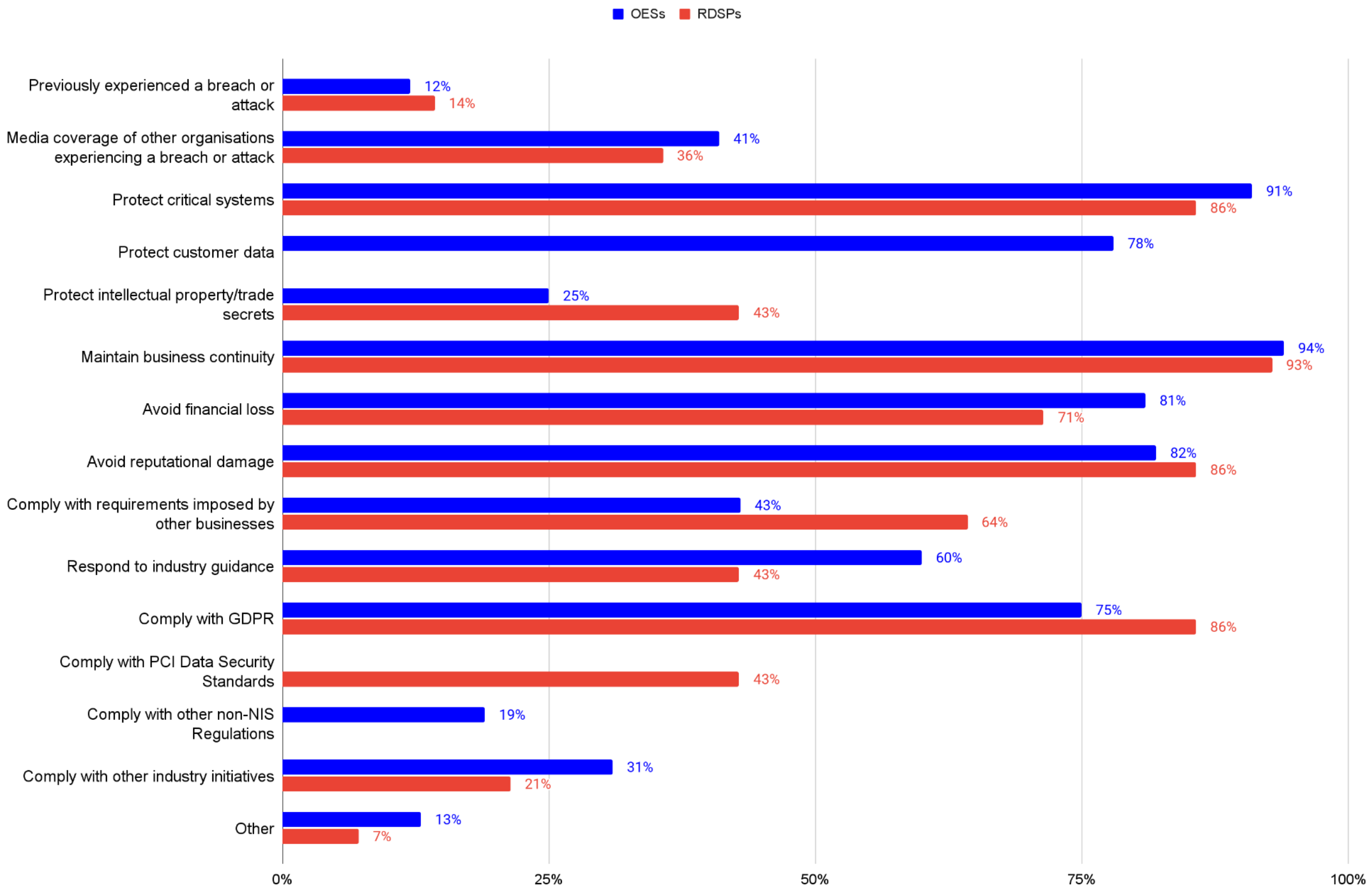
[21] Base: 68 OESs and 13 RDSPs.

[22] Base: 18 OESs.

[23] Base: 18 OESs.

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 service(s) in the past?

Base: 68 OESs and 13 RDSPs



Just as in the last review, firms were already taking action to make improvements before the NIS Regulations came into force. Evidence from the competent authorities also notes that the NIS Regulations are likely to have improved the speed at which improvements were made to firms' cyber security rather than generate new improvements. As the rationale for intervention in the original impact assessment made clear, the UK economy has a dependency on the firms that have been designated under the NIS Regulations and therefore there is an urgency for these firms to make changes. The threat that firms face in the cyber landscape is ever present, and making improvements at a slower pace than necessary is simply not an option for the UK economy and endangers the future security and prosperity of the country.

Key outcomes

Operators of essential services

Both operators of essential services and competent authorities reported that they have seen an increase in resources dedicated to cyber security improvements. While competent authorities indicated that there have been improvements in cyber security in their sector since the introduction of the Regulations, most believe that the NIS Regulations acted as an accelerator for already-planned cyber security improvements. This is essential for good cyber security to reduce the vulnerabilities that exist in systems and therefore reduce the possibilities of attack.

Operators of essential services reported an increase in prioritisation of cyber security at a senior level, reported by 69% of operators of essential services.[24] Moreover, 62% of the organisations who reported an increase in prioritisation also reported having updated/strengthened existing policies/processes as a result of the NIS Regulations. Overall, organisations also reported that they are investing more resources on an ongoing basis into their cyber security throughout the three categories of: physical security (83%); external costs (71%); and internal staff costs (75%).[25] This demonstrates the increase in priority of cyber security.

The majority of operators of essential services reported that they have introduced new policies or processes to manage security risk, with 79% reporting having done so due to the NIS Regulations.[26] Of the organisations that have not improved or introduced processes or policies, all of them stated that they either have plans to introduce new policies or their policies already met the required standards.

Whilst 88% of operators of essential services reported having processes for an incident response prior to the NIS Regulations, 12% had no such procedures.[27] Of the 12%, one third have introduced new procedures/processes and the remaining two thirds are intending to introduce new procedures or strengthen existing ones. This will help to maintain the provision of their essential services. Whilst the NIS Regulations have been in place for 3 years, some organisations may have only been designated for a shorter period, meaning they are at the early stages of implementing the requirements of the NIS Regulations.

Operators of essential services indicated that since the implementation of the Regulations their organisations are more likely to voluntarily report an incident that is under the threshold to their competent authority and to the National Cyber Security Centre in 45% and 42% of the cases, respectively. Next to this, organisations also indicated no change in attitude towards their competent authority and towards the National Cyber Security Centre in 45% and 54% of the cases, respectively.[28] This indicates an improvement in attitudes towards voluntary reporting which can lead to greater oversight of cyber threats to the UK economy.

There appear to be some challenges to organisations' ability to implement the NIS Regulations, with 56% of operators of essential services indicating facing challenges implementing the Regulations.[29] Moreover, there is some concern about the ability of organisations to maintain their compliance with the regulations, with 42% of operators of essential services indicating that they do not have the skills and capacity to deliver their obligations under the NIS Regulations.[30] There is an indication of a link between facing challenges to implement the NIS Regulations among operator of essential services and having the necessary in-house skills and capacity, as 42% of the operator of essential services who felt that they faced challenges to their ability to implement the NIS regulations also reported that they didn't feel they had the in-house skills and capacity to deliver their obligations under NIS.[31] This position matches the wider cyber skills issue in the UK economy where DCMS research highlights a national cyber skills shortage.[32] Nonetheless, 66% of operator of essential services also reported that they have retrained,

[24] Base: 68 OESs.
[25] Base: 68 OESs.
[26] Base: 68 OESs
[27] Base: 68 OESs.
[28] Base: 68 OESs.
[29] Base: 68 OESs.
[30] Base: 62 OESs.
[31] Base: 62 OESs.
[32] Ipsos Mori, Cyber security skills in the UK Labour Market (2021)

up-skilled or hired new staff to manage security risks to their organisation's network and information systems as a result of the NIS regulations, which can assist organisations in mitigating some of the challenges faced by the lack of in-house skills.[33]

There also appear to be challenges with regard to organisations' supplier risk management as 66% of operators of essential services indicated facing barriers that prevent them from conducting appropriate and proportionate risk management of their suppliers and their wider supply chain.[34] This issue appears to be more significant with regards to organisations' wider supply chains, as only 9% of operators of essential services indicated having the resources to manage the risk from both their direct suppliers and their wider supply chain while 51% indicated having the resources to manage the cyber security risk from their direct suppliers but not their wider supply chain.[35] Moreover, 24% of operators of essential services reported not having the resources (19%) or being unsure on how to manage the risk from both direct suppliers and their wider supply chain (9%). Some of the barriers to supply chain risk management indicated by operator of essential services included: lack of cooperation with suppliers (44%); lack of staff resources (12%); perceiving the supply chain as too large or complicated to understand the underlying risks (14%); unspecified resource constraints (19%); lack of skills (7%); issues relating to contracts (5%); and legacy systems (2%).[36] These issues are in line with those highlighted in DCMS's Call for Views on Supply Chain Cyber Security, which sought insights from industry to inform the government's understanding of supply chain cyber security.[37]

Digital Service Providers

Relevant digital service providers did not see as much senior prioritisation as a result of the regulations as the operator of essential services, with only 23% of organisations in the survey reporting this.[38] This is a similar proportion to the last review in which 29% of digital service providers reported this benefit.[39] 80% of organisations that reported not seeing a change in prioritisation stated that cyber security was already a priority for other reasons.[40] In line with this, 36% of relevant digital service providers said that they had updated/strengthened existing policies/processes as a result of the NIS Regulations, 7% said that they intended to do so, 43% reported making no changes as a result of already meeting the required standards, and only 7% reported having introduced new policies/processes.[41] Digital service providers having a lower outcomes than the operators of essential services could be due to different reasons, but the two most likely reasons could be due to: 1) a higher starting point prior to the Regulations being brought in with regards to cyber security; 2) it could be due to the difference in the way the Regulations are applied to operators of essential services and digital service providers, as mentioned previously in this document.

100% of the survey respondents stated that they already had incident response policies in place prior to the NIS Regulations for recovery from a security incident relating to the network and information systems

[33] Base: 68 OESs.
[34] Base: 67 OESs.
[35] Base: 68 OESs.
[36] Base: 43 OESs.
[37] While the scope of the Call for Views is limited to digital supply chains, in the survey respondents were asked to reflect on their overall supply chain risk management capabilities, which may include physical security of non-digital assets.
[38] Base: 13 RDSPs.
[39] Base: 17 RDSPs.
[40] Base: 12 RDSPs.
[41] Base: 13 RDSPs.

used for the provision of their services.[42] However, 46% have strengthened existing processes/procedures since the NIS Regulations, meaning that an incident is likely to have a reduced impact on the organisation and therefore economy. While all of the respondents who indicated having strengthened existing processes/procedures reported these processes reported being influenced or affected by the UK General Data Protection Regulation and Data Protection Act 2018, the majority of organisations indicated having taken actions in several areas with regards to incident response as a result of the NIS Regulations. 46% of the respondents indicated undertaking up-to-date incident response plans, 38% indicated taking action in the form of risk assessment plans, and in 31% of the cases no action was taken.[43]

The majority of relevant digital service providers (62%) indicated not facing any barriers that prevent their organisation from conducting effective risk management of their suppliers, including their wider supply chain.[44] Next to this, all relevant digital service providers who responded to the survey reported having the resources to manage cyber security risks of their network and information systems arising from their direct suppliers.[45] Moreover, in 54% of the cases respondents also indicated having the resources to manage the risk from their wider supply chain. Of the 46% who stated they didn't feel able to manage the risk of their wider supply chain, 60% reported that it was a lack of will amongst suppliers, 40% reported a lack of finances or funding, and a further 40% reported a lack of staff resource.

Overall, while it appears that some organisations were already taking action to improve cybersecurity, there is an indication of a positive effect of the Regulations on governance policies and/or processes to manage security risk, which will help to reduce the risk posed to the economy by these organisations. Moreover, relevant digital service providers also indicated having invested, or planning to invest, in internal staff (54%), physical security of IT (46%), and external costs (31%) related to the security of their network and information systems for providing their services.[46] These investments will therefore lead to further improving organisations' cybersecurity. As with operators of essential services, these issues are also in line with those highlighted in DCMS's Call for Views on Supply Chain Cyber Security.[47]

Among relevant digital service providers, the large majority of respondents indicated that their attitudes have not changed towards voluntarily reporting of an incident that is under the reporting threshold both to their competent authority and to the NCSC (77% and 69% of the cases, respectively). The proportion of relevant digital service providers who reported being more likely to report this type of incident towards their competent authority and to the NCSC was 8% and 15%, respectively.[48]

A policy measure in the recent proposals on cyber measures, published by DCMS, looks to bring the regime of some digital service providers in-line with the regime for operators of essential services. This will mean that if the outcomes being lower for digital service providers is due to the difference in regulatory regime, the outcomes for digital service providers will improve, if the measure is taken forward.

Supporting organisations to implement the Regulations

[42] Base: 13 RDSPs.
[43] Base: 13 RDSPs
[44] Base: 13 RDSPs
[45] Base: 13 RDSPs.
[46] Base: 13 RDSPs.
[47] While the scope of the Call for Views is limited to digital supply chains, in the survey respondents were asked to reflect on their overall supply chain risk management capabilities, which may include physical security of non-digital assets.
[48] Base: 13 RDSPs.

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 Cyber Assessment Framework (CAF). Overall, 84% of operators of essential services reported using the CAF, an increase from the 71% of respondents who reported using this tool in the 2020 NIS Post-Implementation Review.[49] The majority of respondents indicated finding this moderately useful (48%), very useful (39%), or extremely useful (7%) for managing risk to the security of your organisation's Network and Information Systems.[50]

When asked how the CAF could be improved, 23% of operator of essential services said that it should be less specific and more nuanced or holistic, 15% said it should align with other frameworks[51], 8% mentioned that it should be clearer/improve the benchmarking so progress can be tracked and 13% also asked for clearer wording. Other respondents mentioned it being more sector specific and making the requirements more specific.[52]

The review also looked at the extent to which applying the NCSC CAF principles and guidance had a positive impact on several areas relating to the provision of essential services in organisations. This is summarised in Figure 2 below. The majority of organisations reported somewhat positive or extremely positive impacts across all areas, which provides an indication of improvements in different areas relating to cybersecurity as a result of applying the CAF principles and guidance.

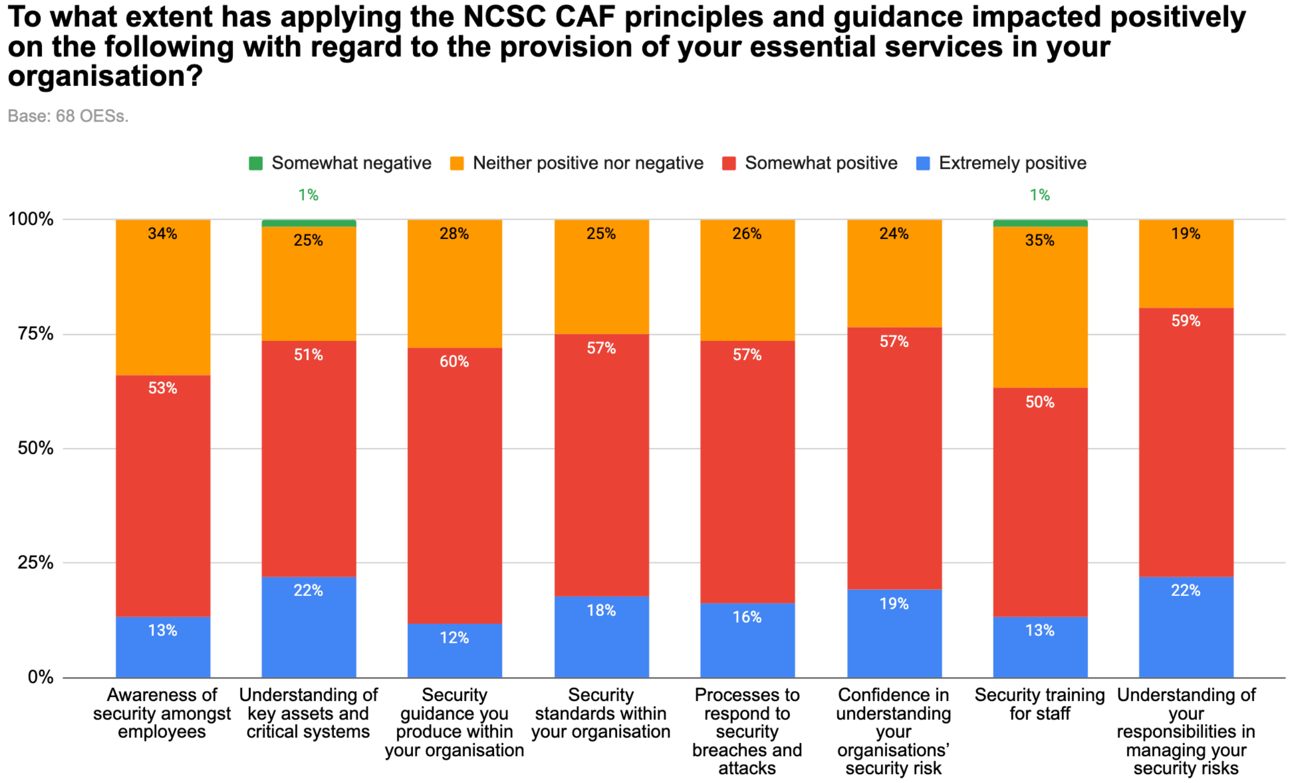
[49] Base: 68 OESs.

[50] Base: 56 OESs.

[51] Half of the respondents who felt the CAF could be improved by aligning with other frameworks linked this to an alignment to the ISO27001 standard.

[52] Base: 39 OESs.

Figure 2: Impact of applying the NCSC CAF principles and guidance



Furthermore, guidance and support from competent authorities on implementing and complying with the Regulations may have helped organisations in improving the security of their network and information systems. Among the respondents, most organisations reported knowing where to find guidance on NIS implementation and compliance (97% of operators of essential services and 100% of relevant digital service providers).[53] This represents a slight increase compared to the 2020 NIS Post-Implementation Review, in which 96% of operators of essential services and 94% of relevant digital service providers knew where to find the guidance.[54] Moreover, similar to the 2020 NIS Post-Implementation Review, 93% of relevant digital service providers and 95% of operators of essential services found the guidance easy to access.[55]

In implementing the NIS Regulations effectively, the majority of organisations also reported having received adequate guidance and support from their competent authority (93% of relevant digital service providers and 68% of operators of essential services).[56] Both groups have seen improvements on the support they have received from their competent authorities compared to the last post-implementation review, where 60% of operators of essential services and 71% of relevant digital service providers reported they had adequate support and guidance from their competent authorities.

Within operator of essential services, respondents pointed to the usefulness of additional support in the form of industry events (26%), information exchanges with other operator of essential services (35%), and the improvement of the educational materials available online (32%), in further assisting them with

[53] Base: 68 OESs and 14 RDSPs.
[54] Base: 113 OESs and 18 RDSPs.
[55] Base: 66 OESs and 14 RDSPs.
[56] Base: 14 RDSPs and 68 OESs.

the implementation of the NIS Regulations.[57] Relevant digital service providers, on the other hand, mostly pointed to the benefits of providing updates to businesses (37%) and providing more information on the ICO or NCSC website (33%).[58]

Enforcement

The Review also aimed to assess the role of the enforcement element of the Regulations in driving improvements amongst organisations. Overall, 100% of relevant digital service providers and 96% of operators of essential services that responded to the survey reported being aware that there is an enforcement regime associated with the NIS Regulations.[59]

Next to this, the majority of organisations indicated that the enforcement regime had not led them to implement any improvements to the resilience of their services (49% of operators of essential services and 69% of relevant digital service providers).[60] However, it is important to note that given that there have been very few enforcement activities taking place, at this stage it is not possible to robustly assess whether the regime can lead to improvements in organisations. The degree to which enforcement activities have taken place is further detailed in Section 8 of this Review. As such, it would be useful to assess the impact of this regime on improvements to organisations in future post-implementation reviews.

Despite not reporting the enforcement regime to be a key driver of improvements, the current enforcement regime was found to be proportionate to the risk of disruption to relevant services in the majority of organisations (72% of operators of essential services and 92% of relevant digital service providers).[61] Among the operator of essential services that disagreed that the enforcement regime was proportionate to this risk, 22% stated that they thought it was too high/severe, 6% felt that it was too low, 6% felt it damaged the relationship between competent authorities and operator of essential services, and 6% felt that it took too long before a penalty was handed down.[62] 44% gave other reasons including there is no clear link between the fine levied and the actions that operator of essential services took prior to the incident and the fact that fines result in double jeopardy as there is already a cost relating to a cyber breach. The only relevant digital service providers who indicated that the enforcement regime was not proportionate to the risk of disruption reported feeling that the Regulations were incorrectly applied to DSP organisations in general.

Summary: Outcomes observed to date

The evidence suggests that the regulations are working to improve the cyber resilience of both relevant digital service providers and operators of essential services. There has been an increase in the prioritisation of cyber security at senior level, as well as indications that the majority of operators have either introduced new policies or improved existing ones where such processes were already in place, improved their incident response management, and a wider awareness of guidance and available support from the competent authorities. Reports of more voluntary reporting is also a positive development, indicating a move towards a more mature cyber sector, willing to take steps and address the threats to essential services.

Some of the tools created for the Regulations, such as the NCSC's Cyber Assessment Framework, have ensured that improvements are made and that firms appear to be speeding up their cyber improvements.

[57] Base: 66 OESs.
[58] Base: 14 RDSPs.
[59] Base: 13 RDSPs and 68 OESs.
[60] Base: 65 OESs and 13 RDSPs.
[61] Base: 12 RDSPs and 65 OESs.
[62] Base: 18 OESs.

There is still more that can be done. There is a lot of uncertainty around the incident response, and which incidents need to be reported; reports received for this Post-Implementation Review, however, indicate that both operators of essential services and relevant digital service providers are aware of the guidance and have found it useful. This indicates that further attention must be given to incident reporting from a legislative perspective, which has been taken forward by DCMS' consultation on the measures to improve the UK's cyber resilience, where it considers amendments to the incident reporting framework.

Capacity constraints and lack of access to the appropriate skills within the sectors still remains an issue with operators of essential service and digital service providers.

In addition to this, one of the most prevalent challenges illustrated from the study is the ability of operators to secure their wider supply chains, with 9% of operators of essential services indicated having the right resources to do so; this comes in contrast with the 54% of digital service providers reporting being able to address this challenge. More could be done in this space, and DCMS has considered measures that would tackle this inability in the 19th January consultation.

Overall, the surveys provide a good basis to indicate that the regulations are having a positive impact and that they are effective in driving behaviour. However, the increased investment and lack of cyber incident reports are not necessarily indicative of the wider policy objective of providing better security for essential services and leading to increased cyber resilience, as it is impossible to say whether the regulations have reduced the amount of incidents that these services would have faced. Better key performance indicators need to be developed to assess this.

Sections 10 and 11 below will consider the response to these challenges, and the role that DCMS, and the wider competent authority community, could fulfil to address them.

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

Costs

The Impact Assessment (IA) identified the costs of implementing and running the Regulations as split between those falling on businesses and additional costs to government from enforcement activity:

- Costs incurred by businesses include (a) familiarisation costs, (b) additional security spending, (c) costs of incident reporting, (d) competent authority costs, including compliance costs, and (e) responding to enforcement activities.
- Costs to the government include (a) setting up a Computer Security Incident Response Team (CSIRT), Single Point of Contact (SPOC), 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 whether the costs estimated in the impact assessment were accurate. Table 2 presents the summary of total costs for the 10-year appraisal period.

Table 2: Summary of costs (2016 prices)

Type of cost/benefit

Type of cost/benefit	Estimates in IA	Estimate in 2022 PIR (average annual costs)	Drivers for change
Familiarisation costs **(Year one only)**	£406,018	£740,377	Increase in familiarisation costs of organisations due to an increase in wages of legal professionals and IT directors in 2018, as well as due to the inclusion of self-reported familiarisation costs by organisations. Often these costs were higher than those that DCMS had forecasted. This is because they often included technical teams and large teams needing to familiarise themselves with the guidance, instead of a few individuals needing to familiarise themselves with the guidance.
Costs of incident reporting	£72,921	£986	The IA assumed that there would be 1,348 incidents per year. PIR estimates 13 incidents per year, this is based on 2 years worth of data. If legislative changes are made, this number should increase but that will be assessed in the impact assessment that will follow.
Additional compliance costs	£237,080	£1,158,634	Increase in estimated additional compliance costs due to an increase in the wages of legal professionals and senior managers , as well as due to the

			inclusion of self-reported additional compliance costs by organisations. Often the costs reported were higher than estimated in the IA, which can be linked to organisations reporting that other teams were involved in these activities including engineers, consultants, and IT staff.
Additional security costs	£40,605,550	£101,139,091	The PIR estimates used 2019 and 2021 survey data which asked about NIS related security investment in three areas: internal staff, physical security and external costs. As the IA estimated additional security spending based on responses obtained during the consultation stage, the increase in the estimations can be understood in the context of organisations having a better understanding of the actual investments required in these areas due to the introduction of the Regulations.
Competent Authority costs	£4,104,035	£4,401,561	Updated estimates from competent authorities on their one off implementation costs, current annual costs and estimated future annual costs. Overall, there was an increase in the costs reported by competent authorities. Some of the drivers for increases in costs mentioned included investments in staff training as well as an overall increase in the resources allocated to the NIS Regulations since their implementation.

Where possible, we have updated cost data assumptions that were made in the impact assessment. 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 (less skewed by outliers). Overhead charges of 30% have been added to the wages, in accordance with the International Standard Cost Model Manual.[63] The compound annual growth rate in median wages for different occupations has been estimated using 2013 through 2021 ASHE wage data. This has been used to estimate future wage growth when modelling future costs from 2022 onwards. This differs from the NIS Post-Implementation Review 2020, in which simple (uncompounded) annual growth rates were calculated using ASHE wage data from 2013 to 2018. This approach was taken as it ensures that any volatility is accounted for in calculations.

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

For internal staff security costs, which are a component of additional security costs, cost estimates were taken from data provided from survey responses, which are in 2021 prices. To deflate the values into 2016 prices, DCMS used the data available in the Annual Survey of Hours and Earnings (ASHE). As cyber security does not have a specific SIC code, SIC code 62 has been used as a proxy. SIC code 62 is the computer programming, consultancy and related activities industry code; these cost figures were adjusted by using the growth rates of the median wage to estimate the staff security costs in 2018, 2019, and 2020 prices. The compounded annual growth rate using median wages between 2013 and 2021 taken from the ASHE for SIC Code 62 has been assumed to be constant for the future years in the appraisal period.

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

Since the Regulations came into force in May 2018, we consider 2018 to be the present value base year to reflect. This is in line with the original 2018 impact assessment but not the 2020 Post-Implementation Review. The current analysts believe that a less appropriate present-value base year was selected for the last post-implementation review. The previous present-value year was 2017 in the 2020 post-implementation review. 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 2021 ASHE (£)	**Hourly wage 2013 ASHE (£)**	**Compound annual hourly wage growth rate (%)**
Legal profession	£26.60	£22.85	1.92%
IT professional	£23.43	£20.06	1.96%
Corporate managers and directors	£22.81	£20.56	1.31%
Computer programming, consultancy and related activities	£20.85	£18.30	1.64%

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 both private and public sector - rather than businesses.

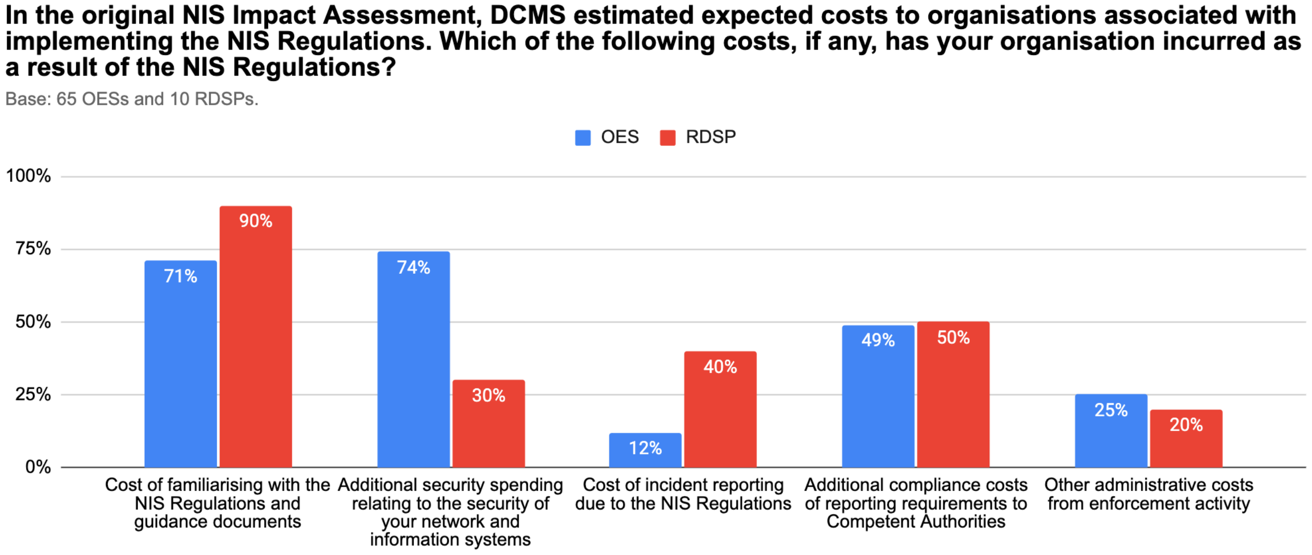
In calculating the direct cost to business, based on consultation with Competent Authorities, we have estimated that approximately 42% of organisations currently in scope of the Regulations are in the public sector. It should also be noted that while costs that public organisations have incurred have been evaluated in the same way as costs to business throughout, these costs are ultimately borne by the government.

In the Impact Assessment, DCMS estimated that the following costs would be incurred by organisations in scope of the Regulations:

- **Costs of familiarisation** with the NIS Regulations and guidance documents (£660.19 per organisation);[64]
- **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);[65]
- **Costs of incident reporting** due to the NIS Regulations (£54 per incident).[66]

As shown in Figure 3, which presents the proportion of organisations in scope of the regulations who reported incurring costs in each of these areas, the majority of operators of essential services reported incurring additional security costs, followed by familiarisation costs. The majority of relevant digital service providers reported incurring familiarisation costs, and half of the respondents reported incurring in additional compliance costs. Overall, fewer organisations reported facing other administrative costs.

Figure 3: Proportion of organisations in scope of the regulations who reported incurring costs associated with implementing the NIS Regulations.



To understand the costs incurred in more detail, the survey also asked organisations whether the costs estimated in the Impact Assessment were accurate. Overall, only 6% of operators of essential services

[64] DCMS, NIS Regulations: Impact Assessment (2018), p. 17
[65] Ibid, p.20
[66] Ibid, p.31

and 17% of relevant digital service providers indicated that these estimates were accurate for their organisation.[67] 33% of operators of essential services and 17% of relevant digital service providers did not agree that these costs were accurate.[68] The majority of organisations (61% of operators of essential services and 67% of relevant digital service providers) were unsure, responding that they did not know, even though organisations otherwise reported incurring these types of costs (Figure 1).[69] This may be because even though organisations can identify having incurred these costs, they might not be able to quantify these separately from their overall spending on security. It should be noted that this question did not allow organisations to indicate the accuracy or inaccuracy of some of the costs, and it is therefore not possible to know whether the organisations that indicated that these estimates were inaccurate referred to some or all of the costs presented in the Impact Assessment. This is something that should be changed for the next review.

Those organisations that indicated not agreeing that the estimated costs were accurate were further asked to clarify, for each of the estimated costs in the Impact Assessment, the number of hours required for work in each area, who was involved, and how much this cost. Overall, only 17 operators of essential services and two relevant digital service providers provided some of this information. With the exception of costs of incident reporting, the majority of these organisations' responses suggested that the estimates were too low. There was also a wide range of costs reported, indicating that there are many factors that affect additional costs, some of which may be specific to the organisation's needs.

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.[70] Organisations that responded to the survey reported an annual weighted average cost of familiarisation of £14,315 in 2016 prices, between those that agreed with the Impact Assessment estimates and those that provided other values.[71] Among these, organisations that responded that the estimated costs in the impact assessment were not accurate for their organisation and that provided further details on the costs of familiarisation incurred. This group of respondents that did not agree with the Impact Assessment estimates reported average familiarisation costs of £62,629 (2016 prices), with costs reported ranging from £1,200 to £500,000.[72] Most organisations reporting these costs pointed to managers and legal professionals being involved in the process of familiarisation with the NIS Regulations, although a few respondents also indicated that IT advisors, engineers, consultants, and cyber advisors were also involved. The respondent that gave an estimate of £500,000 did so sighting that several groups had to be familiarised with the NIS Regulations, including: "Operations, OT support, IT support, Management, Law, Cyber advisors, global support organisation". The response was included, despite being an outlier.

As initial evidence suggests that familiarisation costs exceeded those estimated in the Impact Assessment. It has been assumed that those organisations that did not agree that the estimated costs in the Impact Assessment were accurate incurred familiarisation costs equal to the weighted average reported (£14,315). It has also been assumed that the average number of hours taken for familiarisation costs compliance by the remaining organisations is the same as those estimated in the impact assessment. That is, the remaining organisations are assumed to require eighteen hours of legal and senior management time. ONS ASHE data was used to obtain hourly wages in 2018.

It has been assumed that all organisations in scope faced familiarisation costs, despite only 71% of operators of essential services and 90% of relevant digital service providers that responded to this

[67] Base: 66 OESs and 12 RDSPs.
[68] Base: 66 OESs and 12 RDSPs.
[69] Base: 66 OESs and 12 RDSPs.
[70] DCMS, NIS Regulations: Impact Assessment (2018), p. 17
[71] Base: 67 OESs and 11 RDSPs.
[72] There were 12 responses giving further information on familiarisation costs.

question in the survey having reported facing this cost. This conservative approach is consistent with the NIS Post-Implementation Review 2020 and has been taken as it is likely that all organisations faced some familiarisation costs, even if this was assumed to be business as usual. Moreover, relative to the NIS Post-Implementation Review 2020, there was an overall increase in the proportion of organisations reporting having incurred familiarisation costs by 13% in operators of essential services and 23% in relevant digital service providers.[73] This could indicate that as the NIS Regulations have been in place for a longer period of time, it is likely that organisations are better able to discern the amount spent on these costs from other related security spending. This leads to a total estimate of familiarisation costs of £740,377.37 in 2016 prices.

Table 4: Familiarisation costs, ONS ASHE 2018 revised figures

	Number of hours for familiarising with legislation	Number of hours for guidance documents	Hourly wage 2018 ASHE revised (£)	Total cost per organisation 2016, incl. overhead charge (30%)
Legal profession	6	6	£26.07	£406.69
Information technology and telecommunication directors	3	3	£37.28	£290.78

Median hourly wage source: ONS - Annual Survey of Hours and Earnings, 2018 revised estimates.

The estimate for familiarisation costs is higher relative to the estimate from the Impact Assessment due to both the increase in the wage of IT directors from £34.30 per hour (provisional ASHE 2016 estimates) to £37.28 per hour (revised ASHE 2018 estimates), and the increase in the wage of legal professionals from £25.17 per hour (provisional ASHE 2016 estimates) to £37.28 per hour (revised ASHE 2018 estimates). In addition to this, the estimate of familiarisation costs is higher due to the analysis taking into account self-reported costs by organisations.

We consider that including self-reported costs is an improvement in methodology as it provides a more accurate estimate given the evidence suggesting that familiarisation costs exceeded those estimated in the Impact Assessment. Moreover, we believe that this is an improvement relative to previous methodologies used in the Impact Assessment and 2020 Post-Implementation Review as feedback received from the RPC called for a more robust assessment of the cost of familiarisation to organisations in scope of the Regulations. The respondents that stated their costs were higher, often cited the need for all their technical staff to understand the Regulations and also they cited more senior positions that will have higher salaries than our estimates, such as the infosec manager. DCMS has noted this increase in familiarisation cost and will try to streamline any guidance that we send out to ensure that the Regulations are less burdensome to these organisations.

The NIS Regulations require organisations that have experienced an incident meeting the threshold to report this to their Competent Authority within 72 hours of discovery by completing an incident notification form. The specific information 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. The Impact Assessment estimated that there would be a total annual **cost of incident reporting** of £2,110. This was calculated by estimating a cost per incident of £54, using one hour and fifteen minutes of legal, IT, and corporate time, and then scaling this by the estimated number of

[73] Base: 90 OESs and 15 RDSPs.

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 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 continued to be lower than expected since the Regulations came into force, which implies a lower annual cost than estimated.

Among those organisations that responded that the estimated costs in the impact assessment were not accurate for their organisation and that provided further details on the costs of incident reporting incurred (8 operator of essential services and 1 RDSP), 67% reported zero hours spent annually in incident reporting due to the NIS Regulations, with no associated costs.[74] This could be explained in the context of the low number of reported NIS level incidents in organisations. Overall, organisations that responded to the survey reported an annual weighted average cost of incident reporting of £1,658 in 2016 prices. This figure was mainly driven by one organisation who reported having faced costs of incident reporting of £100,000, it should be noted that this respondent looked to have included costs of the incident response team and not just of reporting. It should be noted that as costs and time spent on incident reporting were provided on an annual basis it is not possible to estimate the cost per incident.

Due to the small number of responses, the majority of which indicated not having incurred any costs of incident reporting, it is not possible to assess whether the estimated cost of reporting each incident (£54), and the estimated time spent on incident notification was accurate or not. 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.

The Annual Survey of Hours and Earnings has been used to update the median average hourly earnings in 2018 for the three occupations above. This is summarised in Table 4 below. Updating the incident reporting costs using revised and provisional wage rates (ASHE 2018-2021) yields a cost of £53.07 per incident in 2018 prices, which has been inflated annually from 2022 using the wage inflation rates in Table 2.

Table 5: Incident reporting wage costs, ONS ASHE 2018 revised figures

	Median hourly wage	**Time spent on incident notification**	**Total cost of incident notification (including 30% uplift)**
Legal profession	£26.07	45 minutes	£19.55
Information technology and telecommunication professionals	£22.00	45 minutes	£16.50
Corporate managers and directors	£22.58	20 minutes	£7.45

Median hourly wage source: ONS - Annual Survey of Hours and Earnings, 2018 revised estimates.

The best (and low) estimate of the annual number of NIS incidents has been updated from Year 3 onwards of the appraisal period to a total of 13 incidents using the number of incidents recorded by NCSC in 2019. The number of incidents and estimated incident reporting costs for Year 1 and Year 2 are taken from the NIS Post-Implementation Review 2020 to reflect the estimation closer to this time period.

[74] A total of 9 respondents provided further information on incident reporting costs.

A flat rate of incidents is assumed for future years. The best (and low) estimate of the total cost of incident reporting was estimated to be £9,857 over the 10 year appraisal period, in 2016 prices.

The estimate for incident reporting costs is lower relative to the estimate from the Impact Assessment due to the updated number of incidents decreasing from 39 to 13 estimated incidents annually. However, if incident reporting thresholds are adjusted in the future, this may affect the number of incidents meeting the reporting threshold.

To account for uncertainty in the future number of incidents, and in line with HMT Green Book guidance, sensitivity analysis has been conducted by following the above estimations for the best (and low) annual number of NIS incidents but considering a scenario in which the number of incidents are doubled (26 total incidents) from Year 3 onwards. This yields a high estimate of the total cost of incident reported of £21,996 over the 10 year appraisal period, in 2016 prices.

The impact assessment 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.[75] These costs were calculated based on estimates of legal and senior management time used (three and a half hours for small organisations, twelve hours for medium organisations, and twenty-four hours for large organisations).[76]

Organisations that responded to the survey reported an annual additional compliance costs weighted average of £36,720, in 2016 prices.[77] Among these, organisations that responded that the estimated costs in the impact assessment were not accurate for their organisation and that provided further details on additional compliance costs incurred reported average additional compliance costs of £151,812 in 2016 prices, with costs reported ranging from £450 to £1,000,000.[78] Most organisations reporting these costs indicated legal teams and management being involved in additional compliance activities, although a handful of organisations also pointed to engineers, IT staff, consultants, and information security managers being involved in these activities. The respondent that provided the response of £1,000,000 was included as they indicated it takes over 2,000 hours of technical staff and middle management, which could generate a very high cost, despite being an outlier.

As initial evidence suggests that additional compliance costs exceeded those estimated in the Impact Assessment, it has been assumed that those organisations that did not agree that the estimated costs in the impact assessment were accurate incurred additional compliance costs equal to the weighted average reported (£36,720). It has also been assumed that the average number of hours taken for additional compliance by the remaining organisations is the same as those estimated to be faced only by large operators of essential services in the impact assessment. That is, the remaining organisations are assumed to require 10 hours of legal professional’s time and 14 hours of senior management time. The reason that some organisations stated it was higher is that they use multiple technical staff to complete their compliance. The original estimates assumed only directors would be involved from a technical standpoint. Organisations reported that they would use lead systems engineers, IT security analysts OPS engineers and OT security engineers. ONS ASHE data was used for hourly wages between 2018 and 2021, with wage growth rates in Table 2 used to estimate wage inflation rates from 2022 onwards.

Table 6: Additional compliance administrative costs, ONS ASHE 2018 revised figures

[75] DCMS, NIS Regulations: Impact Assessment (2018), p. 20
[76] Ibid, p. 20
[77] Base: 66 OESs and 11 RDSPs.
[78] There were 17 responses giving further information on additional compliance costs.

	Median hourly wage	Number of hours	Total per organisation (including 22% uplift)
Legal profession	£26.07	10	£318.01
Corporate managers and directors	£22.58	14	£385.67

Median hourly wage source: ONS - Annual Survey of Hours and Earnings, 2018 revised estimates.

Results of the survey show that 49% of operators of essential services and 50% of relevant digital service providers reported facing additional compliance costs as a result of the introduction of the Regulations (Figure 1).[79] Hence, our best estimate has assumed that these proportions of operators of essential services and relevant digital service providers have faced additional compliance costs in the year 2020/2021. We assume the same proportions for all future years of the appraisal period as, consistent with the 2020 Post-Implementation Review of the Regulations, the results of the survey continue to show that not all operators of essential services face these costs.[80] However, in Year 1 and Year 2 of the appraisal period it has been assumed that the additional compliance costs faced by organisations is equal to those estimated in the 2020 Post-Implementation Review. This leads to a best cost estimate of additional compliance costs of reporting of £11,586,339 over the 10 year appraisal period, in 2016 prices.

High and low estimates of additional compliance costs of reporting were also calculated by varying the proportion of organisations that incur in these costs from 2022 onwards. The high estimate of additional compliance costs of reporting of £13,267,880 (2016 prices) has assumed that all organisations in scope of the Regulations will incur these costs from 2022 onwards. This accounts for the possibility of higher compliance rates in the future as well as alternatives to the CAF framework used by Competent Authorities that lead to additional reporting requirements. On the other hand, the low estimate of £10,310,562 (2016 prices) has assumed that no relevant digital service providers incur these costs from 2022 onwards. This reflects the fact that only operators of essential services are required to provide evidence in this way to competent authorities.

The estimate for additional compliance costs is higher relative to the estimate from the Impact Assessment as a result of both introducing the assumption that the administrative compliance costs that firms incur is equal to the estimated costs for large operators of essential services, as well as having taken into account self-reported compliance costs. We believe that this is an improvement in methodology as it provides a more accurate estimate relative to the evidence suggesting that additional compliance costs exceeded those estimated in the Impact Assessment.

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.[81] 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,

[79] Base: 65 OESs and 10 RDSPs.

[80] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020), p. 30

[81] DCMS, NIS Regulations: Impact Assessment (2018), p.22

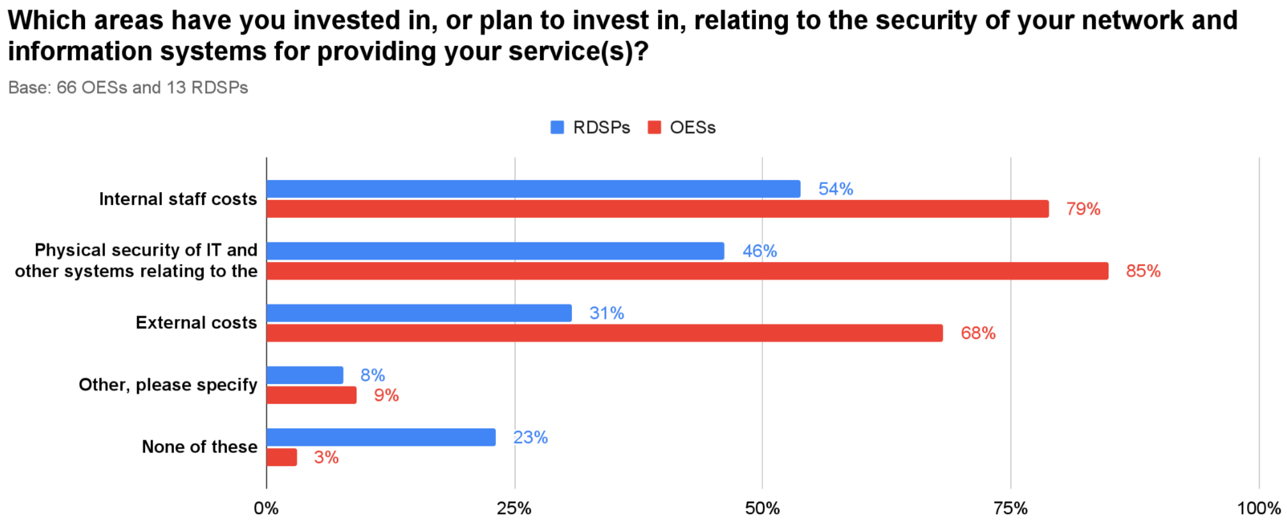
additional risk assessments and audits, staff training and testing and monitoring systems.[82] The additional security spending estimated in the Impact Assessment is summarised in Table 6 below.

Table 7: IA estimated additional cyber security spending estimates by size and type of organisation[83]

	Micro/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 surveys conducted, operators of essential services and relevant digital service providers were asked in which areas they have invested in, or plan to invest in, relating to the security of their network and information systems for providing their services. Selected choices included spending on internal staff costs, physical security of IT and other systems related to the delivery of their service(s), and external costs. The findings are summarised in Figure 4 below.

Figure 4: Proportion of organisations investing, or planning to invest, in areas relating the security of their network and information systems.

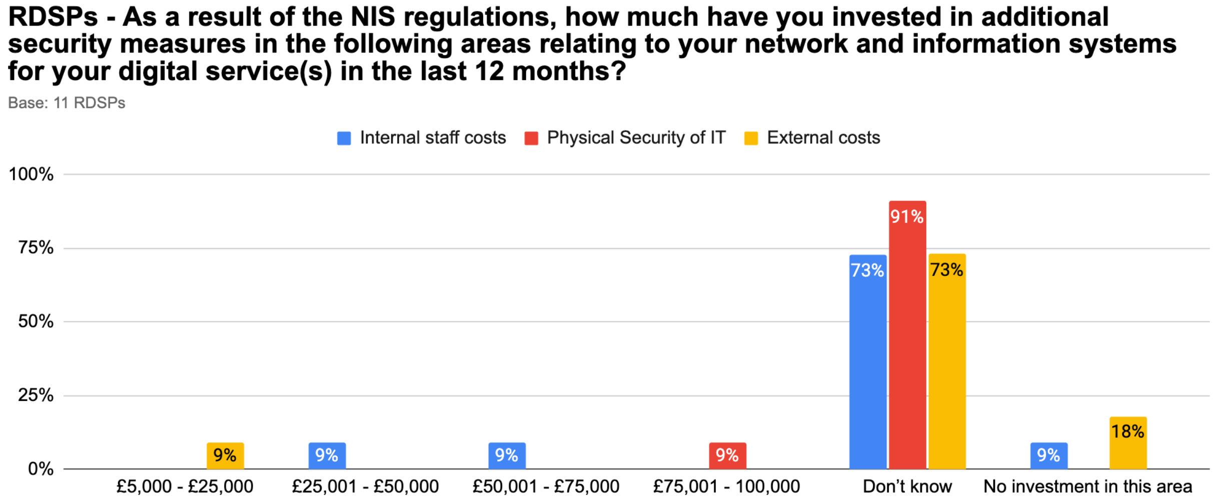


In the surveys conducted, operators of essential services and relevant digital service providers were also asked to report the amount invested in additional security measures as a result of the introduction of the NIS Regulations both in the last and next 12 months. In order to help respondents answer 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. These findings are summarised in Figures 5-8.

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

The large majority of relevant digital service providers who responded to the survey indicated not knowing how much their organisation had invested in additional security measures in all areas relating to their network and information systems in the last 12 months (Figure 3). Given this, and the small number of responses, it is not possible to assess whether the previously estimated additional security costs in the impact assessment were accurate for relevant digital service providers.

Figure 5: Relevant digital service providers - Investment in additional security measures as a result of the NIS Regulations in the last 12 months



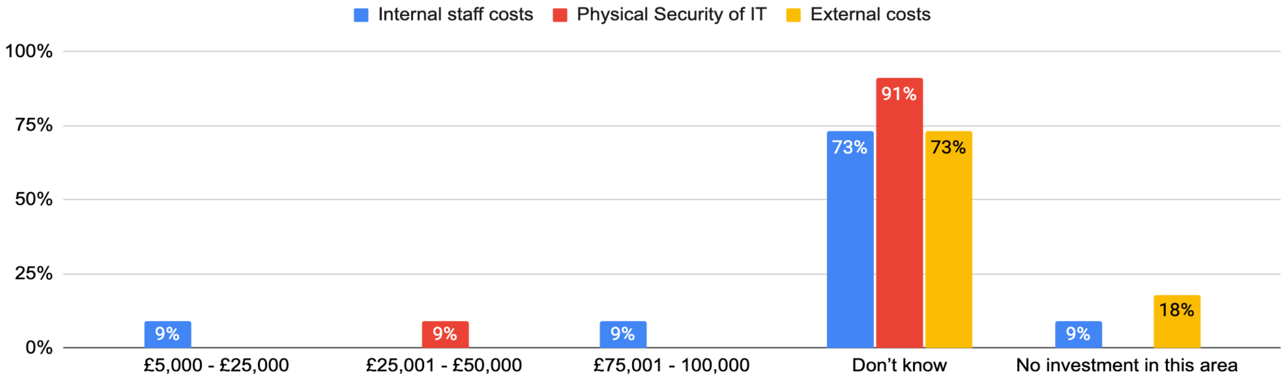
As previous evidence gathered in the 2020 NIS Post-Implementation Review suggested that relevant digital service providers spent more than the high estimated additional costs per business of £50,000, the additional security costs estimated for the appraisal period remain unchanged relative to those presented in the 2020 NIS Post-Implementation Review.[84] In line with this, the assumption that physical costs are one off costs, while internal staff costs and external costs are ongoing annual costs is maintained as there is insufficient evidence of future areas of investment for relevant digital service providers (Figure 6). The total cost of security investments for relevant digital service providers over the 10 year appraisal period is estimated to be £137,409,226, in 2016 prices, with high and low estimates of £139,564,633 and £135,292,926, respectively.

Figure 6: Relevant digital service providers - Investment in additional security measures as a result of the NIS Regulations in the next 12 months

[84] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020), p. 33-34

RDSPs - As a result of the NIS Regulations, how much do you plan to invest in additional security measures in the following areas relating to your network and information systems for your digital service(s) in the next 12 months?

Base: 11 RDSPs



The findings from the survey questions on the amounts invested in additional security measures provided useful and important information on the extent and areas of investment among operator of essential services, and showed that between 17% and 32% of large operator of essential services who responded to the survey spent more that the high estimated additional costs per business of £200,000. This was calculated by taking the lower bound of each of the cost brackets that organisations selected for each of the three categories and aggregating to obtain additional cost figures.

Estimates of additional security costs for operators of essential services in Year 1 and Year 2 of the appraisal period were taken from the 2020 NIS Post-Implementation Review to reflect the estimates calculated based on survey responses from that time period. Next to this, an estimate of additional security costs for operators of essential services has been calculated in Year 3 and Year 4 using the data provided in the survey for investments in additional security measures in the past 12 months. Similarly, operators of essential services' additional security costs in Year 5 and onwards were calculated using survey information on investments in the next 12 months.

Low, middle and high estimates were calculated by taking the low, middle values in each of the cost brackets (Figures 7-8) and applied to the proportion of operators of essential services that reported invested, or planning to invest, in each of the three cost areas (Figure 4). It has been assumed that the distribution of investments for respondents who responded with 'don't know' is the same as the distribution of investment across organisations that did indicate the amounts invested. Cost distributions were calculated and applied separately for each of the areas related to the security of network and information systems before being aggregated to obtain a total cost estimate. It has further been assumed that internal staff costs, physical security costs, and external costs are on-going costs among operators of essential services. This follows evidence obtained from the survey on operators of essential services that indicated that these organisations were planning to invest in all three areas in the next 12 months (Figure 8).

The total cost of security investments for operator of essential services over the 10 year appraisal period has been estimated at £857,097,441 in 2016 prices, with high and low estimates of £914,851,940 and £799,346,893, respectively. These estimates are higher for two reasons: the first is that there was an error in the previous calculations where a cost was converted into a base of millions mid-calculation, causing a much lower estimate being published; the second is that DCMS has reviewed its assumptions and based on the responses received, physical costs are now an ongoing cost and not an implementation cost.

Figure 7: Operators of essential services - Investment in additional security measures as a result of the NIS Regulations in the last 12 months

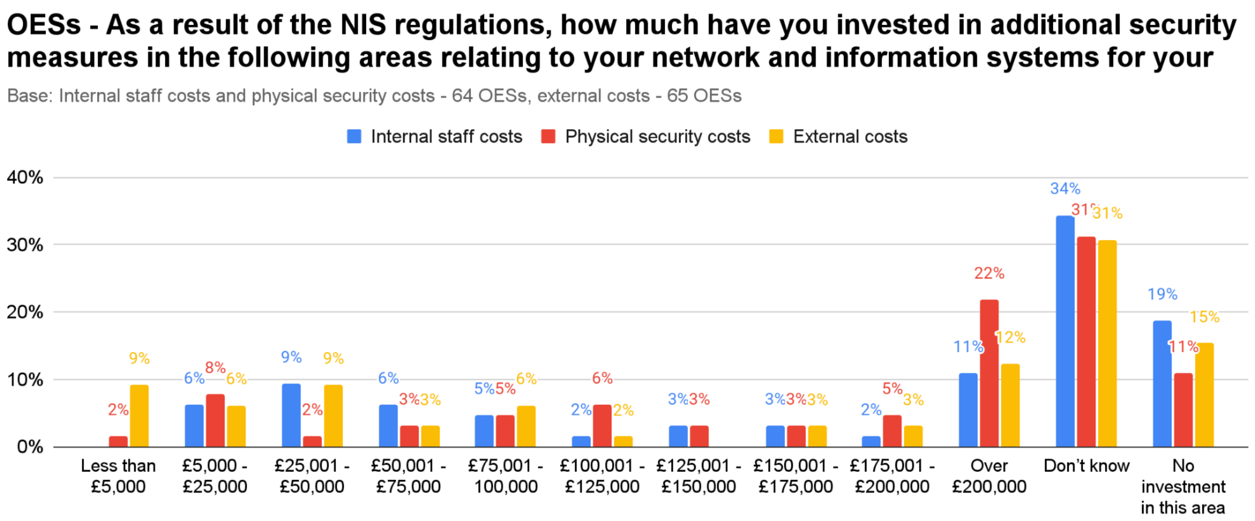
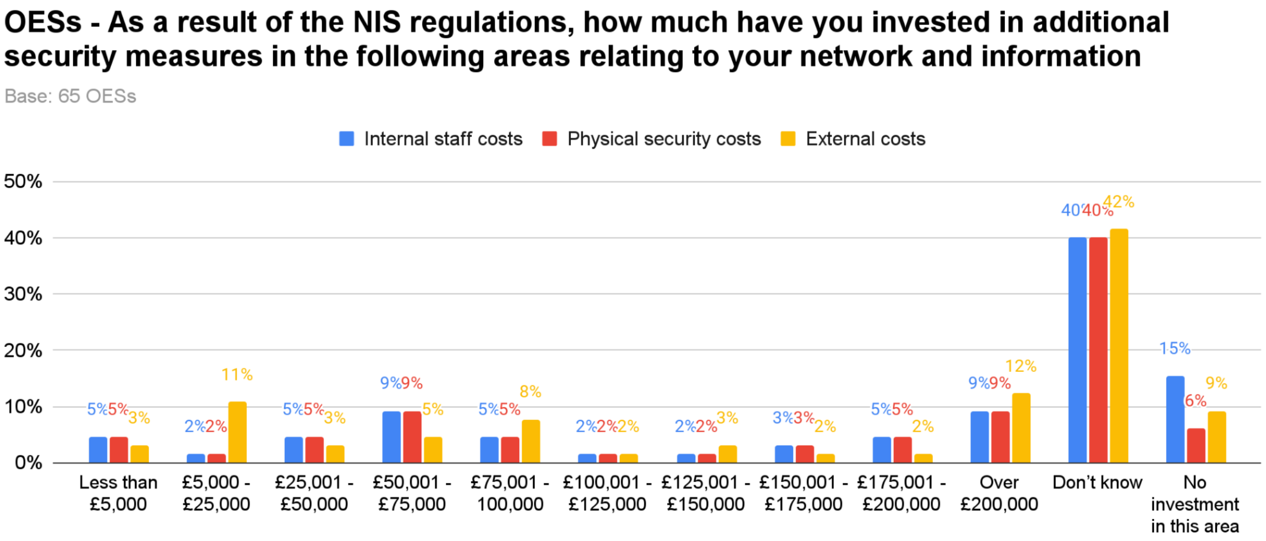


Figure 8: Operators of essential services - Investment in additional security measures as a result of the NIS Regulations in the next 12 months



Overall, aggregating the total cost of security investments for operator of essential services and relevant digital service providers yields a total cost of security investments for all organisations over the 10 year appraisal period of £951,663,313 in 2016 prices, with high and low estimates of £1,014,608,076 and £888,761,885, respectively. Again, note the error and the change in assumption in driving these estimates up.

Whilst DCMS cannot guarantee that this spending on cyber security spending is optimal, the regulations are outcome based in nature and some of this spending will be conducted to improve their cyber security. This is facilitated through spending to improve actions against their Cyber Assessment Framework. The Cyber Assessment Framework looks at meaningful cyber security improvements, and if this spending is to improve against the Cyber Assessment Framework, there is a low probability that this spending is simply a result of complying with regulations rather than improving security outcomes.

The Impact Assessment also identifies **additional administrative costs resulting from enforcement activity** as a possible cost to businesses. Given that few information notices have been issued by Competent Authorities it is not possible to robustly quantify or monetise the burden to organisations from enforcement activities. Moreover, there have been no appeals or penalty notices received. This is in line with the 2020 NIS Post-Implementation Review. However, this may change if in the future there is an increase in enforcement activity in which case this question will be best answered in subsequent reviews.

In addition to testing the assumptions and cost estimates specified in the Impact Assessment, the review team also tested whether there were any **unexpected costs** incurred by organisations that were not addressed in the impact assessment. The majority of operators of essential services and relevant digital service providers reported not having incurred any unexpected costs that were not covered in the original NIS Impact Assessment (83% of operators of essential services and 83% of relevant digital service providers).[85] Unexpected costs which organisations incurred included costs related to independent external auditors and consultants, replacing downstream legacy infrastructure, as well as time spent assessing compliance levels, including extra time spent 'unpicking' the Cyber Assessment Framework. Some operators of essential services reported fees from Competent Authorities and legal consultations as unexpected costs, but these costs were clearly stated in the impact assessment.[86]

In response to the consultation impact assessment, the Regulatory Policy Committee outlined other possible costs that may be incurred by business,[87] which are addressed here in turn:

i) Whether the directive affects the price of essential services and the number of workers employed by essential service providers. Hiring of additional staff was indicated by 43% of operators of essential services and 8% of relevant digital service providers as an action taken with regards to resourcing to support the implementation of the NIS Regulations when they were introduced.[88] However, the evidence indicates that the directive has had no significant effect on the price of essential services as the majority of organisations (93% of relevant digital service providers and operator of essential services) indicated not having passed any costs to consumers as a result of the introduction of the NIS Regulations or this not being applicable as organisations do not charge for their services/control the prices charged to consumers.[89] This is consistent with the 2020 NIS Post-Implementation Review in which only 1% of operators of essential services and 6% of relevant digital service providers reported having passed on costs incurred as a result of the Regulations to consumers.[90]

ii) Whether the measures will have a disproportionate impact on small businesses. There is no direct evidence that the directive has had a disproportionate impact on small businesses. The impact assessment estimated that with one exception (in the digital infrastructure sector), no operator of essential services is a small or micro business, and small and micro businesses are specifically excluded from the DSPs aspect of the directive.[91] Although it is not clear what the overall size of the small business population brought into scope of the Regulations, no small organisations completed the online survey as part of the review process and none of the responding Competent Authorities indicated having a small businesses in scope of the NIS Regulations. This is different from the 2020 NIS Post-Implementation Review in which two small organisations completed an online survey as part of the review process, with two Competent Authorities having indicated having a small business in scope of the NIS Regulations. Small businesses were defined the same way as the 2020 Post-Implementation Review as having: not more than 50 employees; turnover <£10.2m; and balance sheet total <£5.1m. This means that as the NIS Regulations stand there is no direct impact on small and micro businesses as none have been identified as being in the NIS Regulations. Whilst there were 2 SMEs in the last

[85] Base: 65 OESs and 12 RDSPs.
[86] DCMS, NIS Regulations: Impact Assessment (2018), p.18
[87] Ibid, pp.4-5
[88] Base: 68 OESs and 13 RDSPs.
[89] Base: 64 OESs and 13 RDSPs.
[90] Base: 110 OESs and 20 RDSPs.
[91] DCMS, NIS Regulations: Impact Assessment (2018), p.4

review, these companies might have either fallen below the designation thresholds, ceased trading or could have grown into larger organisations. Unfortunately, DCMS does not keep data on which companies are designated under the NIS Regulations, so we cannot check which is true. From other evidence we have gathered, we do not have any evidence that the Regulations are overburdensome, as our estimated costs in the Impact Assessment were smaller for smaller businesses.

iii) Whether costs will differ among essential service providers from different sectors (e.g. energy, transport and health care).

In order to address this question we conducted further analysis to determine whether security investments across sectors systematically differed across and within spending categories (internal staff, physical security, and external costs). This analysis made use of the previously presented survey findings in which organisations were asked to report the amount invested in additional security measures as a result of the introduction of the NIS Regulations both in the last and next 12 months (Figures 7-8). An estimate of average amount invested by sector was obtained by taking the middle values in each of the cost brackets and applied to the proportion of organisations that reported invested, or planning to invest, in each sector. We have excluded from the analysis those respondents who indicated not knowing this information. Moreover, the analysis is only conducted where the number of respondents in the sector was greater than three to ensure anonymity of respondents. Finally, to account for possible time variations in investments (i.e. organisations investing more in the future as a result of having invested less in the past, and vice versa), comparisons across sectors were drawn using the average of past and estimated future investments reported. These findings are summarised in Table 7 below.

Table 8: Estimated average annual investments in additional security measures across sectors[92]

Spending category	Energy	Health	Water	Transport
Internal staff costs	£95,851.30	£26,093.58	£118,125.45	£69,992
Physical security	£134,458.71	£67,013.92	£140,625.58	£106,714.90
External costs	£84,041.88	£16,102.80	£118,750.33	£53,095.25

Organisations in the water sector have the highest average amount invested annually across the three spending categories, followed by organisations in the health sector. Overall, organisations in the health and transport sectors appear to have significantly lower average annual investments relative to organisations in the energy and water sectors. While one possible explanation for this could relate to differences in the preparedness for cyber security across different sectors, it is difficult to assess this without better understanding the main drivers for investment across different sectors. As such, this would be better addressed in subsequent reviews.

DCMS will provide the competent authorities that request their sector's data with a summary of the findings from their sector. Feedback is being highlighted to the competent authority to help them implement the Regulations as effectively as possible in their sector. Costs could vary between sectors due to the different nature of their network and information systems.

iv) Whether the impact assessment has considered all the potential costs and benefits.

[92] Base: internal staff costs - 42 OESs, physical security costs - 44 OESs, external costs - 45 OESs.

Costly interaction between the NIS directive, the UK General Data Protection Regulation (GDPR) and the e-privacy directive. Relevant digital service providers indicated a link between NIS related investments in their organisation and measures taken to comply with the DPA 2018 and UK GDPR in 54% of the cases.[93] Moreover, all of the RDSP respondents who reported having strengthened existing processes/procedures for recovery from a security incident as a result of the NIS Regulations indicated that these processes were influenced or affected by the UK General Data Protection Regulations and the Data Protection Act 2018.[94] Next to this, 78% of operators of essential services and 86% of relevant digital service providers reported complying with the UK General Data Protection Regulation and the Data Protection Act 2018 as a reason for taking action to improve network and information systems security prior to the introduction of the NIS Regulations.[95] Despite these indications of an interaction between the NIS Directive and the UK General Data Protection Regulations, only one out of four organisations that responded to a question on challenges indicated this leading to an increase in costs as a result of having to assess incidents against additional criteria as well as exposure to fines under both NIS and UK GDPR. Based on this, and given that the approach of the directive was aligned with that of the UK GDPR we do not find substantial evidence of this interaction resulting in higher costs for organisations. With regards to financial penalties, the directive included a requirement that other legislation was taken into account to minimise duplication of fines, and thereby minimise the possible costly interaction between the NIS directive and other regulations. DCMS has taken note that one out of four organisations feels there is a costly interaction between the two sets of regulations and we will work with data policy stakeholders going forward to ensure any changes made to the NIS Regulations produces as little costly interaction as possible.

Establishment costs for regulators. A multiple competent authorities approach was identified in the impact assessment as the most suitable approach, allowing lead government departments and regulators to build on their existing sector relationships and use their sector expertise to set guidelines and conduct enforcement activity. As set out in the impact assessment, lead government departments and the devolved administrations have provided their best estimate of additional resources from the information available. In order to assess the accuracy of the estimated establishment costs as part of the review process DCMS asked Competent Authorities to report the cost of implementation of the NIS Regulations, and establishment costs estimates have been updated accordingly. These estimates are laid out in the following section of the post-implementation review.

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. 67% of operators of essential services who responded to the survey indicated having invested, or planning to invest, in external costs related to the security of their network and information systems for providing their services.[96] These costs included outsourcing the management of cyber security, hiring external consultants and/or expertise, among others. It is not clear whether there is an overlap between this category of external resource and the services provided by digital service providers in scope of the Regulations. As such, it is not possible to assess whether there has been an increase in revenue of digital service providers as a direct result of the introduction of the Regulations.

Competent Authority Costs

Under the NIS Regulations, costs incurred by Competent Authorities to regulate NIS are in some cases being passed on to organisations. The impact assessment included high-level estimates of the annual

[93] Base: 13 RDSPs.
[94] Base: 6 RDSPs.
[95] Base: 68 OESs and 13 RDSPs.
[96] Base: 67 OESs.

costs of operating Competent Authorities. As part of the review process DCMS asked Competent Authorities to provide estimates of their annual costs incurred as a result of the NIS Regulations; of the ongoing annual costs they expect to incur in the future; and of their initial one-off implementation costs. This is summarised in Table 8.

The figures suggest that in most cases the estimates in the impact assessment were too high, although the majority of Competent Authorities indicated expecting costs to increase in the future. Some of the drivers for future cost increases include the new legislative measures currently being proposed by DCMS as well as the delivery of the CAF framework. As a result of this, 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 the regulations, including bringing new firms under the regulations or changing the incident reporting guidelines, 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.

Where possible, estimated one-off implementation costs were taken from the NIS Post-Implementation Review 2020 as we consider figures to be more accurate since the review was closer to the implementation period.[97] Most Competent Authorities 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 impact assessment.[98] In both cases the initial implementation cost incurred was lower than those estimated in the impact assessment.

Implementing the Regulations has led to other costs for government, which are addressed here in turn:

- 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 of.

[97] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020), p. 38
[98] DCMS, NIS Regulations: Impact Assessment (2018), p.20

Table 9: Estimated and reported Competent Authority annual costs, 2016 prices

Competent Authority sector	Competent Authorities	Reported one-off implementation costs	Reported annual costs	Reported future annual costs
Transport (maritime, road,rail)	Department for Transport	£7,516.20*	£764,680.20	£764,680.20**
Transport (aviation)	Civil Aviation Authority	£443,550.00	£266,130.00	£266,130.00
Energy (electricity, oil, gas)	BEIS and Ofgem (joint competent authority)[99]	BEIS, Ofgem and HSE:		
		£1,018,317.89*	£1,410,489.00	£1,410,489.00
Digital infrastructure	Ofcom	£39,919.50	£91,388.15	£91,388.15
Health	Department of Health and Social Care	£33,852.04*	£39,916.40	£39,916.40
Drinking water supply and distribution	Defra & Drinking Water Inspectorate	DWI[100]:		
		£79,859.67[101]*	£194,744.18	£203,615.18
Digital service providers	ICO (UK wide)	£97,666.50*	£691,938.00	£1,133,856.62
Devolved Administrations (aggregated across sectors)				
Scotland	Scottish Government, Drinking Water Quality Regulator (Scotland)	Health: £178,509.85*	£221,775	£221,775
		Water:[102]	£50,878	£50,878**
Wales	Welsh Government		£414,755	£414,755
Northern Ireland	Department of Finance (Northern Ireland)	£14,187*	£159,678	£221,775

* Figures from NIS PIR 2020. ** Where no future cost data was provided, it has been assumed that future costs will be equal to current annual costs

The **cost of operating Competent Authorities** was calculated using the estimates provided by the Competent Authorities in Table 8. In Year 1, the cost was assumed to be the one off implementation cost plus the annual cost reported in the NIS Post-Implementation Review 2020.[103] Where competent authorities did not provide an estimation of their implementation costs in the 2020 NIS PIR, this cost was taken to be equal to the estimated cost provided by competent authorities in their report for this Review. Year 2 and Year 3 costs reflect, respectively, the annual costs and future annual costs reported in the NIS Post-Implementation Review 2020.[104] Year 4 and Year 5 cost figures are equal to the reported

[99] BEIS and Ofgem are the joint Competent Authority for the downstream gas and electricity subsectors.

[100] 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.

[101] This was reported to be incurred in the financial year 2020-21 (year three of the appraisal period).

[102] Only annual costs incurred

[103] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020), p. 38

[104] Ibid, p. 38

annual costs (Table 8). Costs in Year 6 onwards are assumed to be equal to reported future annual costs (Table 8). Where future costs were not provided, it is assumed that the annual costs will remain constant for the remainder of the appraisal period.

The total one-off implementation cost of setting up Competent Authorities has been estimated as £1,913,379, while the total ongoing costs have been estimated to be £44,015,607 over the 10 year appraisal period, 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 operator of essential services. These are therefore costs to the government.

The total cost of operating Competent Authorities has been estimated over the 10 year appraisal period to be £44,982,987 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 £40,264,896 and £56,081,017 respectively.

Benefits

The key benefit of the Regulations outlined in the impact assessment 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

Building on the previous post-implementation review, DCMS has received incident data for the years of 2019 and 2020. NCSC, acting in its NIS Single Point of Contact role, collates NIS incident data with a year lag. In 2019 and 2020 there were 13 and 12 incidents respectively. Whilst there appears to be a decline in incidents by 1, this does not show us the risk that these organisations pose to the UK economy. Both operators of essential services and digital service providers were aware of the incident reporting thresholds with 93% and 92% of organisations respectively being aware of the thresholds.[105] Whilst 69% of digital service providers and 69% of operators of essential services found the incident reporting thresholds appropriate for their sector, 7 out of 9 competent authorities reported that the incident reporting threshold was too high, suggesting that the number of NIS incidents in its current form may be an inappropriate metric.

The number of incidents reportable under the NIS Regulations is lower than initially expected in the impact assessment where the best estimate of annual incidents was 39. The number of incidents being lower than expected and decreasing is not likely to be explained by Covid-19, as the pandemic has seen the number of cyber incidents that NCSC are involved in increasing.[106]

Overall, 59% of operators of essential services and 46% of relevant digital service providers who responded to the survey indicated having up-to-date incident response plans as a result of the introduction of the NIS Regulations.[107] As a result of this, the impact incidents have on the provision of services of organisations that fall in scope of the Regulations is likely to be reduced. Moreover, the

[105] Base: 67 OESs and 13 RDSPs.
[106] https://www.ncsc.gov.uk/news/record-number-mitigated-incidents
[107] Base: 67 OESs and 13 RDSPs.

increased cyber resilience as a result of this could mean that there has been a reduction in the number of incidents that meet the thresholds, although there is not enough evidence to conclude this.

Due to the lack of sufficient evidence, it is not possible to build a counterfactual position of the amount of incidents that would have occurred had the Regulations not been introduced. Even if the number of attacks avoided could be calculated, estimating the cost associated with this would entail several difficulties. For example, although the Wannacry attack on the NHS in 2017 was well documented, the costs associated with it were only estimated on the grounds of lost output and IT costs, and did not incorporate the knock-on impact on patients with over 19,000 appointments cancelled.[108] Even without taking into account these social costs, the total financial cost of Wannacry was estimated at £92m.[109] This figure illustrates the potential benefits to the organisation itself of avoiding a cyber breach, thereby highlighting the significant positive impact that the Regulations can have on organisations. The Cyber Security Breaches Survey reveals that the mean cost of a cyber breach to medium/large UK businesses is £3,930 (in 2021 prices)[110]. There are issues with using this estimate as they are the internal costs to businesses and do not include the social costs of an essential service being taken down. As the original impact assessment states, the rationale for intervention is centred on the cost to society and the negative externality that cyber risk in these organisations creates. The £3,930 figure also includes breaches that would never be reported under the NIS Regulations, such as phishing incidents, a second reason that the estimate is an underestimate and inappropriate to use in this analysis.

Furthermore, the size of the benefit external to the organisation can be highlighted in research referenced in the Impact Assessment modelled the economic costs for a sophisticated cyber attack on the 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.[111] 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.[112]

A recent attack on Kaseya demonstrated that digital service providers need to have good cyber security. Up to 1,500 firms were impacted as a result of a digital service provider being breached.[113] This again demonstrates the large impact outside of the firm a cyber attack can have and the negative externality from poor cyber security. This also highlights a further point raised by competent authorities about the risks posed by the supply chains of firms regulated by NIS. Although the estimated cost of the attack remains unclear, the cybercrime outfit initially demanded a payment equivalent to $70m.[114]

Cyber threats to critical national infrastructure in the UK are an ever present threat. A recent independent report commissioned by Bridewell consulting found that 86% of the critical national infrastructure they interviewed have detected a cyber attack on their systems in the past 12 months. Of those 86%, 93% experienced at least 1 successful attack in the last 12 months.[115] This demonstrates that the examples

[108] DHSC, Securing Cyber Resilience in Health and Care (2018), p.14
[109] Ibid, p.14
[110] DCMS, Cyber Security Breaches Survey (2021), p.52
[111] Cambridge Centre for Risk Studies, Integrated infrastructure: cyber resilience in society (2016); DCMS, NIS Regulations: Impact Assessment (2018), p.33.
[112]Cambridge Centre for Risk Studies, Integrated infrastructure: cyber resilience in society (2016); DCMS, NIS Regulations: Impact Assessment (2018), p.34.
[113] https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/
[114] The Guardian, Tech firm hit by giant ransomware gets key to unlock victims' data (2021).
[115] CNI Cyber Report: Risk & Resilience, commissioned by Bridewell consulting.

above could turn into realistic recurring scenarios without the presence of good cyber resilience, enforced by the NIS Regulations.

Other reported benefits

Other benefits than incident reduction have been recorded in the surveys by both the organisations regulated and the competent authorities. 71% of operators of essential services stated that they have an increase in board support for cyber security, and 43% reported the regulations improving their understanding of organisations' aggregate risk.[116] Only 13% of operators of essential services reported not having any unexpected benefits.[117] Other sighted benefits in open text responses include: improving the way they assess their supply chain; improving engagement with customers; and two organisations stated an improvement in general awareness of cyber security.

Relevant digital service providers indicated less unexpected benefits than operators of essential services, as 46% of respondents said they had no unexpected benefits.[118] 31% of relevant digital service providers did report having an improved understanding of their firms' aggregate risks, 31% also stated they have increased board support for cyber security and 23% stated updating general incident management processes.[119] These benefits were lower than reported in the last post-implementation review across all respondents who reported having improved their understanding of their organisations risk (-51% to the last Post-implementation Review), updated general incident management processes (-44%), increased board support for cyber security (-34% to the last Post-implementation Review), and having shared good practises with other relevant digital service providers (-100% to the last Post-implementation Review). These benefits still exist, there are just fewer respondents reporting them.

Aggregated Costs and Benefits

The costs and benefits have been developed from the last review, where certain unknowns such as the number of incidents that are reported under the NIS Regulations are now based on data from previous years. Assumptions that have now been proven to be wrong such as physical costs being a set-up cost instead of an ongoing cost, we have now amended this assumption in our modelling and is 1 reason why costs have increased. Whilst the benefits section was not able to deliver a monetised benefit, this is something that will always be a problem no matter the review period, or resources available. Using evaluation techniques such as quasi experimental designs would not be possible due to the differing regulations in various other countries meaning it would be impossible to determine what is driving the impact. There would also be the issue that other countries report on different definitions of cyber incidents, and some not at all.

The total net present value (table 9) 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% to a base year of 2018. While it has been assumed that Competent Authorities did not pass any of their initial implementation costs onto organisations, 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 impact assessment, 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:

[116] Base: 68 OESs.
[117] Base: 68 OESs.
[118] Base: 13 RDSPs
[119] Base: 13 RDSPs.

Table 10: 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; 2018 present value)	Low/Best: -£402.59m	-£202.54m	£20.4m
	High: -£215.98m		
PIR estimates (2016 prices; 2018 present value)	Low:-£812.1m	-£498.4m	£57.9m
	Best:-£871.7m		
	High: -£935.7m		
PIR estimates - For IA comparison (EANDCB: 2014 prices; 2018 present value)	Low:-£789.8m	-£423.5m	£49.2m
	Best:-£847.8m		
	High: -£910.0m		

There has been a large increase in the net direct cost to business. This has mainly been due to two reasons:

1) a change in assumptions around spending on additional cyber security costs;

2) a correction on the last post-implementation review due to a calculation error.

Firms spending more money on their cyber security, whilst counted as a cost, should increase the benefits, provided the spending is carried out on the right cyber security activities. This increased security will lead to a lower risk posed to the UK economy from a firm's cyber security, a key aim of the policy.

For this policy to break even based on the likely under estimate of the wannacry attack at £92m the NIS Regulations would have to avoid less than 1 wannacry attack per year, although given the likely underestimate of this cost it is likely to be a much lower rate than 1 per year. DCMS's work on quantifying and monetising the cost of breaches going forward will help to better assess the breakeven of the NIS Regulations going forward.

7) Is government intervention still required?

There is strong evidence that government intervention in the form of these regulations is still required. Analysis done through this Post-Implementation Review has indicated that there are incentives to improve network and information systems security (please refer to section 5); these vary from previous experiences of a breach to incentives to avoid financial loss and maintain business continuity. Compliance with other regulations has also been cited as a reason; however, since the introduction of the NIS Regulations, there has been a marked increase in the introduction or strengthening of policies and processes to protect network and information systems. Considering that there is a lack of financial incentive for investment in this space, and the potential impact on the operator and the wider economy due to a breach, it is vital that these improvements continue at a rapid pace. Without regulation, new emerging sectors risk being undermined by operators offering insecure services, putting customers and ultimately the economy at risk.

This aligns with responses from the May 2021 Supply Chain Call for Views[120]. Respondents indicated that despite supply chain cyber security risk being a concern, there was little will from companies themselves to prioritise investment in this area. In the 2021 Cyber Security Breaches Survey, only 36% of large firms reviewed the cyber risks from their immediate suppliers. This highlights the need for regulation to assist organisations in managing their cyber risk. In the Supply Chain Call for Views, respondents were asked about 5 different government actions[121]. More than 80% of respondents stated that each of the 5 government actions to incentivise higher quality of supply chain risk management would be at least somewhat effective. The action with the highest proportion of respondents stating it would be very effective was the option to implement “Regulation to make procuring organisations more responsible for their supplier risk management” with 58% of responses being it would be ‘Very effective’.[122] It can be assumed from this feedback that regulatory incentives are, from industry’s perspective, still deemed the most effective way to drive behavioural change. It is important to note that the government seeks overall to maintain a proportionate approach, and will balance more forceful interventions such as the NIS Regulations, with softer involvement.

Other levers to improve cyber security in UK companies are being explored, such as raising awareness through cyber insurers and other market influencers. These alternative interventions however will apply largely to firms with a lower risk to the economy should they have a cyber breach. DCMS deems that market intervention is still required for the firms that are essential to the UK economy and that the tools used to implement the NIS Regulations such as the Cyber Assessment Framework, ensure that these firms implement the required cyber security improvements.

In order to ensure that the regulations remain appropriate and that their effectiveness is evaluated appropriately, this Post-Implementation Review recommends that the government consider more in-depth and tailored key performance indicators for the next reporting period. As the next Review is due in no more than 5 years time, this will allow for a more in-depth study; the following sections on areas for improvement and next steps will consider the need for this.

[120]https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security

[121] The 5 different government interventions were: Awareness raising of the importance of supply chain risk management through the use of campaigns and industry; Additional support to help organisations to know what to do; Providing a specific supplier risk management standard; Targeted funding to help stimulate innovation and grow commercial offerings that support organisations and their cyber security and; Regulation to make procuring organisations more responsible for their supplier risk management.

[122] https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security, 3.9E: Additional government support required, Q13

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

In view of evidence gathered from regulated organisations, competent authorities and the NCSC, as part of the Post-Implementation Review, there is a strong indication that without NIS, cyber security improvements across essential services in the UK would proceed at a much slower pace. The NIS Regulations also have the added benefit of covering a large number of sectors, which is expected to address some of the inconsistencies of managing risks to networks and information systems across sectors.

In particular, the NIS Regulations will help to fulfil Objective 2 in the Cyber Resilience Pillar of the National Cyber Strategy: “to prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens.”

Areas of improvement in the Regulations’ implementation do remain. However, regulatory intervention seems to be the most appropriate approach, for the reasons outlined in the previous section.

Industry seems to support regulation as the best form of government action. More detail on this is outlined in the May 2021 Supply Chain Call for View findings in section 7 above. Findings from this year’s Post-Implementation Review reinforce this conclusion: regulators have urged to bring third party providers under the scope of the NIS Regulations. Nonetheless, other levers besides regulations are also currently being explored, and DCMS will explore the possibilities by working with stakeholders: including other government departments, cyber insurance companies and industry as a whole. Some of the further legislative measures are included in the proposals to improve the cyber resilience of the UK. Should these other forms of government action prove to effectively improve companies’ approach to cyber security, the NIS Regulations may need to be reconsidered, and a different government approach for essential service sectors currently covered by the NIS Regulations may need to be investigated. It is the current view of DCMS that these non-statutory tools are not as effective at managing the cyber risk of these firms as the NIS Regulations.

The Cyber Assessment Framework is a key highlight of the regulations, this has allowed the experts in the competent authorities to review an organisation’s cyber security arrangements and ensure that improvements are made. There have been a total 67 known operators that have received improvement plans, highlighting the work of the NIS Regulations in improving cyber security in the sectors. Improvement plans would include, amongst many other things, updating legacy systems and software to reduce the vulnerabilities in their systems. Without these improvements, key organisations to the economy could’ve had vulnerabilities that could’ve been exploited. As the objective of the NIS Regulations is to improve the cyber resilience of operators, and the CAF being an effective, outcome-based risk assessment tool which relies on tailored advice to operators in scope, this has also led to a closer relationship between organisations and regulators / the NCSC. As evidenced by responses to the Post Implementation Review surveys, where 86% of regulators highlighted the closer working relationships with organisations as one of the top benefits of NIS.

The Regulations are designed in a way that encourages compliance and enforcement is used as a last resort. This ensures that the regulations are not overburdensome on industry and the regulations are not seen as punitive measures. Enforcement has only been confirmed to have been carried out by 2 competent authorities, which raises the question of "is the enforcement regime appropriate?" DCMS’s stance on this is that the enforcement regime equips the competent authorities with the right tools to ensure the regulations meet their objectives and in its current form is appropriate. NCSC has also been informed of one very successful instance of a competent authority carrying out enforcement, which had very positive outcomes, suggesting that the enforcement regime may be appropriate.

9) EU-derived regulations

This section compares the UK implementation of the NIS Directive to EU member states, identifying areas where UK transposition can be improved.

The UK's implementation of the NIS Directive did not go beyond the minimum requirements of the Directive. The UK Government kept the scope of its implementation to the requirements set out in the Directive. The Government excluded the finance and banking sectors from the scope of the transposition, as these sectors were covered by already existing legislation that provided equivalent measures. No formal assessment of the UK's implementation has been carried out by the EU.

In December 2020 the European Commission put forward a new proposal for the NIS Directive (referred to as NIS 2.0). This proposal would repeal the 2016 iteration of the NIS Directive and make significant changes to the NIS framework across the European Union. Any revised NIS Directive would not be adopted by the UK, as we are no longer a member of the EU. Such changes are of interest to the UK and will be monitored closely in order to assess the impact on companies operating in both the UK and the EU.

The EU NIS framework is based on an EU Directive, and not a Regulation, meaning that all EU Member States (including the UK, at the time) were required to transpose it into national legislation. This meant that EU Member States implemented the provisions required by the Directive into their domestic legislation in their own manner. This resulted in variations in the implementation of the Directive between countries, with some countries including different aspects (such as additional sectors) not mandated by the Directive. This created some divergence between countries in relation to NIS implementation. For instance, the UK's use of an outcome-based risk assessment framework, such as the CAF, was not replicated at EU level, and EU Member States have many different approaches at national level. In addition, operators of essential services have different incident reporting thresholds in different countries, even though they are required to report incidents in different countries in the EU if an impact affected more than one country. This has led to some confusion in when operators should report.

Proposed EU changes to the NIS Directive regime

The EU is proposing significant sectoral expansion for NIS to include sectors such as waste water, public administration, and space, as well as expansion of existing sectors to include new subsectors. The UK is considering some sectoral expansion (see our cyber resilience legislation consultation), but not to the same extent.

There are other key distinctions between the EU and the UK worth noting. One is the requirement for digital service providers and operators of essential services based outside of the EU and UK, but operating in both the UK and the EU to designate a representative in both jurisdictions. The requirement to nominate a UK representative was introduced by virtue of SI 2019/1444. Digital service providers and operators of essential services will also be required to register in both the UK and the EU, following the UK's withdrawal (SI 2019/1444 and SI 2020/1245).

The UK has also amended the incident reporting thresholds for digital service providers, which were established as a Commission Implementing Regulation (2018/151).These rules were harmonised across the EU, including the UK at the time, and set the security elements and factors that established whether an incident was reportable. Under the new amendments, made by SI 2021/1461, digital service providers will be required to report under a lower threshold in the UK having regard to guidance issued by the Information Commissioner as opposed to factors specified by the EU.

Penalties

NIS 2.0 both limits the potential fine to 10 million euros (in comparison to £17 million in the UK), but also provides another criteria of 2% of worldwide annual turnover. This lifts the potential fine for larger-scale operators with high worldwide annual turnovers. The UK has fines capped at £17 million.

Potential divergence

Overall, the changes proposed under NIS 2.0 above will create some differences between the UK and the EU in terms of implementation of NIS. We believe that the UK's implementation, with its outcome focused approach, is flexible enough to manage these differences. The UK has the opportunity to determine which options are best suited to its national objectives. This includes choosing whether or not to align with the EU where this is in our national interest. . We will continue to monitor the impact of changes proposed under the European Commission's new NIS Directive carefully.

10) What are the areas for improvement?

The Government took action to address the challenges identified in the 2020 Post-Implementation Review (through secondary legislation in 2020), and a detailed account of these changes has been added in Section 2 of this document. That legislation, aimed to deliver the recommendations of the previous Post-Implementation Review, as well as some other needed technical changes, came into force on 31st December 2020.

During this evaluation, and based on the chapters above, DCMS has identified a further seven areas of improvement for the NIS Regulations. These include some of the recommendations from the last Post-Implementation Review which could not be implemented through secondary legislation, due to limitations on what is and is not permissible through secondary legislation.

Below are the key areas for improvement that DCMS has identified.

1) Registration of relevant digital service providers and related guidance

For the purposes of the NIS Regulations, entities that provide an online marketplace, online search engine, or a cloud computing service (either alone or in combination) are relevant digital service providers.[123] As such, under Regulation 14[124] they are required to register with the Information and Commission Office so that the ICO can maintain a register of who they are regulating.[125] Guidance for registration is provided on the ICO's website.

More than half (54%) of the relevant digital service providers responding to the latest post-implementation review survey stated that it was not easy for them to identify that their organisations are in scope of the NIS Regulations.[126] This is in contrast with operators of essential services, the majority (85%) of which found it straightforward to understand that they were in scope of the NIS Regulations.[127]

If relevant digital service providers are unable to effectively identify themselves as being in scope of the NIS Regulations, they will not register with the Information Commissioner's Office and the ICO will not be aware of their activities. This leads to the ICO facing challenges to implement the NIS Regulations effectively, and unable to advise relevant organisations on the appropriate and proportionate measures necessary. In parallel, the entity may not realise they are bound by the provisions of the NIS Regulations, and that subsequent incidents may lead to enforcement action (albeit at too late a stage), leading to loss of security, potential impact on consumers and other businesses, and the wider economy.

2) Ensuring that the right organisations are in scope of the NIS Regulations

In the 2020 Post-Implementation Review, several competent authorities reported that the definitions and sub-sectors under the NIS Regulations were not sufficient. There were organisations within their sectors that provided essential services that were not being captured by the legislation and some that were captured but that were not essential. [128] As a result of this feedback, the instrument laid in November

[123] NIS Regulation (1(2)). Small or micro businesses are excluded.
[124] https://www.legislation.gov.uk/uksi/2018/506/regulation/14
[125] https://ico.org.uk/for-organisations/the-guide-to-nis/?template=pdf&patch=1
[126] Base: 13 RDSPs
[127] Base: 67 OESs.
[128] NIS Post Implementation Review 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960574/CCS207_CCS0320329850-001_Network_and_Information_Systems_Regulations_Post-Implementation_Review_Web_V2.pdf, p49.

2020 (which came into force on 31st December 2020) made important amendments to the schedules, to clarify certain definitions and ensure there is more clarity on which organisations are in scope.

However, this only partially resolved the issue as secondary legislation could only amend the numerical or quantitative thresholds, not create new ones or bring new sectors within scope of the Regulations. The feedback from this latest review has highlighted that some competent authorities still did not feel all the correct organisations were designated under the NIS Regulations and that the scope of NIS should be expanded to new organisation types to bolster their cyber resilience and protect essential services.

A key example is managed service providers, which have risen in importance since 2018, and Integrated Health Care Boards which have been brought into NIS by the Department of Health and Social Care (through separate primary legislation). It is clear from these that there is a need for a formal mechanism to assess, consult and decide on whether new sectors should be included within the scope of the NIS Regulations.

To address this, it is important that there are provisions laid out in the Regulations that allow for more flexibility in regards to what sectors and sub-sectors are covered by the NIS Regulations. The consultation launched by DCMS on 19th January 2022 addresses this point, proposing amendments that would allow for NIS to be expanded or amended to cover different areas of the economy. Such changes would be driven by necessity and based upon evidence, in order to ensure that the regulations remain appropriate and proportionate to the risk.

3) Supply chains

As highlighted in the 2021 Supply Chain Security Call for Views, cyber risks permeate throughout supply chains. An incident or attack damaging an insecure third party supplier could travel through to its operator of essential service and relevant digital service provider clients. At present, the NIS Regulations only apply to organisations directly providing an essential service. Some of these operators might rely on other supporting services, in order to deliver their essential service.

Risks around the supply chain have previously been flagged previously as an area of concern. In the original impact assessment for the NIS Regulations, published in 2018, essential service providers identified third party suppliers as a contributing factor to some breaches or attacks. This was also identified later on in the 2020 Post-Implementation Review as an area of improvement. More detailed information on the government's work to tackle this issue can be found in the section concerning amendments to the NIS Regulations since the last Post-Implementation Review above. Although efforts in this direction have been made, supply chain risk has persisted as an issue since the 2020, and emerged again in the findings of the current review.

Only 9% of operators of essential services indicated having the resources to manage the risk from their direct suppliers and their wider supply chain.[129] This represented a considerable decrease (-53% since the last Post-Implementation Review) from the proportion of respondents who indicated having these resources in the 2020 NIS Post-Implementation Review. It is important to note, however, that the fall in this confidence might be due to an increased level of awareness of the complexities of supply chain security, rather than significantly lower resources being available. These differences could simply be down to the change in sample. Nonetheless, it is evident that steps should be taken to increase the ability of operators to manage the security risks arising from their supply chains.

Considerations of potential steps the government and the wider regulatory community may take to address this issue is considered in the section below, under ‘Next steps’

[129] Base: 68 OESs.

4) Capability and capacity of operators and competent authorities

Competent authorities, as well as operators of essential services and relevant digital service providers, have reported that they are facing challenges in regards to their capacity and resources. 42% of all operators of essential services indicated that they do not have the necessary skills and capacity to fulfil their obligations. They also noted that they felt that they do not have the in-house skills and capacity to achieve this.

The key challenges they identified as to their organisations ability to implement the regulations was a lack of finance/funding or a lack of general resources with 35% indicating both categories.[130] In comparison to operators of essential services, relatively fewer relevant digital service providers (21% of total respondents) reported not having the skills and capacity to deliver their obligations under the NIS Regulations. However, similarly to operators of essential services, the challenges they faced when implementing the NIS Regulations were a lack of finance/funding (50%) or a lack of resource (unspecified) (50%)[131]. While the survey did not go into further detail and explore the specific resources they are lacking, it is expected that the resource constraints in this section mean both staff and access to the right level of expertise.

On the regulator side, capacity constraints vary by sector with some lacking more resources than others. In total 5 competent authorities highlighted that they do not have the right tools to implement the NIS Regulations. The main challenges highlighted fall into 2 categories: lack of capacity and capability (staff and training); and limited powers under the current legal framework. Capacity and capability challenges vary across sectors. Different competent authorities highlighted different challenges: a lack of skills and experience to undertake the CAF framework across their sector, difficulties in attracting and retaining sector-specific security skills. Another highlight is a lack of cyber regulator specific training or centralised NIS training in the same way there is GDPR training.

5) Incident reporting

The current legislation does not capture the right type or nature of incidents to achieve the aim of the policy. Changes are needed to obtain the level of incident data required.

Incident reporting is an important process to aid regulators in assessing both the level of threat faced by regulated organisations and their ability to defend and protect themselves. The NIS Regulations outline the requirements for regulated entities to notify their competent authority of an incident as well as the base criteria that an incident must meet in order to be reportable and the relevant factors to consider when determining whether this criteria has been met. The specific parameters for determining whether an incident is reportable by operators of essential services and relevant digital service providers[132] are set out in each sector's competent authority's guidance.

This review has identified two primary challenges with the present incident reporting framework: (1) incident reporting thresholds are too high, and (2) the base criteria of a reportable incident in the legislation is too narrow in scope to capture the most high risk incidents risks.

(1)The current incident reporting thresholds are currently set in statutory guidance. Competent authorities develop such thresholds in cooperation with the regulated entities, following the guidance and principles set out in legislation, and they set out what would qualify as a reportable incident. However, the system does not appear to be working. As of this review, competent authorities have received

[130] Base: 54 OESs
[131] Base: 2 RDSPs
[132] since SI of 2021

little-to-no reports, despite other sources of information, such as the Breaches Survey, indicating a prevalence of incidents within the wider economy and society.

(2) Under the current legislation, an incident is reportable if it results in an actual and material disruption to the service. However, an incident that has a material impact on the networks and information systems of an organisation, but which nonetheless does not disrupt the relevant digital or essential service, would not need to be reported. This leads to an underreporting of incidents and does not take into account the wider resilience of the organisation, the potential for follow-up attacks, and the need for the regulator to share vital information to protect other organisations that were not yet targeted.

The key policy objective of the NIS Regulations is to prevent (where possible) and improve the level of protection against incidents affecting the NIS systems of essential services, which if disrupted, could potentially cause significant disruption to the UK economy, society and individuals' welfare. This objective cannot be achieved if incidents incurred by regulated bodies are not being reported to regulators, who as a result will not have the information to assess and improve the security of the victim organisation, and prevent incidents from reoccurring on the long-term.

6) Enforcement

As outlined in the section concerning Amendments to the NIS Regulations since the last Post-Implementation Review, changes were made in 2020 to regulatory authorities' enforcement powers, information-sharing thresholds, as well as the penalty regime. Despite these efforts to make the enforcement framework more robust, evidence from the present Post-Implementation Review process points to the limited use of enforcement tools (information, enforcement, or penalty notices) by regulators. This is not necessarily a drawback of the Regulations themselves, and the policy and legislative framework of the NIS Regulations is predicated on a collaborative relationship between regulators and regulated entities. Formalised enforcement tools should only be used as a last resort after engagement is no longer fruitful. However, there is evidence from competent authorities to suggest that there are cases where enforcement activities were merited but no action was taken. The use of enforcement tools overall, is much lower than the reported need and so far competent authorities appear to have been less inclined to make use of their regulatory powers.

There is also a reported concern from regulators that the grounds for enforcement (either via enforcement notices or penalty notices) is not clear enough, leading to increased concern around how the competent authorities may respond within certain scenarios.

DCMS will consider this in greater depth in the next period, in order to reach a conclusion and rectify the underlying issue. The Review's findings show that concerns about penalties are prevalent, and often linked to the fact that an incident is already a fine in itself (as described in the case above). However, NIS competent authorities have levied no penalty notices since the regulations came into effect. They have additionally reported being very restrictive with their regulatory powers, relying more on regular engagements, inspections, and information notices rather than any binding provisions of the regulations, such as enforcement notices, civil proceedings, or penalty notices.

7) Increased cross-sector coordination

Competent authorities are responsible for reviewing the application of the NIS Regulations in their sector and assessing the compliance of operators to the requirements of the NIS framework Directive.[133] DCMS issued guidance to help guide competent authorities' implementation of the NIS Regulations.

[133] Guidance for Competent Authorities, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf, p,5.

DCMS guidance[134] encourages competent authorities to instruct regulated bodies to complete self assessments. Alternatively, competent authorities can conduct the assessment directly themselves.[135] The Cyber Assessment Framework is a cyber risk management tool for regulated bodies designed by the NCSC which allows competent authorities to set target levels of cyber security in their sectors, and to assess the level of cyber security in the entities that they regulate. Currently, 10 of the 12 NIS competent authorities rely on the Cyber Assessment Framework to achieve this, with the remaining two using other cyber risk assessment tools.

It has been noted, through this Post-Implementation Review, that the frequency of these assessments is not consistent across all sectors, leading to a lack of understanding of the wider cyber security landscape and creating challenges for certain organisations that operate across sectoral lines. This aspect, however, is reflective of a wider challenge within the NIS Regulations, linked to the high number of competent authorities and different approaches in sectoral implementation. Increased information-sharing, particularly in regards to aspects relating to cross-sectoral implementation is necessary, and more tailored NIS milestones are necessary. Such milestones would need to consider aspects such as frequency of the assessments, cross-sectoral impact of CAF assurance, as well as to evaluate the overall projected outcomes of making the UK a more cyber secure economy.

There is also a reported need for more centralised coordination of NIS efforts across sectors, alongside more tailored and detailed guidance to the competent authorities themselves, particularly in regards to key performance indicators, cross-sectoral impacts of NIS implementation, as well as more in-depth consideration of the strategic approach necessary to achieve the objectives set out by the NIS Framework, be them in supply chain security or in delivering against the National Cyber Strategy.

[134] Ibid., p.13.
[135]DHSC and Scottish Gov use CAF alternatives.

11) Next steps

Recommendation

While the NIS Regulations have positively impacted cyber resilience in the essential service sectors they apply to, the review findings confirm feedback about their limitations which may have reduced their effectiveness. It is therefore right that we look for areas where we can make improvements to the regulations (albeit noting that they have already been amended several times in the last 4 years - once substantively, three times to make rectifications arising from the UK's withdrawal from the EU, and once to correct some a drafting error). Some areas had been previously identified by DCMS for further improvements and DCMS has used the findings of this review to shape the government's legislative policy solutions, published on 19 January 2022, for public consultation.

1) More robust oversight

The primary area for development is the need for more authoritative oversight. DCMS has played a policy ownership role of the NIS Regulations since their inception, working with lead government departments and competent authorities to shape NIS Policy. One thing that appears common throughout the range of feedback in this review is the need for clear direction from DCMS and cross sector consistency on implementation. DCMS has done some of this, but it is clear that more needs to be done.

DCMS should set the tone by issuing revised and updated guidance to competent authorities, setting out the requirement for a common approach to assessment and performance indicators. DCMS should also explore ways to make such guidance more binding on authorities. DCMS should establish a process by which competent authorities report against performance indicators and are held accountable for their performance. Such indicators could be linked to the delivery of the National Cyber Strategy and its performance framework. This would help evaluate both the adoption of NIS measures within operators of essential services and relevant digital service providers as well as the performance of the competent authorities, taking into account the objectives of the National Cyber Strategy.

2) Improve the process for registering digital service providers

Registration of digital service providers cannot be left to digital service providers alone. The ICO and DCMS also need to increase their efforts to ensure that the right entities are registered. The Government will continue to support the ICO in the work it is already carrying out to identify firms that should be under the Regulations and support them in notifying those organisations of their responsibilities. Both the government and the Information Commissioner, should consider ways to increase awareness of the NIS Regulations with all potential digital service providers.

The government should consider options to provide the Information Commissioner with increased information-seeking powers (similar to existing ones available to competent authorities of operators of essential services) to ascertain whether an organisation qualifies as a relevant digital service provider and thus be subject to the NIS Regulations.

3) Ensuring that the right organisations are in scope of the NIS Regulations

As set out above, the department has launched a consultation on new delegated powers which would allow the government to make changes to the scope of the NIS Regulations, either by amending the types of sectors and sub-sectors or by adding, removing, or amending the types of organisations that would fall within those sectors. These powers would allow for the Regulations to be amended in the future and allow the UK to adapt its legislative environment to future threats.

To begin with, initial assessments have identified managed service providers, as part of the digital services providers section, as the priority new sector that should be considered for adding to the scope of the NIS Regulations. This is also part of the same consultation. While this Post-Implementation Review has not identified any other sectors that need to be included at this time, it has underlined a need for the government to maintain the powers to make such additions in the future.

4) Supply chain security

The main reason that operators of essential services gave for not being able to monitor their supply chains was a lack of cooperation with the suppliers and then a lack of resources. Reports received indicate that operators of essential services in particular are facing challenges when attempting to impose certain requirements within their wider supply chains, and regulators are unable to support such efforts as these organisations do not fall within the scope of the NIS Regulations. DCMS, through the January 2022 consultation, has put forward two proposals to resolve part of this issue.

Firstly, the proposal to create a power to designate critical dependencies seeks to identify, impose duties, and then regulate certain supply chain organisations that present systemic risks to operators of essential services, either due to their market concentration, reliance on those services, or other factors. Such an organisation would then fall within the scope of the NIS Regulations and thus a competent authority can impose requirements to ensure the security of their networks and information systems. The banking and financial services sector, which is outside of scope of the NIS Regulations, is developing a framework to designate certain third party service providers to financial institutions as ‘critical’ and enhance direct, regulatory oversight of any services they provide to financial institutions which, If disrupted, could have a systemic impact on the financial regulators’ objectives. This may create opportunities for cooperation between competent authorities and sectoral regulators outside the NIS framework.

Secondly, the proposal to include managed service providers, which often play a critical role in the supply chains of essential services, under NIS will reduce the risk of disruption to essential services who rely on managed services to operate."

However, these measures are meant to resolve only the most significant and widespread vulnerabilities in supply chains, especially those that are shared by multiple organisations. It is not a holistic response to the supply chain challenges set out here.

In addition to the direct amendment of the NIS Regulations to address on an individual basis the most critical of third party suppliers, efforts need to be made to diminish the overall level of risk posed by supply chain providers beyond the scope of NIS across the wider economy. As such additional levers are being explored. DCMS will consider options such as amending guidance to tackle supply chain security concerns, including the prospect of using standards and certification, such as Cyber Essentials and Cyber Essentials +, to address this issue. Regardless of the solution, a long-term approach requires cross-government consideration in order to be effective and such a proposal cannot be put forward by a Post-Implementation Review of the NIS Regulations.

5) Competent Authority capability and capacity

Improving the capacity and capability of competent authorities is necessary to ensure an effective implementation of the regulations; however, tackling the capability and skills shortage across the economy will require a government-wide response and will come with challenges. DCMS does not control the budgets for the various competent authorities.

For those regulators that are government departments, DCMS will commit to persuading those departments to ensure that they meet their legal obligations to fund their NIS oversight. For these, plus those regulators that are not central government departments, DCMS aims to ensure that competent authorities are able to recover the costs of regulation from those being regulated, in line with government policy. Under the current regulations, competent authorities can charge a good portion of their NIS implementation costs back to the firms that they regulate. Under DCMS's new proposals, launched as part of our public consultation in January, the measure to expand the cost recovery of NIS enforcement actions should help resolve in part some resourcing issues faced by NIS Regulators.

Some additional ways to improve resource-efficiency will be considered, such as promoting collaboration across authorities and with authorities outside of NIS. For instance, collaborating with banking and financial services regulators for the designation of critical dependencies. Existing frameworks, such as CBEST and TBEST should be explored to test assumptions and highlight areas for further development.

6) Incident reporting

As mentioned earlier, the review has identified two primary challenges with the present incident reporting framework: (1) incident reporting thresholds are too high, and (2) the definition of a reportable incident in the legislation is too narrow in scope to capture all the most high risk incidents.

(1) Bringing incident reporting thresholds to an appropriate level: As set out in this review, there is an underreporting of incidents affecting the wider economy under the NIS Regulations. Competent authorities are able to update the incident reporting thresholds by issuing new statutory guidance. In order to address the lack of incident reporting, the thresholds should be reviewed by all competent authorities and lowered, if necessary, so that incidents that affect the service provided by operators in scope are notified.Any changes should be discussed with their sectors to ensure that it is understandable, achievable, and deliverable. This change would not need a legislative amendment.

(2) Amending the definition of a reportable incident in the legislation. In order to ensure that the relevant incidents are reported the definition of what constitutes a reportable incident needs to be changed.

DCMS, through its 2022 consultation on improving the UK's cyber resilience, has proposed measures to change the incident reporting framework to require operators of essential services and relevant digital service providers to report all incidents that have a material impact on the confidentiality, integrity, and availability of those networks and information systems, and that have a potential impact on the continuity of the service. This should bring defining incidents into a context that is more readily understood by industry, through reference to the widely known Confidentiality, Integrity and Availability triad. Through this measure, the department believes that regulators will receive better information on high risk incidents, leading to a more effective implementation of the NIS Regulations and, by extension, increasing the cyber resilience of the UK.

Annexes

Annex A: Relevant digital service providers survey

Privacy notice

Department for Digital, Culture, Media & Sport Privacy Notice [for Network and Information Systems (NIS) Regulations: Post Implementation Review 2022]

Who is collecting my data?

The Department for Digital, Culture, Media & Sport (DCMS) helps to drive growth, enrich lives and promote Britain abroad.

We protect and promote our cultural and artistic heritage and help businesses and communities to grow by investing in innovation and highlighting Britain as a fantastic place to visit. We help to give the UK a unique advantage on the global stage, striving for economic success.

Purpose of this Privacy Notice

This notice is provided within the context of the changes required by the Article 13 & 14 of UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This notice sets out how we will use your personal data as part of our legal obligations with regard to Data Protection.

DCMS' personal information charter (opens in a new tab) explains how we deal with your information. It also explains how you can ask to view, change or remove your information from our records.

What is personal data?

Personal data is any information relating to an identified or identifiable natural living person, otherwise known as a 'data subject'. A data subject is someone who can be recognised, directly or indirectly, by information such as a name, an identification number, location data, an online identifier, or data relating to their physical, physiological, genetic, mental, economic, cultural, or social identity. These types of identifying information are known as 'personal data'. Data protection law applies to the processing of personal data, including its collection, use and storage.

What personal data do we collect?

Most of the personal information we collect and process is provided to us directly by you. This includes:

- Any personal identifiers, such as region or sector that are included in your responses to open questions. As the number of operator of essential services (operator of essential services) in some areas is small, this may lead to your organisation being identifiable
- Information on the use of the survey website. This includes IP address and analytical cookies

How will we use your data?

We use personal information for a wide range of purposes, to enable us to carry out our functions as a government department. This includes:

Analysis of survey responses by all organisations that are covered by the NIS regulations. The collated results of the survey will be used in the post-implementation review which seeks to establish whether the regulations have achieved their original objectives and remain appropriate. The information you provide as part of this survey will inform future policy making with regard to the NIS Regulations.

What is the legal basis for processing my data?

To process this personal data, our legal reason for collecting or processing this data is: Article 6(1)

a. you have freely given your consent – it will be clear to you what you are consenting to and how you can withdraw your consent

The lawful basis that we rely on to process your personal data will determine which of the following rights are available to you. Much of the processing we do in DCMS will be necessary to meet our legal obligations or to perform a public task. If we hold personal data about you in different parts of DCMS for different purposes, then the legal basis we rely on in each competent authorities may not be the same.

What will happen if I do not provide this data?

You are not required to complete the survey or enter information which may result in you or your organisation becoming identifiable. 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.

Who will your data be shared with?

We may share this information with the National Cyber Security Centre and Competent Authorities.

If you write to us on a subject that is not our policy area, and the response needs to come from another government department, we will transfer your correspondence, including the personal data, to that department.

You can also ask us for details of any circumstances in which we can pass on your personal data without telling you. This might be, for example, to prevent and detect crime or to produce anonymised statistics.

We won’t make your personal data available for commercial use without your specific permission.

How long will my data be held for?

We will only retain your personal data for 2 years in line with DCMS retention policy:

- it is needed for the purposes set out in this document

Will my data be used for automated decision making or profiling?

We will not normally use your data for any automated decision making. If we need to do so, we will let you know.

Will my data be transferred outside the UK and if it is how will it be protected?

We will not usually send your data overseas. If we need to do so, we will let you know.

What are your data protection rights?

You have rights over your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (ICO) is the supervisory authority for data protection legislation, and maintains a full explanation of these rights on their website.

DCMS will ensure that we uphold your rights when processing your personal data.

How do I complain?

The contact details for the data controller's Data Protection Officer (DPO) are:

Data Protection Officer
The Department for Digital, Culture, Media & Sport
100 Parliament Street
London
SW1A 2BQ
Email: dpo@dcms.gov.uk

If you're unhappy with the way we have handled your personal data and want to make a complaint, please write to the department's Data Protection Officer or the Data Protection Manager at the relevant agency. You can contact the department's Data Protection Officer using the details above.

How to contact the Information Commissioner's Office

If you believe that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. You may also contact them to seek independent advice about data protection, privacy and data sharing.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: www.ico.org.uk

Telephone: 0303 123 1113

Email: casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

Changes to our privacy notice

We may make changes to this privacy policy. In that case, the 'last updated' date at the bottom of this page will also change. Any changes to this privacy policy will apply to you and your data immediately.

If these changes affect how your personal data is processed, DCMS will take reasonable steps to let you know.

This notice was last updated on 20/07/2021.

- I confirm that I have read and understood this statement

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. This is the second of such reviews and DCMS would like to thank all organisations that provided their expert reviews in the first post-implementation review. The responses from regulated organisations helped DCMS to develop policy positions and ensure that the regulations are both needed and if any refinements should be made. The full findings of the previous post-implementation review can be found published here. Insert as link [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960574/CCS207_CCS0320329850-001_Network_and_Information_Systems_Regulations_Post-Implementation_Review_Web_V2.pdf]

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 the 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 cyber team within 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, 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. The data collected from this survey will be shared with the Cabinet Office for the purposes of developing national cyber security policy. The data we share outside the DCMS cyber team will be aggregated, so it cannot be used to identify individual organisations.

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@dcms.gov.uk.

Please confirm below that you have read and understood this statement, about how your 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 the DCMS team responsible for this survey at nis@dcms.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 dpo@dcms.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@dcms.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
   - 2 or more of these services

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
   - 13-24 months
   - 25-36 months
   - Over 36 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? Please select all that apply
   - 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 Payment Card Industry Data Security Standards
   - 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 with other RDSPs
    - Provide more information onto the ICO or NCSC website
    - 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, our policies/processes already met the required standards set out in the NIS regulations
    - No change, please specify why……..

12. Have the NIS Regulations increased the prioritisation of security at a senior management level within your organisation?
    - Yes
    - No

13. Please explain your answer…

14. Do you feel that 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 that 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)?

    For the purpose of this survey, a supplier is an organisation that provides products, services or processes that, if affected, will result in disruption to the essential service(s) that you provide.

    - 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
    - No, our processes/procedures already met the required standards set out in the NIS Regulations
    - None of the above, please explain

Display q.22 only:

If Q21 = Introduced new processes/procedures

Or Q21 = Strengthened existing processes/procedures

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

23. With regard to incident response, have you taken action in any of the following areas as a result of the NIS regulations? 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 that 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…………………

<u>Lessons learned</u>

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, civil proceedings 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

Display q.34a if q.34a = over 200,000

34a. You selected that you plan to invest over £200,000 on Internal staff costs (including wages and training). Please specify how much this will be.

Display q.34b if q.34b = over 200,000

34b. You selected that you plan to invest over £200,000 on 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). Please specify how much this will be.

Display q.34c if q.34c = over 200,000

34c. You selected that you plan to invest over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this will be.

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 above)?
    - 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)? Please select all that apply:
    - 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…
    - None of these

41. As a result of the introduction of the NIS regulation, how much have you invested in additional security measures in the following areas relating to your network and information systems for your digital service(s) in the last 12 months?
    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

    Display q.41a if q.41a = over 200,000

41a. You selected that you plan to invest over £200,000 on Internal staff costs (including wages and training). Please specify how much this will be.

Display q.41b if q.41b = over 200,000

41b. You selected that you plan to invest over £200,000 on 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). Please specify how much this will be.

Display q.41c if q.41c = over 200,000

41c. You selected that you plan to invest over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this will be.

42. As a result of the introduction of the NIS regulation, how much do you plan to invest in additional security measures in the following areas relating to your network and information systems for your digital service(s) in the next 12 months?
    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

Display q.42a if q.42a = over 200,000

42a. You selected that you plan to invest over £200,000 on Internal staff costs (including wages and training). Please specify how much this will be.

Display q.42b if q.42b = over 200,000

42b. You selected that you plan to invest over £200,000 on 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). Please specify how much this will be.

Display q.42c if q.42c = over 200,000

42c. You selected that you plan to invest over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this will be.

43. 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

44. 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.45 if q.44 = yes

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

46. 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

Innovation

47. Do you feel that the NIS Regulations have impacted your organisation's ability to innovate?
    - Yes
    - No
    - Don't know

Display q.48 if q.47 = yes

48. How do you feel the regulations have impacted your organisation's innovation?
    - Large negative impact
    - Negative impact
    - Positive impact
    - Large positive impact

Display q.49 if q.47 = yes

49. Could you please explain your previous answer about the impact the regulations have had on your organisation's ability to innovate?

Member State Considerations

50. In addition to your operations in the UK, do you operate in any EU member states?
    - Yes
    - No
    - Don't know

51. 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.52 if q.51 = yes

52. Please explain your answer……….

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

Annex B: Operators of essential services survey

Privacy notice

Department for Digital, Culture, Media & Sport Privacy Notice [for Network and Information Systems (NIS) Regulations: Post Implementation Review 2022]

Who is collecting my data?

The Department for Digital, Culture, Media & Sport (DCMS) helps to drive growth, enrich lives and promote Britain abroad.

We protect and promote our cultural and artistic heritage and help businesses and communities to grow by investing in innovation and highlighting Britain as a fantastic place to visit. We help to give the UK a unique advantage on the global stage, striving for economic success.

Purpose of this Privacy Notice

This notice is provided within the context of the changes required by the Article 13 & 14 of UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This notice sets out how we will use your personal data as part of our legal obligations with regard to Data Protection.

DCMS' personal information charter (opens in a new tab) explains how we deal with your information. It also explains how you can ask to view, change or remove your information from our records.

What is personal data?

Personal data is any information relating to an identified or identifiable natural living person, otherwise known as a 'data subject'. A data subject is someone who can be recognised, directly or indirectly, by information such as a name, an identification number, location data, an online identifier, or data relating to their physical, physiological, genetic, mental, economic, cultural, or social identity. These types of identifying information are known as 'personal data'. Data protection law applies to the processing of personal data, including its collection, use and storage.

What personal data do we collect?

Most of the personal information we collect and process is provided to us directly by you. This includes:

- Any personal identifiers, such as region or sector that are included in your responses to open questions. As the number of operator of essential services (OESs) in some areas is small, this may lead to your organisation being identifiable
- Information on the use of the survey website. This includes IP address and analytical cookies

How will we use your data?

We use personal information for a wide range of purposes, to enable us to carry out our functions as a government department. This includes:

Analysis of survey responses by all organisations that are covered by the NIS regulations. The collated results of the survey will be used in the post-implementation review which seeks to establish whether the regulations have achieved their original objectives and remain appropriate. The information you provide as part of this survey will inform future policy making with regard to the NIS Regulations.

What is the legal basis for processing my data?

To process this personal data, our legal reason for collecting or processing this data is: Article 6(1)

a. you have freely given your consent – it will be clear to you what you are consenting to and how you can withdraw your consent

The lawful basis that we rely on to process your personal data will determine which of the following rights are available to you. Much of the processing we do in DCMS will be necessary to meet our legal obligations or to perform a public task. If we hold personal data about you in different parts of DCMS for different purposes, then the legal basis we rely on in each case may not be the same

What will happen if I do not provide this data?

You are not required to complete the survey or enter information which may result in you or your organisation becoming identifiable. 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.

Who will your data be shared with?

We may share this information with the National Cyber Security Centre and Competent Authorities.

If you write to us on a subject that is not our policy area, and the response needs to come from another government department, we will transfer your correspondence, including the personal data, to that department.

You can also ask us for details of any circumstances in which we can pass on your personal data without telling you. This might be, for example, to prevent and detect crime or to produce anonymised statistics.

We won’t make your personal data available for commercial use without your specific permission.

How long will my data be held for?

We will only retain your personal data for 2 years in line with DCMS retention policy:

- it is needed for the purposes set out in this document

Will my data be used for automated decision making or profiling?

We will not normally use your data for any automated decision making. If we need to do so, we will let you know.

Will my data be transferred outside the UK and if it is how will it be protected?

We will not usually send your data overseas. If we need to do so, we will let you know

What are your data protection rights?

You have rights over your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (ICO) is the supervisory authority for data protection legislation, and maintains a full explanation of these rights on their website

DCMS will ensure that we uphold your rights when processing your personal data.

How do I complain?

The contact details for the data controller's Data Protection Officer (DPO) are:

Data Protection Officer
The Department for Digital, Culture, Media & Sport
100 Parliament Street
London
SW1A 2BQ
Email: dpo@dcms.gov.uk

If you're unhappy with the way we have handled your personal data and want to make a complaint, please write to the department's Data Protection Officer or the Data Protection Manager at the relevant agency. You can contact the department's Data Protection Officer using the details above.

How to contact the Information Commissioner's Office

If you believe that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. You may also contact them to seek independent advice about data protection, privacy and data sharing.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: www.ico.org.uk
Telephone: 0303 123 1113
Email: casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

Changes to our privacy notice

We may make changes to this privacy policy. In that case, the 'last updated' date at the bottom of this page will also change. Any changes to this privacy policy will apply to you and your data immediately.

If these changes affect how your personal data is processed, DCMS will take reasonable steps to let you know.

This notice was last updated on 20/07/2021.

- I confirm that I have read and understood this statement

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 operator 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. This is the second of such reviews and DCMS would like to thank all organisations that provided their expert reviews in the first post-implementation review. The responses from regulated organisations helped DCMS to develop policy positions and ensure that the regulations are both needed and if any refinements should be made. The full findings of the previous post-implementation review can be found published here.

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 the 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 cyber team within 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, 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. The data collected from this survey will be shared with the Cabinet Office, for the purposes of developing national cyber security policy. The data we share outside the DCMS Cyber Team will be aggregated, so it cannot be used to identify individual organisations.

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 five 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@dcms.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 the DCMS team responsible for this survey at nis@dcms.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 dpo@dcms.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@dcms.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 demographics

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

    Display q.2 if q.1 = Energy
    Display q.3 if q.1 = Transport

2. In which energy subsector do you provide your essential services?
    - Electricity
    - Gas
    - Oil

3. In which transport subsector do you provide your essential services?
    - Air
    - Maritime
    - Rail
    - Road

4. Are you a parent company?
    - Yes
    - No

    Display q.5 if q.4 = Yes

5. What size* is your organisation? Please answer this for the group to which your organisation is a part of.
    - Small (≤50 employees)
    - Medium (51-250 employees)
    - Large (>250 employees)

    Display q.6 if q.4 = No

6. What size* is your organisation?
    - Small (≤50 employees)
    - Medium (51-250 employees)
    - Large (>250 employees)

7. 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
    - Department for Finance (Northern Ireland)
    - Scottish Government
    - Welsh Government
    - Don't know

8. 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 to 25
    - 26 to 30
    - 31 to 50
    - 51+
    - Don't know

9. How long has your organisation been designated as an OES?
    - Less than 6 months
    - 6-12 months
    - 13-24 months
    - 25-36 months
    - Over 36 months
    - Don't know

Impact of the NIS Regulations

10. 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(s)?
    - Yes
    - No
    - Don't know

11. 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? Please select all that apply
    - 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 General Data Protection Regulation (GDPR)
    - To comply with other non-NIS Regulations (excluding GDPR), please specify ____
    - To comply with other industry initiatives
    - Other, please specify ____
    - Don’t know

Guidance

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

Display q.13 if q.12 = Yes

13. Is this guidance easy to access?
    - Yes
    - No, please explain

14. Have you received adequate guidance and support from your Competent Authority to implement the NIS Regulations effectively?
    - Yes
    - No, please explain ____

15. 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
    - Information exchanges with other operator of essential services
    - Improve the educational materials available online
    - Other, please specify ____

Security Risk Management

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

17. 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, our policies/processes already met the required standards set out in the NIS Regulations
    - No change, please specify why

      ____

18. Have the NIS Regulations increased the prioritisation of security of network and information systems at a senior management level within your organisation?
    - Yes
    - No

19. Please explain your answer

____

20. Do you feel there are any challenges to your organisation’s ability to implement the NIS Regulations?
    - Yes, please explain what these are

      ____
    - No

Skills

21. 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

22. 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

23. 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

24. Are there any barriers that prevent you from conducting appropriate and proportionate risk management of your suppliers and your wider supply chain e.g. supplier’s suppliers?

    For the purpose of this survey, a supplier is an organisation that provides products, services or processes that, if affected, will result in disruption to the essential service(s) that you provide.
    - Yes
    - No

    If yes, please explain why.

    ____

25. Do you feel you have the capacity to manage cyber security risks of your network and information systems arising from your suppliers and your wider supply chain e.g. your 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 of 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

26. 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 provision of your essential service?
    - Yes
    - No
    - Don't know

27. 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
    - No, our processes/procedures already met the required standards set out in the NIS Regulations
    - None of the above, please explain
      ____

28. 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 resources required to enact your incident response plan
    - Carry out regular exercises to test your incident response plan
    - Carry out continuity planning for an incident response
    - No action taken
    - Other, please specify ____

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

30. Is the current deadline of 72 hours from discovery of an incident which meets the reporting threshold sufficient time to report to your Competent Authority?
    - Yes
    - No, please explain ____
    - Don't know

31. Do you think the incident identification thresholds for reporting NIS incidents are appropriate for your sector?
    - Yes
    - No, please explain ____
    - Don't know

32. Since the implementation of the NIS Regulations, how has your attitude towards voluntarily reporting of an incident that is under the reporting threshold changed to:

	More likely to voluntarily report	Less likely to voluntarily report	Stayed the same	Do not have a voluntary reporting process
Your Competent Authority)	●	●	●	●
Your lead Government Department	●	●	●	●
NCSC	●	●	●	●

33. Please explain your answer

____

Lessons Learned

34. The operators of essential services that are in scope of the NIS Regulations are those that meet the designation thresholds set out in Schedule 2 of the regulations. Did your organisation understand which designation thresholds apply to you?
    - Yes
    - No, please explain
    - Don't know

35. To what extent has applying the NCSC CAF principles and guidance impacted positively on the following with regard to the provision of your essential services 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

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

Display q.37 if q.36 = Yes

37. 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.38 if q.36 = Yes

38. How could the Cyber Assessment Framework be improved?

    ____

Enforcement Regime

39. Are you aware that there is an enforcement regime associated with the NIS Regulations?

- Yes
- No

Display q.40 if q.39 = Yes

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

Display q.41 if q.39 = Yes

41. 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, please explain ____

Costs and Benefits

42. 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 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

Display q.42a if q.42a = Over £200,000

42a. You selected that you invested over £200,000 on Internal staff costs (including wages and training). Please specify how much this was.

Display q.42b if q.42b = Over £200,000

42b. You selected that you invested over £200,000 on 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). Please specify how much this was.

Display q.42c if q.42c = Over £200,000

42c. You selected that you invested over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this was.

43. 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

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

45. 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.46 if q.45 = no

46. If no, please clarify number of hours **annually**, 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			

47. 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

48. 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)? Please select all that apply:
    - Internal staff costs (including wage 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

49. How much have you invested in the last 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)?
    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

    Display q.49a if q.49a = over £200,000

49a. You selected that you have invested over £200,000 on Internal staff costs (including wages and training). Please specify how much this will be.

Display q.49b if q.49b = over £200,000

49b. You selected that you have invested over £200,000 on 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). Please specify how much this will be.

Display q.49c if q.49c = over 200,000

49c. You selected that you have invested over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this will be.

50. How much 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)?
    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

Display q.50a if q.49a = over £200,000

50a. You selected that you plan to invest over £200,000 on Internal staff costs (including wages and training). Please specify how much this will be.

Display q.50b if q.49b = over £200,000

50b. You selected that you plan to invest over £200,000 on 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). Please specify how much this will be.

Display q.50c if q.50c = over 200,000

50c. You selected that you plan to invest over £200,000 on External costs (including outsourcing the management of cyber security, hiring external consultants and/or expertise). Please specify how much this will be.

51. 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.52 if q.51 = Yes

52. If yes, can you quantify these costs? ____

53. 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 cyber security
    - Sharing good practice with other OESs
    - Other, please specify ____
    - No unexpected benefits
    - Don't know

Innovation

54. Have the NIS Regulations impacted your organisation's ability to innovate?
    - Yes
    - No
    - Don't know

Display q.55 if q.54 = Yes

55. How do you feel the NIS Regulations have impacted your organisation's innovation?
    - Large negative impact
    - Slight negative impact
    - Slight positive impact
    - Large positive impact

Display q.56 if q.54 = Yes

56. Could you please explain your previous answer about the impact the regulations have had on your organisation's ability to innovate?

Member state considerations

57. In addition to your operations in the UK, do you operate in any EU member states?
    - Yes
    - No
    - Don't know

Display q.58 if q.57 = Yes

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

Display q.59 if q.58 = Yes

59. Please explain your answer……….

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

Annex C: Competent Authority Report

Purpose of the report

DCMS would firstly like to thank you for taking part in the first Post-Implementation Review of NIS Regulations, your responses helped identify policy positions on cost recovery, the appeals mechanisms and incident thresholds, to name a few. As the legislation had only been in force for 2 years at the last review, the costs and benefits of the legislation hadn't been fully realised. To ensure DCMS fully identifies and understands the impacts of the legislation, DCMS committed to running a second review 2 years after the first review. This is why, once again, DCMS is seeking out your expert opinion on the NIS Regulations to help shape future policy positions.

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.

The questionnaire results may be shared with the Cabinet Office and National Cyber Security Centre for the purposes of development of the National Cyber Strategy (the NIS national strategy under Regulation 2) and accompanying internal Spending Review investment case.

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 report 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

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

How many small businesses* do you have in scope of NIS in your sector / region?

* Table 1 below defines the parameters used in this assessment to define business size. An organisation needs to match 2 of the criteria to be considered a certain sized organisation.

Table 1: Organisation size parameters

Organisation size	Employees	Aggregate turnover (net / gross)	Aggregate balance sheet total (net / gross)
Small	≤50 employees	<£10.2m/£12.2m	<£5.1m/£6.1m
Medium	≤250 employees	<£36m/£43.2m	<£18m/£21.6m
Large	>250 employees	>£36m/£43.2m	>£18m/£21.6m

13. IF MORE THAN 0, have you observed a cost impact on small businesses you regulate due to NIS?

- Yes
- No

If YES, please give further details here:

14. IF YES, do you think the costs incurred by these small businesses have a disproportionately larger impact than the larger organisations you regulate?
    - Yes
    - No

If YES, please give further details here:

15. 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 with EU member states
    - 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
    - A greater understanding of the level of cybersecurity across the sector/region
    - An ability to intervene where this is in the national interest
    - A common framework/standard to assess cybersecurity
    - Other (please specify in the box below)

OTHER: Please give further details here.

16. 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.

17. 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:

18. 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:

Assessment of organisations' compliance

19. How many assessments of the security of network and information systems have been carried out in your sector since 2018, indicating how many are self assessments and how many are independently verified?

Please give further details here:

20. How many operators are assessed as meeting the assessment baseline (i.e. CAF basic profile or similar)?

Please give further details here:

21. How many operators have improvement plans in place under the assessment framework (CAF or similar)?

Please give further details here:

22. What is your assessment of overall compliance of your sector against the requirements set by the NIS Regulations?

Please give further details here:

23. How many Information Notices have you used, and why?

Please give further details here:

24. How many Enforcement Notices have you used, and why?

Please give further details here:

25. How many Appeals have you received?

Please give further details here:

26. How many Penalty Notices have you used, and why?

Please give further details here:

Specific policy questions

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

If NO, please give further details here:

28. 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:

29. 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:

30. What are your views on the current **incident reporting** thresholds for your sector / region?

Please give further details here:

31. 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:

32. Do you believe that the regulations adequately offer information-sharing provisions to allow effective domestic collaboration with other relevant authorities? (For example, DCMS, NCSC, the Cabinet Office and other government departments)

- Yes
- No

If NO, please give further details here:

Capacity & capability

33. 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:

34. What areas do you think you are most effective as a CA as applying the regulations?

Please explain here:

35. In which areas of applying the regulations are you seeking to build future capability?

Please explain here:

36. 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:

37. 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.

38. What are your views on the current support provided by the NCSC as the Computer Security Incident Response Team? And what more could they do to support you?

Please give further details here.

39. 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.

Innovation

40. Do you feel that the NIS regulations have impacted your sector's ability to innovate?
    - Yes
    - No
    - Don't know

Display q.37 if q.36 = yes

41. How do you feel the regulations have impacted your sector's innovation?
    - Large negative impact
    - Negative impact
    - Positive impact
    - Large positive impact

Display q.38 if q.36 = yes

42. Could you please explain your previous answer about the impact the regulations have had on your sector's ability to innovate?

Annex D: Assumptions

Assumption	Additional information
General assumptions	
The appraisal length is consistent with the NIS Impact Assessment and therefore 10 years	
The standard discount rate of 3.5% will be used for the economic appraisal.	
The PV base year will be 2018 following the NIS Impact Assessment	

The price base year will be 2016 following the NIS Impact Assessment, and prices were deflated using OBR GDP Deflators.	
Overhead charges of 30% were added to the wages, in accordance with the International Standard Cost Model Manual.	
There were an estimated total of 129 RDSPs in the 2020 NIS PIR	We have estimated the number of OESs and RDSPs in scope of the NIS regulations based on evidence provided by Competent Authorities (CAs). Where a CA did not provide this figure, the designated number of organisations was taken from NCSC figures (2020). 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.
There were an estimated total of 481 OESs in the 2020 NIS PIR	
This Review estimated a total of 169 RDSPs	
This Review estimated a total of 436 OESs	
This Review estimated a total of 253 public organisations regulated under NIS	Taken from CA returns, where a CA did not provide feedback we take the number of organisations designated that was reported in the 2020 NIS PIR
This Review estimated that a total of 42.52% are public organisations	
The compound annual growth rate (CAGR) in median wages for different occupations has been estimated by taking the average of the difference between 2013 and 2021 ASHE wage data	
Familiarisation costs	
The number of hours for familiarising with legislation and for guidance documents is taken from the NIS Impact Assessment Estimations	
We assume that all organisations faced familiarisation costs	
We take the number of organisations that faced familiarisation costs from the 2020 NIS PIR as this cost was incurred closer to that period	
We assume that familiarisation costs are a one-off implementation cost	
Security costs	
Based on the findings we update the assumption that physical security costs are a one-off for OESs as organisations indicated that they are still investing in this area. We did not update this assumption for RDSPs due to a lack of sufficient responses.	
External costs and physical security costs are assumed to be constant through the appraisal period	

Wage growth for internal staff costs over the appraisal period is taken from the ASHE for SIC Code 62, which is the computer programming, consultancy and related activities industry code	
In line with the last PIR we assume that the distribution of 'don't knows' is equal to those that did provide an estimate	
Responses of 'less than £5,000' are inputted as £4,999. Responses of 'over £200k' are inputted as £200,001	
Additional compliance costs	
As initial evidence suggests that additional compliance costs exceeded those estimated in the NIS 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 NIS Impact Assessment.	
Only essential service providers will be required to provide evidence in this way to competent authorities.	
The time spent on incident notification, is taken from the NIS Impact Assessment estimations	
Following NCSC's report of the number of incidents in the year to December 2019, we estimate a total of 13 incidents. We will assume a flat rate of incidents for future years. In the high case we have assumed the number of incidents will double.	
CA costs	
Sensitivity analysis has also been conducted to account for uncertainty in future costs by varying total costs by 20%	
In line with the 2020 NIS PIR we assume that CAs have not passed this cost onto they organisations that they regulate	
In line with the 2020 NIS PIR we do not incorporate wage inflation into the costs that CAs face	
In line with the 2020 NIS PIR it has 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.	
Costs incurred by Competent Authorities of regulating private sector organisations have been assumed to have been passed on to business	