Final stage impact assessment

Title:	Cyber Security and Resilience (Network and Information Systems) Bill
Type of measure:	Primary legislation
Department or agency:	Department for Science, Innovation and Technology
IA number:	DSIT002(FIA)-25-DTI
RPC reference number:	RPC-DSIT-25054-IA (1)
Contact for enquiries:	Kelly.North@dsit.gov.uk
Date:	12 November 2025

Table of Contents

1. Summary of proposal

The cyber threat has grown more intense, frequent and sophisticated, and the UK's businesses and vital public services are being increasingly targeted by hostile cyber actors. The government has been clear that it will take the decisions necessary to protect our national security, our economy and society from those who seek to do us harm. The Cyber Security and Resilience (Network and Information Systems) Bill ('the Bill') will strengthen the UK's cyber defences, safeguard our critical infrastructure and better protect more businesses than ever from costly cyber attacks in a way that does not overburden them.

The Bill will take proportionate steps to bolster UK cyber security legislation, aligning with international partners wherever possible. The Bill will update the Network and Information Systems Regulations 2018 (NIS Regulations), the UK's only cross sector cyber security legislation, which were transposed from European Union law under the European Communities Act 1972. The NIS Regulations cover essential services in five sectors (transport, energy, drinking water, health, and digital infrastructure) and some digital services (online marketplaces, online search engines, and cloud computing services). This means that not all sectors or services, such as retail, are in scope of the Regulations. Twelve regulators (called "competent authorities" in the regulations) are currently responsible for enforcing the regulations.

The cyber landscape is constantly evolving, with hostile actors changing tactics to circumvent protections. The NIS Regulations have not kept pace with the worsening cyber threat landscape, and the government does not currently have the necessary powers to update them responsively. Meanwhile the EU is updating its cyber regulations via the Network and Information Systems 2 Directive (NIS 2) and other countries (such as Australia) are updating their cyber security laws, meaning that the UK is falling behind its international partners. The Bill will address the specific cyber security challenges faced by the UK, while aligning, where appropriate, with the approach taken in the EU NIS 2 Directive (NIS 2). The Bill will bring the UK regulations up to date by bringing more entities into scope, equip regulators with proportionate powers to fulfil their duties and provide the government with sufficient powers to amend the NIS Regulations in the future.

The Bill will bring more types of services into scope of the NIS Regulations, enhancing the cyber resilience more services and closing the gaps that cyber criminals are currently exploiting.

- The Bill will bring relevant managed service providers (RMSPs – organisations which provide an ongoing managed IT service to another organisation)[1], data centres (the buildings which house and process much of the data generated in the UK - from photos taken on smartphones to patients' NHS records) and large load controllers (which ensure appliances continue to be powered with the electricity they need by responding to electricity usage signals) into scope of the NIS Regulations. These entities will be regulated by the Information Commissioner, Department for Science, Innovation and Technology (DSIT)/Ofcom (joint) and Ofgem respectively. By bringing these entities into scope, they will be required to take steps to manage their cyber risks and report incidents to regulators, better protecting them from the effects of cyber attacks and making them less attractive to malicious actors. In turn this will safeguard the services the public and businesses rely on to go about their lives.

[1] "Relevant managed service providers" or "RMSP" is used in this impact assessment to refer to the MSPs in scope of this measure.

- The Bill takes steps to strengthen vulnerabilities in the supply chains for operators of essential services (OESs) and relevant digital service providers (RDSPs). The Bill will enable regulators to designate "critical suppliers" to bring them in scope of the NIS Regulations – ensuring potential weak links are identified and reinforced. This will strengthen our essential services against cyber attacks on its critical suppliers, the effects of which are felt by the public using those services. The current blanket exemption for small and micro-enterprises (SMEs) will be amended, so that regulators can designate an SME as a "critical supplier" should it be necessary to safeguard a supply chain from the impacts of a cyber attack.

The Bill will deliver a stronger regulatory landscape by empowering regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties.

- The Bill will improve incident reporting by expanding the criteria to capture more forms of damaging cyber attacks, updating incident reporting times and streamlining reporting to regulators and the National Cyber Security Centre (NCSC), which responds to serious cyber incidents impacting the UK. This will empower regulators, the NCSC and government to better assess regulatory compliance and be alerted to unfolding incidents, enabling them to support organisations in responding to incidents. Over time, improved incident reporting will build a better picture of the cyber landscape and build defences against malicious actors.
- The Bill will also strengthen information sharing by ensuring that regulators are able to share information with public authorities and vice versa. This will enable government and regulators to plan efficiently and effectively against cyber threats.
- The Bill will extend existing powers to enable the Information Commission (formerly the Information Commissioner's Office, or ICO) to request information to proactively identify cyber risks in the digital services that they regulate.
- The Bill will better resource regulators to effectively drive and support compliance with cyber security requirements, by improving the cost recovery regime so that it is more comprehensive and flexible, reducing the need to pass the costs of regulation to the taxpayer.
- As the Bill expands the scope of NIS Regulations and enhances oversight, consistency across sectors becomes increasingly important. The Bill will enable the Secretary of State to designate a Statement of Strategic Priorities to establish a unified set of objectives for regulators to seek to achieve, and to set expectations for the implementation of the regulations.
- The Bill will improve the ability of regulators to enforce the NIS Regulations, leading to a more successful regime. The maximum fine will be amended - enabling potentially higher fines than currently possible, when appropriate - reflecting the significance of the regime. This has been developed taking into account comparable legislation. Further, the penalty bands will be simplified to make them fairer, clearer and more effective, and fuller case circumstances will be considered by regulators when determining a fine - including proportionality to the organisation, as well as patterns of non-compliance.

The Bill will strengthen the cyber security baseline for regulated entities, ensure that the NIS Regulations keep pace with the ever-changing cyber landscape and equip government to take decisive action to protect our national security.

- New technologies and emerging threats require agile regulations – it does not take long before they can fall out of date. The Bill will provide the Secretary of State with

proportionate powers to update the NIS Regulations via secondary legislation. This will ensure that the NIS Regulations can remain effective against the evolving cyber threats facing the UK now and in the future.

- The Bill will enable government to update and strengthen the existing security requirements for regulated entities and to bring them into closer alignment with NCSC recommendations and international best practice. The Bill will also enable the government to set stronger supply chain duties through secondary legislation to better protect public services from a disruption in their supply chain.
- Additionally, to protect against imminent threats, the Bill will give the Secretary of State the power to issue a direction to a regulator or regulated entity, where it is necessary and proportionate for national security. This will ensure that the government can respond swiftly to cyber threats which pose risks to our national security, protecting our interests and the safety of our citizens.

The majority of the Bill's measures were announced at the King's Speech 2024 and have therefore not been included in an options assessment. The measures new to the Bill are bringing data centres and large load controllers into scope, strengthening the NIS Regulation's enforcement mechanisms, and enabling the Secretary of State to designate a statement of strategic priorities and issue directions in the interest of national security. The government consulted on bringing data centres into scope last year, completing in February 2024[2], and there is ongoing engagement with sector, including the data infrastructure quarterly forum. The government consulted on requiring all organisations remotely controlling large amounts of electrical load (300MW in aggregate or more) to comply with the provisions of the NIS Regulations and to be deemed designated OESs in July 2022.[3] A second consultation in April 2024 built upon these proposals and set out principles for developing the large load controllers cyber security assurance framework.[4] Both consultations gathered support with ongoing engagement with the sector. For the measures to strengthen the enforcement mechanisms, this was an area that was identified as needing refinement in the NIS post-implementation review and we have developed the measures in close collaboration with regulators. With regards to the power to designate a statement of strategic priorities, the Bill specifies that the Secretary of State must consult with regulators and also receive Parliamentary approval before the statement of strategic priorities can be designated.

2. Strategic case for proposed regulation

There is a growing threat to our essential and digital services from malicious cyber actors. Cyber attacks are becoming more frequent and sophisticated, with criminals circumventing protections with new techniques and targeting our increasingly complex supply chains to find weak links. At the same time, more state-backed actors are targeting British businesses and services for espionage and extortion, threatening our national security and way of life. Meanwhile, the UK's only cross-sector cyber legislation, the NIS Regulations, have fallen out of date and are insufficient to tackle the cyber threats faced by the UK in 2025 and beyond. In the year preceding September 2025, NCSC managed 429 cyber incidents, 204 of which were nationally significant – meaning they had a substantial impact on national security, economic stability, or public safety. This is a sharp increase from the 89 nationally significant incidents the previous year.[5] Of these incidents, 18 were classified as "highly significant" in

[2] Consultation: Protecting and enhancing the security and resilience of UK data infrastructure
[3] Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control - GOV.UK
[4] Delivering a smart and secure electricity system: implementation - GOV.UK
[5] It's time to act - NCSC Annual Review 2025

nature, marking a 50% increase from the previous year. Ordinary people pay the price for these attacks, whether this be from disrupted public services or an unstable business environment which undermines economic growth.

Cyber incidents cost UK businesses billions annually, with recent cyber attacks severely disrupting organisations such as Jaguar Land Rover, Marks and Spencer, Royal Mail and the British Library. Between 2015 – 2019, UK businesses lost approximately £87 billion when factoring in damaged assets, financial penalties, and lost productivity.[6] Last year, 43% of businesses reported having experienced some kind of cyber security breach or attack in the last 12 months.[7] This equates to approximately 612,000 UK businesses.[8] Cyber attacks are costly to business and create a precarious environment in which to expand or grow. This instability damages the competitiveness of companies and hinders the UK's economic progress. Robust but proportionate cyber regulation is needed to create a stable and secure environment in which businesses can thrive. The cost of doing nothing is too great.

Our growing dependency on technology has made supply chains more vulnerable, with ransomware and data extortion emerging as significant threats. These vulnerabilities have caused real world impacts for UK citizens. In 2024, a ransomware attack on a key supplier to the NHS led to over 11,000 postponed acute outpatient appointments and elective procedures. The Bill's measures to regulate critical suppliers are targeted at only the most critical suppliers, seeking to counteract the growing threat of supply chain vulnerability without placing unnecessary burdens on businesses.

Our outdated regulations are also threatening the UK's national security. Attacks on our allies highlight the serious threat posed by state-sponsored actors targeting critical national infrastructure (CNI) —systems essential for public safety and the functioning of the country. These incidents underscore the urgent need for the UK to ensure its defences are modern, resilient, and fully equipped to meet evolving challenges. Chinese state sponsored threat actors have already targeted US critical sectors. For example, Volt Typhoon is a cyber threat acting on behalf of China and has targeted energy, transport and water sectors in the US and could be laying the groundwork for future disruptive and destructive cyber attacks. Additionally, Russia has launched destructive attacks against the Ukrainian government. For example, in February 2022, a cyber attack against Viasat, a US satellite communications company, began approximately one hour before Russia launched its further invasion of Ukraine. It was an attempt to cripple Ukrainian military operations and communications which spilled over into Europe affecting both organisations and citizens. This was followed by destructive and disruptive cyber attacks on Ukrainian CNI, telecoms providers, government entities and an attempted attack on power grids. The Bill will bolster the UK's resilience to threats like these in the long-term by strengthening the intelligence available to regulators and government and ensuring that government can respond swiftly to serious threats to our national security through the powers of direction.

We consider it necessary to legislate in this space rather than rely on non-legislative measures, as these have shown to be ineffective. The scale of the problem is too great and an updated regulatory framework, clearly laid out for businesses and regulators, will ensure that protections are implemented at pace and consistently. In the last 12 months, only 49% of businesses have carried out activities to identify cyber risks, despite 72% of businesses identifying cyber security as a high priority; and only 27% of businesses have Board level

[6] Beaming, 'Five Years in Cyber Security', 2020
[7] Cyber security breaches survey 2025 - GOV.UK
[8] *Ibid.*

representation with responsibility for cyber security.[9] This is despite the range of tools available to businesses to improve their cyber awareness and security, such as NCSC's Cyber Aware campaign, the 10 Steps guidance and Cyber Essentials. Only 12% of businesses and 15% of charities surveyed in the Cyber Security Breaches Survey 2025 were aware of the 10 Steps guidance or Cyber Essentials.[10] This demonstrates that guidance and voluntary measures alone will not be sufficient to secure our cyber landscape.

In addition, the 2022 Second Post-Implementation Review (PIR) of the NIS Regulations found that the regulations are not working as intended in several areas, such as incident reporting.[11] In 2019, 2020 and 2021, there were only 13, 12 and 22 NIS incidents reported, respectively.[12] This is because the definition of a significant incident is too narrow. The lack of reports being made is an issue highlighted by regulators, as several high-profile incidents are being reported in the press without crucial details about them being reported to the regulators.[13] This limits regulators' ability to use important intelligence to plan effectively, issue guidance and support entities to bolster their cyber resilience. This highlights the need for change to keep the NIS Regulations effective.

Without intervention, the UK's essential and digital services will continue to be vulnerable to cyber attacks, with real life impacts on the citizens and businesses that rely on them. The services that businesses and the public rely on every day should be subject to robust protections, like those already in place for other vital sectors, like telecommunications or finance. It is important that we learn from the successes of these regimes and carry these across to ensure the resilience of our essential and digital services. Additionally, without intervention, we would fall behind our international partners, such as the EU, which has already increased the number of organisations in scope of their regulations, and Australia which has updated its laws to allow designation of critical supply chains. Businesses could be discouraged from innovating and investing in technologies in the UK, which would impede on this government's growth objectives – we cannot have growth without stability.

Updating the regulatory framework can only be done through primary legislation. Following the UK's departure from the EU, the European Communities Act 1972 was repealed, and we no longer hold appropriate powers to update the framework without new primary legislation.

Table 3.2 lists the strategic case for change measure by measure.

3. SMART objectives for intervention

The Bill will make crucial updates to the NIS Regulations. These updates balance the essential need to strengthen the UK's cyber defences to protect essential and digital services and UK national security, whilst minimising costs to business in the immediate term. SMART objectives for each measure are set out in Table 3.2 but there are several overarching objectives behind strengthening the UK's cyber security and resilience.

Firstly, it is crucial to protect the services that people and businesses rely on so that they can get on with their day-to-day lives without interference. Cyber criminals are

[9] Cyber Security Breaches Survey 2025
[10] Ibid
[11] DSIT , Second PIR of the Network and Information Systems Regulations 2018 (2022)
[12] Ibid
[13] Sky News, 'Nine cyber attacks on UK's transport sector missed by mandatory reporting laws' (2021)

increasingly targeting digital and essential services and their supply chains, causing disruption to the lives of working people and businesses, with significant costs to government and the economy. Cyber criminals are increasingly attacking CNI, seeing essential services and their supply chains as lucrative targets. An independent report commissioned by Bridewell consulting found that 86% of the CNI they interviewed have detected a cyber attack on their systems in the past 12 months.[14] Of those 86%, 93% experienced at least one successful attack in the last 12 months.[15] An objective of the Bill is to tackle these vulnerabilities by bringing more entities into scope and empowering regulators to better fulfil their duties. In turn, this will disincentivise cyber attackers and minimise the impacts if organisations are targeted. The measurable objective here is to increase the number of entities regulated by NIS and therefore increase the number of organisations taking steps to assess and reduce their cyber security risks. In turn, this should result in a reduction in the impacts any cyber attacks can have on businesses, essential services and their end users.

Secondly, cyber security is a critical enabler of economic growth. We cannot have growth without stability. Cyber attacks are disruptive and costly to business, and where businesses are being targeted, we know that leaders may be hesitant to expand and innovate. By bringing more entities into scope and strengthening the baseline security requirements of digital services, the Bill seeks to reduce the likelihood and impacts of the cyber attacks that are so disruptive to businesses across the economy. This will in turn create a more secure and robust environment in which businesses can operate without fear of devastating cyber attacks, which is essential to economic growth. That is why a key objective of this Bill is to protect businesses from cyber attacks to foster an environment in which investment and innovation can thrive. Having better defences against cyber attacks, achieved by bringing more entities into scope and empowering regulators to better fulfil their duties, will reduce the time businesses must take to deal with cyber attacks, often halting their services to do so. When an attack does occur, improved incident reporting will allow regulators and NCSC to use this information to provide advice and guidance to, and to engage with, other businesses and organisations. This will enable them to take action to protect themselves and mitigate the wider impacts of the specific attack or type of attack. The measurable objectives here are to prevent more cyber attacks and, if an incident does occur, reduce the disruption, cost and down-time as businesses deal with them.

Thirdly, cyber security is essential to protecting the UK's national security. NCSC's Annual Review 2024 described the threat landscape as "diffuse and dangerous", with persistent attacks from hostile states and organised crime.[16] NCSC's Annual Review 2025 emphasised the intensified nature of this threat.[17] A key objective of the Bill is to ensure that government can act decisively against cyber threats through proportionate powers. Not only will it upgrade UK's cross cutting cyber security regulations but ensure that the framework is not stagnant in the future. The Bill will also ensure that unexpected and imminent threats to national security can be responded to appropriately through the power to direct regulators and regulated entities to take a specific action. The measurable objective is to create proportionate delegated powers that allow government to make changes via secondary legislation when needed, so that it is not beholden to the timescales of primary legislation in the future and ensure that it can respond to imminent cyber attacks where national security is threatened.

[14] CNI Cyber Report: Risk & Resilience, commissioned by Bridewell consulting.
[15] Ibid
[16] Annual Review 2024
[17] It's time to act - NCSC Annual Review 2025

Rationale for intervention

The current regulatory regime is out of date, leaving the UK's services and CNI vulnerable to cyber attacks, significantly impacting both individuals and businesses. There are five market failures across different sectors of the economy that have been identified as a result of the UK's current cyber security regime.

a. **Externalities** occur when the production or consumption of a good incurs costs or benefits on a third-party outside of the transaction. The benefits of cyber security are felt more widely than just the organisation implementing the security. This is because each cyber attack on an individual or organisation has impacts outside the costs to the victim, such as consumers, commercial clients, or third parties. For example, an attack that leaks user personal information negatively impacts users and the attacked organisation may not shoulder the full costs of restoring their networks but pass it on to their customers. Individuals and third-party entities are often forced to bear the cost from a cyber attack inflicted on any organisation.

b. **Public goods** are either under-provided by the market or not provided at all. Cyber security is a form of public good at times when it is:

- Non-excludable: the benefits of a secure digital infrastructure are not limited to individuals who directly contribute to its security. Everyone, including organisations and individuals, benefits from a more secure environment, regardless of their individual actions or financial contributions.
- Non-rivalrous: the use of secure digital infrastructure by one entity does not diminish its availability or quality for other entities. A secure network, for example, remains secure for all users, even if some users are not directly involved in maintaining its security.

c. **Information asymmetry** refers to when one party in a transaction has more information than others. In cyber security, information asymmetry is very common, for example organisations often do not have information on how robust the cyber security is for all elements in their supply chain.

d. **Imperfect information** is where businesses have incomplete information regarding the cyber security risks they manage.

e. **Coordination failure** occurs when individuals or firms could collectively benefit from a more desirable outcome, but their actions are not coordinated, leading to an inefficient or suboptimal result. As both networks and supply chains are interconnected, failure of one can cause widespread disruption. The table below highlights the specific market failures that are present in certain parts of the UK's cyber security regime.

Table 3.1: Summary of the market failures in cyber security regime

Market	Externalities	Public good	Information asymmetry	Imperfect information	Coordination failure
MSPs in scope	✓	✓	✓	✓	✓
Data centres in scope	✓	✓	✓	✓	✓
New energy essential service in scope	✓	✓	✓	✓	✓
Enable regulators to designate critical suppliers	✓	✓	✓	✓	✓
Improving incident reporting			✓		✓
Strengthen information sharing		✓	✓		✓
Duty on RDSPs to provide risk information				✓	
Regulators' cost recovery mechanisms	✓				
Strengthen enforcement mechanisms		✓			✓
Statement of strategic priorities		✓			✓
Enable the government to update the NIS Regulations framework in the future	✓	✓	✓	✓	✓
Security and resilience requirements	✓			✓	
Improve supply chain security	✓	✓	✓		✓
Power for the SoS to direct a regulator, where it is necessary and proportionate for national security				✓	
Power for the SoS to direct a regulated entity, where it is necessary and proportionate for national security				✓	

Table 3.2 sets out the SMART objectives measure by measure, alongside the strategic case for change and more information on which market failures they address.

Table 3.2: Strategic case for change, SMART objectives and market failure addressed by measure

Measure	Strategic case for change	SMART objectives	Market failures addressed
Amend the NIS Regulations by bringing more entities, sectors and services into scope.			
1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations	MSPs provide essential digital services to our CNI and economy. They are an attractive target for cyber attacks, because of their widespread and trusted access to their clients' networks. These networks enable cyber criminals to disrupt hundreds, even thousands of organisations, by successfully attacking only one MSP. By bringing RMSPs into scope of the NIS Regulations, RMSPs will be required to uphold similar standards of cyber security as the RDSPs currently in scope, deterring cyber attackers and minimising the impacts should an incident occur. *The sustained attacks against MSPs that formed the tactical campaign known as Operation Cloud Hopper show that by attacking one MSP in a supply chain, many end users can be significantly impacted.* [18]	To reduce the risk that a compromise of a managed service will cause to either it or its customers' businesses, as well as reducing the risk of an MSP being used as an attack vector to compromise a customer's system. This will mitigate disruption to the UK's essential services and CNI as well as the economy and wider society.	**Externalities** – By bringing RMSPs into scope, the government can ensure operators take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Regulation reduces the negative impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Public good** – It also addresses the under-provision of cyber security as a public good by mandating baseline protections that benefit the wider digital ecosystem. **Information Asymmetry** – Bringing RMSPs in scope will ensure relevant parties that engage with them in the supply chain will have better information on cyber security risks. **Imperfect information** – By bringing RMSPs into scope, the

[18] Operation Cloud Hopper, PwC (2021).

Measure	Strategic case for change	SMART objectives	Market failures addressed
			government ensures organisations improve the knowledge of their own cyber security risks. **Coordination failure** – MSPs are deeply interconnected with critical services and digital supply chains. Regulation improves coordination, sets consistent standards, and enables better risk and information sharing across the network.
2. Bring data centre infrastructure into scope of the NIS Regulations	Data centres house and support the technology and data that meet the demands of our digital lives. They underpin almost all economic activity, including for essential services. Data centres also support innovation, including the development of AI and other technology. In recognition of their critical role, data centres were designated as CNI in 2024, however they are currently not regulated directly, unlike other CNI utilities and adjacent infrastructure. This leaves data infrastructure vulnerable to cyber attacks. Disruption or compromise of data centre infrastructure can have significant negative impacts on the public, businesses, and national and economic security.	To reduce the risk of disruption or compromise of data centres by having appropriate and proportionate measures in place to manage risks. This will strengthen the consistency of security and resilience risk mitigation of operators within scope, in line with other essential services and CNI. Secondly, to improve information flows between data centre operators and authorities. This will give the regulator and government visibility of the sector, risks and trends to formulate policy. The third objective is to provide a platform for secure growth and investment. The impacts of the regulation will apply across a proportionate majority of the sector, minimising the risk of market distortion and creating a level playing field from which to grow and innovate with confidence.	**Externalities** – By formally designating data centres as CNI and moving toward direct regulation, the government can ensure operators in scope take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Regulation reduces the negative impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Public good** – It also addresses the under-provision of cyber security as a public good by mandating baseline protections that benefit the wider digital ecosystem.

Measure	Strategic case for change	SMART objectives	Market failures addressed
	For example, outages at Google and Oracle data centres in 2022 led to a major data outage for the NHS.		**Information asymmetry** – Security and resilience are key in data centres' business models. They have little to no incentive to wilfully declare their vulnerabilities and outages, especially in the absence of similar public information about their competitors. Bringing them in scope will give regulators and government visibility of the sector. Bringing them into the regulations will improve the awareness of other parts of the supply chain of the cyber security risks associated with data centres. **Imperfect information** – By bringing data centres into scope, the government ensures organisations improve the knowledge of their own cyber security risks. **Coordination failure** – Data centres are deeply interconnected with critical services and digital supply chains. Regulation improves coordination, sets consistent standards, and enables better

Measure	Strategic case for change	SMART objectives	Market failures addressed
			risk and information sharing across the network.
3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations	Load control enables the remote control of consumer appliances (known as Energy Smart Appliances) in commercial, industrial and domestic environments, by responding to electricity usage signals. Large Load Controllers are organisations who control 300MW of electrical load or more in aggregate and who send signals controlling load to and from energy smart appliances. Despite their importance in the fast-growing market of smart flexibility services, these controllers currently lack cyber security requirements. This poses significant risks, as a cyber attack on large load controllers could lead to severe disruptions and power outages. Such attacks would undermine consumer confidence and discourage the adoption of smart, flexible energy solutions, thereby impacting the UK's Clean Power 2030 and Net Zero goals. Additionally, widespread disruptions to the grid could lead to significant economic and social impacts, further affecting broader HMG objectives. *Case study: Cyber attacks on energy systems can cause blackouts, financial losses, and national security threats.*	To reduce the risk of disruption to the wider grid by placing cyber security requirements on large load controllers. This will align these organisations who could have a critical impact with other essential services and CNI. They will be required to meet cyber security standards and report to their regulator (Ofgem), which will provide assurance of the sector's resilience against the growing threat landscape and give the regulator and HMG visibility of the sector, risks and trends enabling informed policy formulation. Improving cyber security in this sector will also enable growth and investment in smart energy, furthering the government's green energy objectives whilst maintaining confidence in the reliability of the UKs energy system, leading to acceleration of the adoption of sustainable energy practices.	**Externalities** – By bringing large load controllers in scope, the government can ensure these organisations take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Regulation reduces the negative impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Public goods** – Without proper regulation, market participants may underinvest in smart energy, as they cannot capture the full social benefits of a secure, resilient grid. By introducing cyber security standards and regulations for large load controllers, the government ensures that the social value of a secure and reliable grid is realised. **Information asymmetry** – By implementing clear cyber security requirements and encouraging information sharing about risks and vulnerabilities, the

Measure	Strategic case for change	SMART objectives	Market failures addressed
	For example, the 2021 Colonial Pipeline attack in the US disrupted fuel supply across the eastern United States. The impact on disturbances to the energy market can also be seen during the Heathrow transformer fire in March 2025.		government can correct this information asymmetry, ensuring that all stakeholders understand the risks and take appropriate actions. This would enhance trust and accelerate the adoption of smart, flexible energy solutions necessary for achieving Net Zero goals. **Imperfect information** – By bringing large load controllers into scope, the government ensures organisations improve the knowledge of their own cyber security risks. **Coordination failure** – Large load controllers are deeply connected with supply chains. Regulation improves coordination, sets consistent standards, and enables better risk and information sharing across the network.
4. Enable regulators to designate critical suppliers	Supply chain vulnerabilities are a major risk to essential and digital services. A cyber-attack on a supplier to an essential or digital service, or a compromise of its network and information systems, can cause major disruption and data breaches,	To effectively manage risks to the provision of essential services and key digital services which are introduced by third parties by virtue of the overreliance, dependency, or concentration within that sector. This measure establishes a framework to designate certain suppliers where if that organisation provides goods	**Externalities** – By bringing these suppliers in scope, the government can ensure these organisations take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Regulation reduces the negative

Measure	Strategic case for change	SMART objectives	Market failures addressed
	threatening economic resilience and national security. *For example, in June 2024, Synnovis, a supplier to the NHS, suffered a ransomware attack that resulted in 11,000 postponed outpatient appointments and elective procedures, and an urgent call for blood donors. This demonstrated the real world impacts a cyber attack on a supply chain can have on working people.*	or services to a provider of essential or digital services, the supplier relies on network and information systems for the purposes of that supply, and an incident affecting that supplier's network and information systems could cause disruption to essential or digital services who rely on them (or essential or digital services generally) and that disruption is likely to have a significant impact on the economy or day-to-day functioning of society in the whole or any part of the UK. Designated suppliers would be subject to proportionate duties to ensure consistent and effective management of risks (although these requirements will be introduced under secondary legislation). This targeted approach will improve visibility of key suppliers, ensure more consistent risk handling across sectors, and enhance national resilience aligning with the UK's strategic priorities on economic growth, national security and economic resilience. It provides a strategic tool to address cross-sector vulnerabilities and respond more effectively to emerging threats.	impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Public goods** – Expanding the scope to critical suppliers leads to better protection of public infrastructure and services necessary for the protection and well-being of businesses and individuals. **Imperfect information** – By bringing critical suppliers into scope, the government ensures organisations improve the knowledge of their own cyber security risks. **Information asymmetry** – Bringing these designated suppliers in scope will give regulators and government greater visibility of these important organisations. Bringing them into the regulations will improve the awareness of other parts of the supply chain of the cyber security risks associated with these suppliers. **Coordination failure** – Designated suppliers will be

Measure	Strategic case for change	SMART objectives	Market failures addressed
			deeply connected with key organisations within NIS regulated sectors. Regulating these suppliers will improve coordination, set consistent standards, and enable better risk and information sharing across the network.
Empower regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties			
5. Improving incident reporting	Effective incident reporting is essential to enable regulators to understand immediate impacts across their sectors and to monitor compliance with security requirements; to facilitate timely assistance and support from the NCSC; to augment the government's overall understanding of the threat landscape; and (via transparency notifications) to enable users of to take mitigating action where the services they depend on have been disrupted or used as a vector for compromising their own systems. In 2019, 2020 and 2021, there were only 13,12 and 22 NIS incidents reported, respectively.[19] With 43% of businesses reporting experiencing a cyber breach last year, it is clear that many incidents that could have a significant impact in the UK go unreported.[20] The lack of	To support a more comprehensive and immediate understanding of incidents, sectoral impacts and regulatory compliance through an expansion of the incidents that are reported to regulators and an earlier notification of unfolding incidents. Secondly, to facilitate the timely support needed for incident management through swifter sharing of incident reports with the NCSC. Thirdly, to enable appropriate mitigating actions on the part of customers of affected entities through the issuing of transparency notifications following the reporting of incidents.	**Information asymmetry** – Key stakeholders (regulators, NCSC, and businesses) may lack real-time or complete data regarding evolving cyber threats. When incident reports are made available simultaneously to regulators and the NCSC, it ensures that accurate and up-to-date information is shared promptly, allowing regulators to monitor threats and provide assistance in a timely manner. **Coordination Failure** – This also corrects coordination problems that can prevent effective decision-making, regulatory oversight, and overall cyber security resilience.

[19] DSIT, Second PIR of the Network and Information Systems Regulations 2018 (2022)

[20] Cyber security breaches survey 2025 - GOV.UK

Measure	Strategic case for change	SMART objectives	Market failures addressed
	reports being made under the current reporting threshold is an issue that has been highlighted by both regulators and by several high-profile incidents that have been reported in the press but not to regulators under the NIS Regulations.[21] The Bill will proportionately expand the scope of incidents to be reported, ensuring that businesses are not unduly burdened. It will also address risks inherent in the current 72-hour reporting requirements by mandating quicker initial notification, and address the regulatory gap that currently exists in terms of requiring user notification of incidents. *For example, in 2023, ransomware actors exploited a vulnerability on the file transfer platform MoveIt, with implications for British businesses and the US Department for Energy. This was not reportable under the NIS Regulations 2018.*		
6. Strengthen information sharing provisions, such as by enabling regulators to share	Information sharing under the NIS Regulations helps ensure the regime functions effectively. It is vital that there are clear gateways to share information between entities involved in implementing the NIS Regulations	To strengthen and expand information sharing provisions under the NIS Regulations to provide greater certainty on what information can be shared, and with whom. This will in turn support delivery of the regulatory functions of regulators, inform government policy development on	**Public good** - the sharing of information on cyber security is a public good in that it one entity's benefit from the sharing of information does not prevent others from benefitting, and one entity's use of the information

[21] Sky News, 'Nine cyber attacks on UK's transport sector missed by mandatory reporting laws' (2021)

Measure	Strategic case for change	SMART objectives	Market failures addressed
information for specific purposes with each other and public authorities, and vice versa	and appropriate safeguards on how that information is used. However, current information sharing provisions do not provide for clear gateways for regulators to share information with UK public authorities (including DSIT), and vice versa.	national security, critical infrastructure and cyber resilience, and enable effective evaluation of the NIS framework and its implementation.	does not diminish the ability of others to use the information (subject to relevant safeguards). As such, without intervention, information sharing would be underprovided and may affect the effectiveness of the NIS regulatory regime. **Information asymmetry** – These changes will improve the effectiveness of current data sharing between regulators and public authorities which can in turn allow more effective collaboration in tackling threats. Changes will provide greater certainty in the data sharing arrangements. **Coordination failure** – This helps correct the coordination problems that can prevent effective decision-making, regulatory oversight, and overall cyber security resilience.
7. Ensuring the Information Commission has appropriate information related to risk	Once the Bill's measures take effect, an estimated 2,000 organisations will be regulated by the Information Commission. The Information Commission will be expected to determine the appropriate level of supervision for each of these regulated entities, taking risk into account. To do	To ensure that the Information Commission receives information relevant to risk assessment from regulated entities, to support the Information Commission to adopt a more flexible, proactive oversight regime for RDSPs. The powers in the Bill will allow for a general duty for RDSPs and RMSPs to provide risk-based information	**Imperfect information** – Currently, relying on voluntary data submissions is inadequate, leading to gaps in risk assessment and oversight. By establishing clearer data-sharing mechanisms under the Bill, the Information Commission will be

Measure	Strategic case for change	SMART objectives	Market failures addressed
	this effectively, the Information Commission will require sufficient data to assess the wider risk posed by the regulated digital services/managed services. Relying on individual voluntary requests for this information, as the Information Commission currently do, will not be sufficient for collecting data across all of the Information Commission's regulated entities and assessing the associated risks. *For example, there have been attacks impacting the Ministry of Defence's payroll systems and the HMG estate (FCDO/HMT) through or involving an MSP. By understanding if the MSP has government clients, they are better equipped to enforce appropriately.*	to the Information Commission and, where necessary, to update that information. This in turn should help to reduce disruption to the UK's essential services, CNI and wider economy.	able to receive comprehensive information across the entities it regulates, improving its ability to assess risk and apply appropriate supervision.
8. Improving regulators' cost recovery mechanisms	It is vital for the resilience of our essential services that the UK have better-resourced regulators that can support organisations to reach and maintain an appropriate level of cyber security. Currently, regulators are constrained in their ability to recover the full costs associated with overseeing and enforcing the NIS Regulations, and in the ways in which those costs can be recovered (i.e. through direct invoicing rather than fees). This risks both undermining the	Firstly, to enable regulators to carry out the full extent of their duties and functions with fewer constraints in how they recover costs, enhancing the effectiveness of the regulatory regime and overall compliance with security and resilience requirements. Secondly, to achieve a fairer allocation of costs by making those organisations that generate the cyber risk pay costs associated with the regulation of that risk, minimising the burden on taxpayers and the public purse. Thirdly, to provide clarity and predictability for regulated entities and	**Externalities** – This would make the provision of regulation of cyber security more sustainable and efficient, benefiting the public by reducing the need to pass the cost of regulation on to the taxpayer.

Measure	Strategic case for change	SMART objectives	Market failures addressed
	effectiveness of the regulatory regime and displacing costs on to the taxpayer where regulators depend on public-sector funding.	regulators by enabling fee-based methods of cost recovery, in addition to direct invoicing.	
9. Enable the Secretary of State to designate a statement of strategic priorities	The NIS Regulations apply across a number of different sectors and are currently enforced by 12 different regulators. We assess that, to date, the implementation and success of the NIS Regulations have been inconsistent. This has led to some NIS sectors being relatively more vulnerable to hostile activity and disruption than others. *For example, a statement of strategic priorities could require regulators to seek to take risk-based approaches to enforcing the NIS Regulations, ensuring that all regulators focus their resources where risk is most prominent.*	To ensure that the NIS Regulations are applied consistently and effectively across sectors, this measure will enable the Secretary of State to set outcomes that regulators will be required to seek to achieve. The success of this measure will be measured in the steps that regulators take in working towards these outcomes, and in the consistency with which regulators undertake their functions. The Secretary of State will publish an annual report that will set out the steps that regulators have taken in order to seek to achieve the outcomes in the statement of strategic priorities, and regulators will be required to provide information upon request to DSIT to aid in the drafting of this report. The Secretary of State's report, based on the information provided by regulators, will enable an assessment of the success of this measure.	**Coordination failure** – This measure will provide better consistency in approach between regulators/sectors, as all would be required to work towards the same outcomes. **Public good** – Inconsistent enforcement and implementation of the NIS Regulations across different sectors has created a situation where the public good of cyber resilience is under provided in certain sectors, more so than others. This measure will ensure that cyber resilience becomes a more evenly distributed public good, with minimal gaps that could otherwise be exploited by attackers. This fosters a more secure, equitable environment where the collective benefits of cyber security are shared across all sectors, reducing vulnerabilities and mitigating wider societal risks.
10. Strengthen the enforcement mechanisms in	A successful regulatory regime requires an effective sanctions framework, to deter non-compliance	To ensure that regulators are able to take effective, proportionate and predictable	**Public good -** Increasing the efficacy of the enforcement regime deters non-compliance

Measure	Strategic case for change	SMART objectives	Market failures addressed
the NIS Regulations	and incentivise entities to deliver on their duties. Regulators report that enforcement under the NIS Regulations has been constrained by unclear band structures and a maximum penalty which is insufficient to deter non-compliance across all NIS sectors. In light of the considerable risks arising from non-compliance, it is vital that the enforcement regime is improved to ensure the success of the regulations and the resilience of key infrastructure.	enforcement action against non-compliance. Success will be measured by the effect it will have on increasing compliance and deterring non-compliance. Measures are developed in line with existing precedence, taking into account pertinent factors to the NIS regime, and their use will be reviewed by the Secretary of State periodically, to ensure they remain both effective and proportionate.	across the NIS sectors which is essential for the protection of our national security and resilience. **Coordination failure -** Unclear penalty bands structures means that enforcement action is inconsistent across regulators and prevents effective regulatory enforcement action.
Ensure that the NIS Regulations keep pace with the ever-changing cyber landscape and equip government to take decisive action to protect our national security			

Measure	Strategic case for change	SMART objectives	Market failures addressed
11. Delegated powers to enable the government to update the NIS Regulations framework in the future	Following the UK's departure from the EU and the repeal of the European Communities Act 1972, the government no longer has appropriate powers to amend the NIS Regulations. This has left our cyber security legislative framework unable to respond to new threats and developments in the wider cyber landscape. This ultimately risks the cyber resilience of the services that the UK economy and society relies on. *For example, the government may wish to add new sectors to be in scope of the NIS Regulations, if there is compelling evidence that doing so is necessary to reduce cyber risks in that area. Had this power been in place, the government could have brought data centres – which the public and businesses rely on – into scope sooner.*	To ensure that the government is able to respond in a timely manner and make changes to the NIS Regulations to ensure that they cover the appropriate services that the UK economy relies on, and that both regulated entities and regulators are equipped and confident in managing the risk to these services. The Bill allows for the Secretary of State to publish a Code of Practice that will set clear guidelines and good practice for regulated entities in scope to follow, supporting them to meet the requirements imposed by the regulations.	**Imperfect information** – Granting the government powers to update the NIS Regulations ensures collective resilience, improves information flow, and keeps the framework effective, proportionate and responsive. **Externalities** – By having the power to update the NIS Regulations, the government can continue to ensure relevant organisations take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Regulation reduces the negative impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Public goods** – By having the availability to update the NIS Regulations, the government can continue to ensure that cyber security standards and regulations for relevant organisations are fit for purpose into the future. **Information asymmetry** – By being able to update the NIS Regulations and ensure the

Measure	Strategic case for change	SMART objectives	Market failures addressed
			continuation of cyber security requirements and information sharing about risks and vulnerabilities, the government can correct any information asymmetry into the future. **Imperfect information** – By being able to update the NIS Regulations, the government ensures that organisations improve the knowledge of their own cyber security risks into the future. **Coordination failure** – Organisations continue to become increasingly interconnected through supply chains. Having up to date regulation improves coordination, sets consistent standards, and enables better risk and information sharing across the network.

Measure	Strategic case for change	SMART objectives	Market failures addressed
12. Security and resilience requirements	It is crucial that security requirements for services and firms that provide digital services are proportional and appropriate. Existing security requirements are aging, below NCSC's recommended level, and are unlikely to provide sufficient risk mitigation. They therefore need to be updated. Whilst there is a wide duty for OESs to take "proportionate technical and organisational measures to manage risks", more detailed security requirements currently only apply to RDSPs. There is no mechanism to update these or extend their application. The Bill will enable security requirements to be set via secondary legislation to meet current threats and vulnerabilities, while also giving the government the flexibility to raise these in the future if/when further threats are identified and updates are necessary. *For example, the EU were able to update NIS 2 to expand the range of sectors that this covered and to introduce additional security requirements for regulated entities to meet. This power will enable the UK to do likewise.*	To ensure that the Secretary of State has the power to set security requirements that meet the identified threat level, and that these can be applied consistently.	**Externalities** – Having better security requirements ensures that organisations are best equipped to mitigate and minimise the impact of security and resilience risk, including cyber compromise. Aligning private incentives with public interest. Regulation reduces the negative impacts that cyber attacks have across the economy by requiring minimum standards and risk mitigation. **Imperfect information** – By allowing security requirements to be set and updated through secondary legislation, the Bill ensures that standards remain aligned with current risks. This provides regulated entities with better guidance on what is expected, reducing uncertainty and aligning their investment with actual vulnerabilities. It also improves transparency and reduces information asymmetries between firms, regulators, and the public, leading to better-informed decisions and a more secure digital market overall.
13. Enable government to	Supply chain vulnerabilities are a major risk to essential and digital services. A	To foster better practices to protect essential and digital services by	**Externalities** – Supply chain vulnerabilities create costs that

Measure	Strategic case for change	SMART objectives	Market failures addressed
improve supply chain security	cyber-attack on a supplier to an essential or digital service, or a compromise of its network and information systems can cause major disruption and data breaches, threatening economic resilience and national security. While OESs carry obligations under the NIS framework, there is insufficient clarity and capability to effectively manage supply chain risk. Improving security across the supply chain is therefore vital to reduce systemic cyber risks and enhance the resilience of key sectors and services. *Case study: In December 2020, the network management software company SolarWinds got hacked, resulting in a widespread breach of multiple government agencies and private companies. A total of 18,000 customers and businesses were impacted*.	embedding duties on operators to manage risks arising from their critical suppliers. Interventions will reduce the likelihood and impact of supply chain-related cyber incidents by embedding clear accountability and improving supplier risk governance. The objectives include increased adoption of secure and resilient procurement practices, better oversight and transparency of third-party risks, and a reduction in the number and severity of disruptions caused by supplier failures. These outcomes support stronger regulatory engagement, improve sector-wide preparedness, and align with the UK's strategic priorities on economic growth, national security and economic resilience.	affect not just individual companies but also individuals and the broader economy. Strengthening security helps internalise these costs, reducing broader systemic risks. **Public good** – Supply chain security benefits everyone in the economy, not just the involved entities. Mandatory cyber security measures ensure this public good is provided, enhancing national and economic resilience. **Information asymmetry** – Businesses may lack awareness of supply chain risks, leading to poor decisions. Improved risk management capabilities and clearer guidelines under the Bill address information gaps, enabling better security planning. **Coordination failure** – Supply chains are interconnected, and one failure can cause widespread disruption. This measure enables improved coordination and information sharing, correcting network effects and enhancing overall system resilience.

Measure	Strategic case for change	SMART objectives	Market failures addressed
14. Introduce a power for the Secretary of State to direct a regulator, where it is necessary for national security	Geopolitical or technological developments can quickly lead to unexpected increases in the threat posed to regulated entities' networks and systems. The government does not have the ability to ensure that sectors respond to increased threats by adopting more stringent security measures. This is something regulators would be best placed to implement, but government has insufficient powers to require action from regulators in unforeseen circumstances that threaten national security. *For example, the Secretary of State may use the power if the overall threat landscape faced by the UK worsens, such as in response to international conflicts.*	To ensure that regulators respond at pace to sudden changes in the threat landscape, where this is necessary for national security, by adjusting regulatory expectations for regulated entities. This will result in NIS-regulated entities being better protected from malicious cyber activity in periods of heightened tension, reducing levels of disruption to services. The success of this policy will be measured through the effectiveness of action that regulators take in response to directions issued, and the degree to which that action limits the level of disruption caused by malicious cyber activity.	**Imperfect information** – By empowering the government to ensure that regulators encourage their sectors to adopt stronger security measures during heightened threats, this measure addresses imperfect information by ensuring regulators act on critical intelligence they might otherwise be privy to, thereby strengthening system-wide resilience.
15. Introduce a power for the Secretary of State to direct a regulated entity, where it is necessary for national security	At present, the government does not have a power to direct regulated entities to address cyber threats, even where this is judged to be essential for safeguarding national security. The growing threat posed by high capability actors and hostile states means that this gap could be exploited with increasing regularity and impact, putting the operation of critical infrastructure at risk.	To ensure that regulated entities respond at pace to threats to their networks and information systems which pose national security risks. The success of these powers will be measured through assessing organisations' compliance with directions they have received, and the effectiveness of the action (required in the directions) taken in addressing the threat. We also expect that the existence of the powers will encourage organisations to voluntarily take action to address national	**Imperfect information** – By enabling the government to direct an entity to take specified steps in response to national security threat, this measure addresses imperfect information by requiring an entity to address a threat that it might not be aware of.

Measure	Strategic case for change	SMART objectives	Market failures addressed
	For example, the Secretary of State may use the power if the government becomes aware of a cyber incident on the network of an operator of an essential service, where the incident could disrupt the provision of the service to the degree that it constitutes a national security threat.	security threats before a direction is issued to them.	

4. Description of proposed intervention options and explanation of the logical change process whereby this achieves SMART objectives

Preferred option – amend and future-proof the NIS Regulations. The proposed measures are:

1. Bring RMSPs into scope of the NIS Regulations, to be regulated by the Information Commission.
2. Bring data centres at or above 1MW capacity and enterprise data centres at or above 10MW capacity into scope of the NIS Regulations, to be regulated by Ofcom and DSIT as a joint regulator.
3. Introduce load control as an essential service in the electricity sector and bring large load controllers (those with a potential aggregate load of 300MW or above) in scope of NIS Regulations, to be regulated by Ofgem.
4. Enable regulators to identify and designate specific high-impact suppliers as 'designated critical suppliers', bringing them under comparable obligations as OESs and RDSPs.
5. Improve incident reporting by expanding the incident reporting criteria, updating incident reporting times, streamlining how information is shared with NCSC, and enhancing transparency requirements for RDSPs, RMSPs being brought into scope, and data centres.
6. Strengthen information sharing provisions, such as by providing a clear gateway for regulators to share information with public authorities, and vice versa.
7. Expand the duty in secondary legislation on RDSPs to provide information to the Information Commission to enable them to take a more proactive approach to assessing the risk of RDSPs and RMSPs being brought into scope.
8. Improving cost recovery by enabling the full costs of NIS-related functions to be recoverable through flexible cost recovery mechanisms.
9. Grant the Secretary of State the power to designate a Statement of Strategic Priorities, providing a unifying set of objectives for regulators to seek to achieve.
10. Strengthen the enforcement mechanisms in NIS Regulations by amending the maximum penalty threshold and simplifying the banding structure, enabling an effective, proportionate regime and better compliance.
11. Grant the Secretary of State powers to update the regulatory framework in the future, such as by ensuring that the right sectors and sub-sectors are in scope of the NIS Regulations, making improvements to how the NIS Regulations are implemented, or changing duties and responsibilities to ensure they remain effective.
12. Enable the Secretary of State to update security and resilience requirements via secondary legislation.
13. Enable the government to set stronger supply chain duties for OESs and RDSPs in secondary legislation.
14. Grant the Secretary of State the power to direct regulated entities to take action to address threats and incidents, when it is necessary and proportionate for national security.
15. Grant the Secretary of State the power to direct regulators to take action, when it is necessary and proportionate for national security.

Table 4.1: Bill Theory of Change

Policy	Objectives	Inputs	Activities	Assumptions	Output	Outcome
Bringing data centres into scope	Reduce risk of disruption or compromise of a data centre	Data centre in scope of the NIS Regulations	Data centres meet relevant duties set out in legislation including: notifying and providing certain information, having in place appropriate and proportionate measures to manage risks, and reporting significant incidents.	It is assumed that these firms will improve their cyber security as they are designated under NIS. Evidenced in NIS Post-Implementation Review.	Improved cyber security and resilience of data centres	Protect essential services and businesses so that the public can get on with their lives
Bringing relevant managed service providers (RMSPs) into scope	Reduce risk that compromised RMSPs pose, including to an end business	RMSPs in scope of the NIS Regulations	RMSPs subject to the same duties as those placed on firms that provide digital services.		Improved cyber security and resilience of RMSPs	
Bringing large load controllers into scope	Reduce risk of disruption or compromise of a large load controller	Large load controllers in scope of the NIS Regulations	Large load controllers meet relevant duties set out in legislation including: notifying and providing certain information, having in place appropriate and proportionate measures to manage risks, and reporting significant incidents.		Improved cyber security and resilience of large load controllers	

Designation of critical suppliers	Reduce risk that critical suppliers pose to OESs and RDSPs by bringing them in scope of the regulations	Enable regulators to bring the most critical suppliers in scope of the NIS Regulations	Regulators are able to designate the most critical suppliers, this extends to small and micro DSPs. Critical dependencies would be brought in scope of the core security requirements and incident reporting obligations.		Improved oversight of supply chain risk	
Statement of strategic priorities	Provide a clear and coherent framework for cyber security regulation across all sectors	Providing SoS with the power to publish a Statement of Strategic Priorities	Publication of a Statement of Strategic Priorities to be updated every three to five years in consultation with regulators. Report on regulators' activity in relation to priorities to be published annually.	Assumption that setting consistent objectives will lead to move effective implementation of the Regulations.	Regulators across all sectors implement the regulations in a consistent manner	Ensure that regulators are well-equipped to implement the NIS Regulations, creating a stable environment which fosters economic growth
Information sharing	Improve information sharing to support effective functioning of NIS regime.	Strengthen and expand information sharing gateways	Regulators are able to share information with public authorities, and vice versa, including government.	Assumption that strengthening information sharing will improve the functioning of the NIS regime.	Clear gateways to share information between entities involved in NIS implementation and strengthened safeguards on how information is used	

Incident reporting	Provide regulators and NCSC with a stronger footing to address incidents and emerging risks	Updating and enhancing current reporting requirements	Expanding the incident reporting criteria, updating incident reporting times, streamlining reporting, and enhancing transparency requirements for firms that provide regulated digital services, managed services and data centres.	It is assumed that there will be more incidents reportable under the NIS Regulations and that firms aren't currently reporting these incidents.	Regulators and NCSC have a more comprehensive view of the threat landscape	
Information gathering	Improve Information Commission's ability to proactively identify and address cyber risks	Provide the Information Commission with more information to identify the most critical firms	Duties on RDSPs and RMSPs to provide risk-based information with the Information Commission upon registration and afterwards via Information Notices.	Assumption that a more proactive approach will help identify and mitigate of cyber risk.	Information Commission take a proactive approach to identify and mitigate cyber risks	
Cost recovery	Enable regulators to carry out all duties under a flexible cost recovery mechanism	Overhaul of the cost recovery regime	Allow regulators to set a fees regime, recover costs, or a mixture of these processes to cover the expenses of the regulations, including enforcement.	Financial constraints are assumed to be a barrier for regulators' effectiveness.	Regulators have the resources to effectively perform their duties	

Enforcement reforms	Drive compliance through more effective and proportionate enforcement	Enable regulators to issue higher maximum penalties based on % turnover.	Regulators issue penalties that are calibrated to be meaningful and proportionate. Regulated entities have fewer incentives for non-compliance and are less willing to absorb fines as the cost of doing business.	It is assumed that an effective sanctions regime, which is proportionate, which is certain to be used and can be used quickly, will lead to better compliance.	Increased compliance with NIS	
		Simplify the penalty band structure.	Regulators issue penalties in a more transparent, predictable and consistent manner.		More consistent application of enforcement tools by regulators	
					Increased transparency and predictability of sanctions	
Enable government to update NIS in the future	Ensure the regulatory framework is adaptable to emerging threats	Providing SoS with the power to update the regulatory framework	Government is able, following appropriate consultation, to introduce new requirements and duties for regulated entities, and to bring new sectors/sub-sectors in-scope of regulations, where considered appropriate and proportionate.	Assumption that these powers will enable the legislation to adapt to the changing cyber landscape.	Legislation remains relevant and effective	Strengthening the UK's national security and ensuring the regulations remain effective in the context of an evolving threat landscape
Security and resilience requirements	Establish clear principles and objectives for firms to follow best practice	Provide SoS with the power to update existing requirements	Government is able to set security requirements by regulation that would apply to RDSPs and extend beyond RDSPs, if appropriate and proportionate			

		in the regulation				
Powers of direction	Ensure Government can respond swiftly to incidents and threats with national security risks	Empower SoS to issue directions to regulated entities	Regulated entities are issued with a direction in relation to a specific cyber incident or threat for reasons of national security.	Assumption that the power to issue directions will enable the government to respond swiftly and decisively to protect the UK from national security threats.	Regulated entities promptly address threats and incidents which pose a significant risk to national security.	
	Increase resilience of whole sectors in periods of heightened risk	Empower SoS to direct a regulator to take action	Regulators are issued with directions, requiring them to exercise their functions in a way that supports action to be taken across their sectors in response to a worsening threat landscape.		Sectors adopt more stringent security measures in periods of heightened risk	

5. Summary of long-list and alternatives

This section sets out the long list of policy options that have been considered for each of the Bill's measures. These long list options have then been systematically analysed using "Critical Success Factors" (CSFs), which are the attributes that any proposal must have, if it is to achieve successful delivery of its objectives. The set of CSFs used to assess each reform can be seen below:

- Strategic fit – does the policy meet our objectives? Is it in harmony with other work from UK Government and internationally?
- Effectiveness – is the option likely to be effective in solving the problem? More specifically, each option needs to meet at least one of these criteria (not every option will be relevant to all three):
    - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability and national security are in scope (where not already covered by other domestic legislation)?
    - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?
    - Does it ensure that the regulations themselves are appropriate in an ever-changing cyber landscape?
- Feasibility – how realistically achievable and proportionate is the option for all relevant stakeholders?

Measures to bring more entities into scope of the NIS Regulations

5.1 Measures to bring relevant managed service providers (RMSPs) into scope of the NIS Regulations

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility

		scope of?			
Option 1 - Do nothing	Low	Low	N/A	Low	High
Option 2 - guidance	Low	Low	N/A	Low	High
Option 3 – awareness for customers	Low	Low	N/A	Low	Medium
Option 4 – bring MSPs into scope, except SMEs	High	High	N/A	High	High
Option 5 – bring all MSPs into scope	Low	High	N/A	Medium	Medium

Option 1: Do nothing

Doing nothing would not be effective in addressing the market failure present, and would not ensure that the most appropriate and socially and economically significant sectors are in scope of the vital cyber security regulations. By extension, it would leave the NIS Regulations outdated and not appropriate in an ever-changing landscape. Both public and private organisations are increasingly reliant on MSPs to deliver critical internal business services. The cyber security and resilience of MSPs, and of the services they offer, is often critical to the business continuity of the organisations they provide services to. MSPs have unprecedented access to their customer's IT systems, networks, infrastructure, and data. This makes them an attractive target for malicious actors and vulnerable to cyber attacks. This has included the Cloud Hopper attack on MSPs and the attack on the Ministry of Defence's personnel system. These highlight the vulnerabilities of MSPs and, by extension, the critical services they support. MSPs are not currently directly regulated under the NIS Regulations. Therefore, although 'do nothing' would be feasible for MSPs, it would not be feasible for UK Government to leave them in the current position of not being mandated to manage security risks to their network and information systems nor to report cyber incidents to a regulator. There is voluntary guidance on the minimum security standards that all companies should adopt, issued by the NCSC, but this is not enforceable, meaning that action has not been taken by many MSPs. The prevalence of recent attacks, with the slow uptake of voluntary actions, demonstrate that regulatory action is needed.

Option 2: Encourage the use of voluntary cyber standards and guidance for MSPs

This option is feasible for UK Government as NCSC already provides a range of world-class voluntary guidance which can be used by MSPs to enhance their cyber security and

resilience. This includes a Cyber Security Advisory published jointly by NCSC and Cyber Security authorities in Australia, Canada and the USA.[22] Voluntary cyber standards and products, such as Cyber Essentials, are also available to MSPs, however, this is not mandatory.

However, this option is expected to be ineffective as we do not have evidence of take up or consistent application of this guidance by MSPs. The government recognises voluntary guidance and cyber standards have not been sufficient to address the specific security risks associated with the widespread use of MSPs. By extension, it would leave the NIS Regulations outdated and not appropriate in an ever-changing landscape where MSPs are increasingly relied upon for our digital lives, thereby leaving a gap where the sector is not covered by appropriate protections, leaving many operators of essential and digital services at risk. With the EU bringing MSPs into scope via NIS 2, not legislating in this space would be a poor strategic fit with international precedent. As a result, this option has not been taken forward to short list appraisal.

Option 3: Develop awareness and education for customers of MSPs

An alternative option is to develop education and awareness campaigns aimed at the customers of MSPs. Campaigns could focus on providing guidance and educating buyers of managed services, so they better understand the risks associated with MSPs and how they make procurement decisions that align with their unique security needs. By influencing the demand side to focus more on cyber security, we may be able to change market behaviours. This option would be feasible for UK Government, MSPs and their stakeholders, but would require significant resource in order to develop education and undertake awareness campaigns. In addition, this option would not be effective in ensuring that appropriate sectors are included in scope of cyber regulations, and not effective at solving the market failure, again leaving a gap where critical sectors that many operators or essential and digital services rely on are not covered by appropriate protections. By extension, it would leave the NIS Regulations outdated and not appropriate in an ever-changing landscape. When this policy option was tested in a call for views in 2021, only 31% of respondents thought it would be very effective in promoting uptake of a future framework for MSPs' cyber security and resilience[23], and only 1% thought it would be completely effective. The government agrees with this assessment because of the low uptake of previous campaigns and guidance. For example, only 24% of businesses knew of the Cyber Aware campaign, and only 12% knew of the 10 Steps Guidance or Cyber Essentials.[24]

Therefore, this option has not been carried forward to the short list.

Option 4: Bring all managed services provided by large and medium providers in scope of the NIS Regulations via the Bill. Small and micro businesses would be exempt, unless designated as a critical supplier by a regulator **(preferred option)**

This intervention would be effective in addressing the market failure mentioned above. MSPs are not currently directly regulated under the NIS Regulations, and MSPs are therefore not mandated to ensure security standards for their network and information systems nor to report cyber incidents. The intervention would be effective in bringing a vital sector in scope of cyber security legislation. It would legally require RMSPs to implement effective measures

[22] Cyber Security Advisory
[23] Figure 7 Government response to the call for views on supply chain cyber security - GOV.UK
[24] Cyber security breaches survey 2025 - GOV.UK

to manage the risks posed to relevant network and information systems that their services rely on, as well as ensure that all these firms report relevant incidents. The Information Commission would also be able to assess compliance and intervene where necessary, including in the small and micro organisations that provide the most critical services. This option is feasible for UK Government as there is a good understanding of the UK MSP market and this Bill provides a regulatory vehicle for making this change. To ensure a proportionate approach where we capture MSPs that are most vulnerable, small and micro MSPs will be exempt, unless designated as a critical supplier where deemed important to reducing significant vulnerabilities, in line with the strategic aims of the Bill. This approach is proportionate and consistent with the approach taken by the EU, fulfilling the strategic fit of international alignment where appropriate.

The 2022 consultation on proposals to improve the UK's cyber resilience demonstrated that the proposals regarding digital service providers received overwhelmingly positive feedback.[25] 84% of respondents approved of the measure to expand the regulation of digital service providers, and 79% approved of the measure to amend the supervisory regime for digital service providers. Furthermore, the majority of respondents (70%) indicated that they thought the exemption should be modified to enable a small number of critical providers to be brought under scope of the NIS Regulations.[26]

This option has been taken forward to short list appraisal as it is expected to be effective, feasible, and has strong strategic fit. It was also announced as part of the package of measures in the 2024 King's Speech.

Option 5: Bring all managed services into scope of the NIS Regulations, including small and micro businesses

Broadly, the firms with the largest externalities from their cyber risk are the medium and large firms covered by the NIS Regulations, as these are the firms with the largest number of customers. To regulate all services provided by small and micro MSPs would be disproportionate, as many do not pose serious vulnerabilities. DSIT is therefore planning to maintain the strategic fit with RDSPs where there is currently an exemption for small and micro businesses, still allowing them to be captured where deemed by the Information Commission and other regulators as a critical supplier, to ensure the Bill provides the appropriate protections for the most economically and socially critical parts of the economy. Therefore, this option will not be carried forward to short list appraisal.

After consideration of these long list options against the critical success factors, option 4 has been identified as the only viable option that can be taken to the short list, along with the 'do nothing' option. Therefore, option 4 is the preferred option for this measure.

5.2 Measures to bring data centres into scope of the NIS Regulations

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to	Effectiveness - Does it improve the ability of regulators to fulfil their duties	Effectiveness – Does it ensure that the NIS Regulations themselves are	Feasibility

[25] Government response to the call for views on proposals to improve the UK's cyber resilience - GOV.UK
[26] *Ibid.*

		protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	in respect to the Network and Information Systems regulations?	appropriate in an ever-changing cyber landscape?	
Option 1 - Do nothing	Low	Low	N/A	Low	High
Option 2 – default trajectory	Low	Low	N/A	Low	High
Option 3 – bring 1MW/10MW data centres into scope	High	High	N/A	High	Medium
Option 4- Bring 0.5MW/5MW Data centres into Scope	Medium	Medium	N/A	Medium	Low
Option 5 – bring all data centres into scope	Medium	Medium	N/A	Medium	Low

Option 1: Do nothing

Doing nothing would leave data infrastructure outside the scope of the NIS Regulations. This approach avoids any immediate regulatory burden on data centre operators, allowing them to continue their operations without additional compliance costs or administrative requirements. Although this would be a feasible approach for data centres, it would not be effective in ensuring that the appropriate entities and services are in scope of the vital cyber security regulations. By extension, it would leave the NIS Regulations outdated and not appropriate in an ever-changing landscape where data centres are increasingly relied upon for our digital lives. This makes them an attractive threat vector. Doing nothing would mean

that the vulnerabilities and risks associated with data centres would not be addressed, leaving them susceptible to cyber threats. Data centres underpin almost all economic activity, including the day to day running of the services the public rely on. Disruption or compromise of data centre infrastructure can have significant negative impacts on the public, businesses, and national and economic security. For example, this was seen in the Google and Oracle data centre outages in 2022 that caused a major NHS data outage.

Option 2: Default trajectory (commercial mitigation, voluntary measures and partial regulation over time)

It is likely that many data centres would be brought into scope of the NIS Regulations via the Bill without being brought in as a specific sector. This is because data centres are a critical part of the supply chain for many essential services and CNI, and could therefore be brought into scope under the measure to allow regulators to designate critical suppliers (measure 5.4). This would beneficially introduce security and resilience protections for some data centre sites and services and some of their dependent customers. However, this would likely leave vulnerabilities through inconsistent and ineffective regulation to ensure all appropriate data centres are in scope of vital cyber security regulations. Again, by extension, the NIS Regulations would be left outdated and ineffective when data centres are being increasingly relied upon for our digital lives. DSIT could pursue risk mitigation in the industry through voluntary measures, such as issuing NCSC/National Protective Security Authority joint guidance and encouraging raised standards. This option would be feasible for data centres, however would likely lead to unintended consequences such as inconsistent standards across the industry and vulnerabilities continuing to arise, despite uptake of voluntary standards. As data centres underpin almost all economic activity, including the day to day running of the services the public rely on, this option would not meet our objectives and as a result has not been taken forward to a short list appraisal.

Option 3: Designate data centres at or above 1MW capacity and enterprise data centres at or above 10MW capacity to be regulated under the NIS Regulations **(preferred option)**

Designating (non-enterprise) data centres at or above 1MW capacity, and enterprise data centres at or above 10MW capacity, under the NIS Regulations would bring these facilities into the regulatory framework, ensuring that they adhere to specific security and resilience standards.

Service	**Definition**	**Recommended threshold**	**Rationale**
Data centre	Provide services to **multiple** organisations	1MW or above	This ensures that the regulatory framework captures the majority of third-party data centres, while excluding only the smallest facilities and preventing the capture of objects such as an office server room etc. This threshold brings approximately 81% of UK data centres into scope, covering 182 out of 224 known sites.
Enterprise data centre	Sole purpose of delivering services to its	10MW or above	Unlike third-party data centres, which are in scope at 1MW, enterprise data centres serve only

	own organisation		the internal IT needs of a single organisation and are often subject to robust internal governance. Setting a higher threshold ensures that only the largest and most critical enterprise facilities, those with the greatest potential impact on national resilience and security, are brought into scope.

The preferred approach would bring approximately 81% of the market into scope of the NIS Regulations whilst still allowing for small operators to continue without facing disproportionate compliance costs. This therefore provides an option which is both effective for the government's objectives and feasible for key stakeholders. Additionally, if a data centre operating at below the threshold is deemed to be a key risk, then it can still be designated as a critical supplier and be placed under the NIS Regulations (per measure 5.4).

This measure would be effective in ensuring the appropriate services are in scope of vital cyber security regulations and reflective of the current cyber security threat, where data centres are an increasingly attractive threat vector due to the possible disruption an attack can cause. It will enhance the protection of critical data and infrastructure, reducing the risk of cyber attacks and other security incidents. Although it would impose additional compliance costs and administrative requirements on some data centre operators, we are confident that the approach is proportionate and feasible for these operators. This approach is proportionate and consistent with the approach taken by the EU, fulfilling the strategic fit of international alignment where appropriate. The benefits of improved security and resilience outweigh the drawbacks associated with feasibility. Therefore, this is the preferred option for enhancing the security of data centres. Engagement with industry representatives at the first Data Infrastructure Forum (October 2024) and follow-up workshops confirmed that industry representatives were broadly supportive and content with this approach. Representatives agreed that this regulation would bring significant benefits and establish a 'level playing field' with regulatory certainty and stability in the industry.

This option has been taken forward to short list appraisal because it is expected to be effective, feasible and has a strong strategic fit. The policy was also announced as part of the Cyber Security and Resilience policy statement, published 1 April 2025.

<u>Option 4: Designate co-location and co-hosting data centres at or above 0.5MW capacity and enterprise data centres at or above 5MW capacity to be regulated under the NIS Regulations</u>

Designating data centres (non-enterprise) at or above 0.5MW capacity and enterprise data centres at or above 5MW capacity under the NIS Regulations would bring these facilities into the regulatory framework, ensuring that they adhere to specific security and resilience standards.

This approach would bring approximately 91% of the market into scope of the NIS Regulations, allowing only the very smallest operators (with a combined MW capacity of 3MW) to continue without compliance requirements. However, many small sites will still face compliance challenges.

Whilst this provides an option which is effective for the government's objectives, key stakeholders suggest this is too heavy handed. If a data centre operating at below the threshold is deemed to be a key risk, it can still be designated as a critical supplier and be placed under NIS Regulations (per measure 5.4).

This measure would be effective in ensuring the appropriate services are in scope of vital cyber security regulations and reflective of the current cyber security threat, where data centres are an increasingly attractive threat vector due to the possible disruption an attack can cause.

It will enhance the protection of critical data and infrastructure, reducing the risk of cyber attacks and other security incidents. However, it would impose significant additional compliance costs and administrative requirements on some data centre operators, and we are not confident that this approach is proportionate and feasible for these operators.

This approach is more heavy handed than that taken by the EU, capturing almost all data centres in the UK, including many sites which pose no strategic risks. We do not consider this option feasible as it may include numerous small entities that are not typically categorised as data centres, including office server rooms. This option does not align well with the government's broader goal of fostering economic growth by creating an environment conducive to innovation. It would place an unnecessary and disproportionate burden on smaller businesses, and is therefore not suitable for short list appraisal. It has therefore not been taken forward for short list appraisal.

Option 5: Designate all data centres

Designating all data centres to be regulated under NIS would establish a 'level playing field' and set industry clear expectations on what cyber standards owners and operators are required to meet. This option would include smaller data centres that could be classed as CNI but would fall under the threshold to be in scope of the NIS Regulations, as set out in option 3. We do not see this option as feasible because it will potentially capture large numbers of small entities which would not typically be considered data centres, potentially including such things as office server rooms. This option is a poor strategic fit with the broader government objective of securing economic growth through creating the right environment in which to innovate. It would be an unnecessary and disproportionate burden on smaller businesses, and is therefore not suitable for short list appraisal.

After consideration of these long list options against the critical success factors, option 3 has been identified as the only viable option that can be taken to the short list, along with the 'do nothing' option. Therefore, option 3 is the preferred option for this measure.

5.3 Measures to bring large load controllers into scope of the NIS Regulations

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	Low	N/A	Low	High
Option 2 – Voluntary Standards	Medium	Low	N/A	Low	High
Option 3 – Bring LLCs controlling 300MW and above in scope	High	High	N/A	High	Medium
Option 4 – Bring all load controllers in scope	Low	Medium	N/A	Medium	Low

Option 1: Do nothing

Doing nothing would come at zero additional cost to regulators or large load controllers, however it would not ensure all appropriate sectors are in scope of the vital cyber security regulations, and allow key organisations in this growing market to go unregulated and leave them, and by extension consumers, exposed to significant cyber risk. Internal research highlighted that load controllers provide critical services to the grid and, if compromised, could lead to grid-level impacts and regional power disruption. With little to no regulatory framework

in place, compromise of a large load controlling organisation could offer an attractive prospect for a threat actor. Given the changing energy landscape and the growing access of load controllers across the energy sector, doing nothing poses a significant cyber security and grid stability risk, and would therefore leave a critical gap in the NIS Regulations. Although this option would be feasible for stakeholders involved, it would not be a strong strategic fit with wider government objectives.

Option 2: Encourage the use of voluntary cyber standards

Government has explored whether the use of voluntary cyber standards, such as Cyber Essentials, would be sufficient to mitigate the risk from load controllers. This measure would come at little to no costs to regulators and the additional costs to firms are voluntary, therefore making it a feasible option for HMG. However, while existing voluntary initiatives do stipulate technical cyber requirements, NCSC assessed that these are not likely to drive the level of adequate and consistent cyber resilience needed for managing the potential risk from this market. Furthermore, the voluntary nature of this measure is likely to cause an uneven uptake and level of cyber standards across the industry, therefore making it ineffective and leaving the NIS Regulations outdated for an ever-changing landscape where load controllers play an increasingly greater role in the energy sector. In addition, it would be a poor strategic fit in relation to the government's objectives and international practices, in particular the EU. Therefore, this option cannot be taken forward to short list appraisal.

Option 3: Designate large load controllers as part of the NIS Regulations **(preferred option)**

This option offers a coherent and proportionate approach by integrating load control into an already established regulatory framework, ensuring a strong strategic fit with both the government's strategic aims and international practices, namely the EU. It brings the most critical businesses in the load control market in scope of cyber security legislation, ensuring that regulation remains aligned with the evolving nature of essential energy services.

As load control becomes an increasingly vital component of the electricity system, particularly in the context of a decarbonised, flexible energy system, this option ensures that regulation keeps pace with the technological advancements and the changing cyber risk that comes with this. This option will require large load controllers to demonstrate that they are implementing effective measures to prevent and mitigate a cyber attack, providing assurance to government regarding the sector's resilience against the evolving threat landscape, therefore making it a feasible option for government, as only businesses who control 300MW and above, and therefore can have an individual critical impact on the grid, will be in scope.

Importantly, this approach is both targeted and achievable for stakeholders involved. By setting a clear threshold (load controllers managing 300MW or above), it ensures that only those organisations with the potential to cause significant disruption to the electricity grid are brought into scope. This makes the option proportionate and manageable for both industry and the regulator.

The 300MW threshold was established in consultation with the National Energy System Operator (NESO) and is grounded in operational realities of grid management. NESO maintains high and low frequency reserves based on the loss of the largest supplier of electricity to the grid. NESO adjusts these reserves in accordance with the grid's resilience.

If a cyber compromise caused a sudden drop in electricity demand that was larger than what the system is prepared for, it could throw the grid off balance, potentially leading to serious disruption to the national electricity supply. When the grid is already in a less resilient state, for example during a low demand period, NESO has advised that the grid stability could be impacted by a 300MW loss in demand.

Therefore, a compromising attack on a large load controller controlling 300MW or above, causing unforeseen changes in load, could impact the frequency beyond which NESO is able to manage to keep the system stable and thereby cause major disruption to electricity supply. This threshold has been broadly supported by industry after going to public consultation.

The number of organisations undertaking load control activities in the UK is currently relatively small, but it is expected to grow significantly over the next decade as more consumers adopt smart technologies. Introducing a fixed threshold ensures organisations are brought into scope as soon as they begin managing a level of load that, if compromised, could cause impacts to energy supply under vulnerable grid conditions.

This approach aligns with the existing regulatory treatment of other energy subsectors under the NIS Regulations. It also ensures that only the most relevant and high-impact organisations are subject to regulation, maintaining a proportionate and risk-based approach. Furthermore, it supports a regulatory framework that remains responsive and appropriate in an ever-changing cyber threat landscape, ensuring long-term resilience and adaptability.

This option has been taken forward to short list appraisal as it is expected to be effective, feasible, and has a strong strategic fit with the government's wider aims.

Option 4: Designate all load controllers as part of the NIS Regulations

This option would achieve the desired effect of ensuring load controllers are implementing effective cyber security measures and designating all load controllers across the network would allow for a consistent and 'level playing field'.

However, this approach presents several critical drawbacks. Load controllers represent an emerging and rapidly evolving sector, and imposing NIS regulatory requirements on all load controllers would impose a disproportionate burden, particularly on the smaller businesses, potentially stifling innovation and market growth. It would also place a significant strain on the regulator (Ofgem), making enforcement resource-intensive and potentially unmanageable.

This blanket approach is not a strategic fit with the government's broader aims, including enabling innovation, supporting emerging technologies and delivering the Clean Power 2030 mission. It fails to reflect the current cybersecurity landscape, where risk varies significantly across entities. Smaller load controllers are unlikely to pose an individual risk to energy supply, and subjecting them to the same regulatory standards as larger operators is neither necessary nor proportionate.

We estimate that the costs of this option would outweigh the benefits, delivering poor value for money for all stakeholders. Small load controllers would face high compliance costs, while regulatory bodies would be burdened with additional resource demands.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable options suitable for shortlisting,

alongside the ‘do nothing’ baseline. Therefore, option 3 is the preferred option for taking this measure forward.

5.4 Measures to allow regulators to designate critical suppliers that are fundamental to the provision of essential and digital services

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	Low	Low	N/A	High
Option 2 – advice, guidance	Low	Low	Low	N/A	High
Option 3 – enable regulators to designate ‘critical suppliers’	High	High	High	N/A	Medium
Option 4 – enable DSIT SoS to designate ‘critical suppliers’	Medium	Medium	Low	N/A	Low

<u>Option 1: Do nothing</u>

Supply chains are becoming increasingly complex, and are an attractive target for cyber criminals who can target one aspect of the supply chain and cause wide-reaching impacts for the continuity of essential and digital services. Examples of recent attacks on critical suppliers include the 2024 Synnovis attack that resulted in 11,000 postponed outpatient appointments and elective procedures, and an urgent call for blood donors. The affected NHS trusts declared a critical incident, highlighting how an attack on a single supplier can have far-reaching impacts on the delivery of vital public services.

Doing nothing would not be effective in ensuring the appropriate entities are in scope of vital cyber security regulations. It would fail to address the significant risks posed to essential and digital services, where we know over recent years that the threat facing the UK has grown more intense, frequent, and sophisticated, and aggressors are seeking to exploit vulnerabilities in the supply chain that could cause significant disruption. This was highlighted by the 2022 PIR as a significant downfall of the NIS Regulations 2018, and recent examples (such as those highlighted above) demonstrate the human impacts of doing nothing.[27]. This therefore does not address the risks in the evolving cyber landscape and is not a good strategic fit, as it risks undermining the outcomes that we are seeking to achieve in the Bill through the continuity of services and protecting the public and businesses from the impacts of devastating cyber attacks.

Option 2: Voluntary advice and guidance

The existing Cyber Assessment Framework (CAF) provides advice for relevant firms regulated under NIS to secure their supply chains through contractual means. The government, working with regulators, could issue further advice and guidance, or make amendments to the existing CAF, to raise awareness of the threat arising from 'critical suppliers'. This would be supported by guidance on how to voluntarily work with regulators to identify and manage these dependencies. This would be a feasible option for government and regulators, with little financial burden on them.

NIS legislation already requires regulated entities to consider the security of their supply chains, and the CAF provides advice on how to do this. However, the CAF has proven not to be effective at identifying and securing supply chain risks, and the effectiveness of advice and guidance is limited for the following reasons:

- 'Critical suppliers', by their nature as the sole supplier to many firms involved in the provision of essential services in highly concentrated markets, exhibit strong market power. This structural imbalance means that firms directly involved in the provision of essential services have severely limited ability to require 'critical suppliers' to improve their cyber security through contractual means. Addressing this market failure therefore requires sector-wide regulatory intervention in order to be effective (Option 3).
- Guidance cannot place legal reporting duties on OESs to require specific information from 'critical suppliers' necessary to manage risk, nor does it provide the necessary enforcement measures to compel 'critical suppliers' to improve their cyber security management. Given the scale of the threat posed to essential services by hostile attackers seeking to use vulnerabilities in their supply chain, and the negative

[27] Second PIR of the Network and Information Systems Regulations 2018 - GOV.UK

externalities of such an attack, we judge that a reliance on voluntary action on behalf of firms that provide essential services would be inadequate.

This option would not address the growing vulnerabilities posed by supply chains, which are an increasingly attractive vector to cause possible disruption to essential and digital services, and therefore does not contribute to the government's objectives of protecting the continuity of essential services. Thus, it is a weak strategic fit and cannot be taken forward to short list appraisal.

Option 3: Enable regulators to designate certain suppliers as 'critical suppliers', bringing them into scope of the NIS Regulations **(preferred option)**

This option would be most effective in ensuring that appropriate entities are in scope of vital cyber security regulations. Although it would require some work from regulators to designate the critical suppliers, statutory threshold criteria would need to be met in order for a supplier to be designated, ensuring that only a small number of the most important suppliers are captured: if they provide goods or services to a provider of essential or digital services; the supplier relies on network and information systems for the purposes of that supply; an incident affecting that supplier's network and information systems could cause disruption to essential or digital services who rely on them (or essential or digital services generally); and that disruption is likely to have a significant impact on the economy or day-to-day functioning of society in the whole or any part of the UK. Small and micro RDSPs, previously exempt from the NIS Regulations, would be capable of being designated as 'critical suppliers' if they meet the threshold criteria (and are therefore deemed critical to an essential service). We judge that removing the SME exemption but applying strict criteria to designation would strike the right balance between ensuring effectiveness and feasibility.

Additionally, this option will improve the ability of regulators to fulfil their duties by allowing them to better understand supply chain risk in their sectors through enhanced information gathering powers. Where there are significant risks that cannot reasonably be managed by regulated entities, regulators can directly address the risk through designation. This approach is consistent with the wider NIS Regulations, whereby the regulators are the experts in their field and will be best placed to target the most critical suppliers whose vulnerabilities could pose a threat to our essential services. Designated critical suppliers would be under legal duties to adopt appropriate cyber security measures, and regulators would have the tools to ensure that designated suppliers are meeting these duties. This targeted approach will improve visibility of key suppliers, ensure more consistent risk handling across sectors, and enhance national resilience aligning with the UK's strategic priorities on economic growth, national security and economic resilience.

This would reduce the risk posed to essential and key digital services through the supply chain vector for attack, which stems from the overreliance, dependency, or concentration of specific critical suppliers within a sector. We judge that supply chains will only continue to diversify, with more digital services becoming relied upon for the everyday running of essential services. As such, we deem this option the most effective in ensuring appropriate regulations in the changing cyber landscape now *and* in the future, in which our supply chains are becoming increasingly complex and vulnerable. This option also provides a strategic tool to address cross-sector vulnerabilities and respond more effectively to emerging threats. We assess that this would improve the cyber resilience of those critical suppliers, and significantly reduce the risk of disruption posed to essential and digital services.

There are already domestic examples of action taken in this area which reflect the risk posed to key services from their supply chains and options to address them – including the 2023 update to the Financial Services and Markets Act, which brought Critical Third Parties into scope of cyber requirements. This demonstrates that this option is a good strategic fit, and consistent with other work the government is doing to address supply chain vulnerabilities.

This measure is supported by stakeholders and industry. A 2022 consultation found that a significant majority (90%) of respondents supported the government's authority to designate critical suppliers, with unanimous agreement (100%) from organisations already within scope of the NIS Regulations 2018.[28] That is why this measure was announced as part of the package of measures in the 2024 King's Speech.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable option suitable for shortlisting, alongside the 'do nothing' baseline. It is a strong strategic fit with the government's objectives of protecting the public and the essential services that they rely on. Therefore, option 3 is the preferred option for taking this measure forward.

Option 4: Enable DSIT SoS to designate 'critical suppliers'

We considered this option as a means of ensuring greater cross-sector consistency and coordination in the designation of critical suppliers. Under this approach, the Secretary of State for DSIT would be responsible for all designations, applying the same statutory threshold criteria as Option 3, and bringing designated suppliers into scope of the NIS Regulations. This centralised model would place all designation powers in the hands of DSIT, rather than sectoral regulators.

While this could help drive a uniform approach, we believe it would ultimately be less effective than Option 3. Regulators are best placed to identify, designate and oversee critical suppliers due to their existing relationships with regulated entities, their understanding of supply chains within their sectors, and their sector-specific technical expertise. These factors are essential for making informed, proportionate designation decisions and ensuring effective oversight once suppliers are in scope. The NIS framework is built on a federated model that aligns responsibility with sectoral expertise, and this option would break from that structure.

Although centralised designation could support consistency in principle, we believe this can be achieved under Option 3 through DSIT-issued guidance, promoting cooperation and alignment between regulators while retaining the benefits of sector-led implementation. Against the critical success factors, this option scores less strongly than Option 3, as it is less likely to effectively address supply chain risks due to the absence of sectoral insight and expertise. This reduces its likely impact in improving the resilience of essential and digital services and protecting the public and the economy from cyber threats, and would therefore be a weaker strategic fit. As such, Option 4 does not offer sufficient additional value to justify moving away from the regulator-led model.

Measures to empower regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties

[28] Proposal for legislation to improve the UK's cyber resilience - GOV.UK

5.5 Measures to amend and strengthen the incident report duties of organisations in scope beyond the limit of continuity of service

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	Low	N/A	High
Option 2 – voluntary reporting	Low	N/A	Low	N/A	Medium
Option 3 – expand reporting criteria	High	N/A	High	N/A	Medium
Option 4 – require all incidents to be reported	Low	N/A	Low	N/A	Low

Option 1: Do nothing

Doing nothing would maintain the status quo whereby very few incidents are formally reported to regulators, leaving them without the vital information needed to fulfil their duties.

Under the current regime, cyber attacks like ransomware, pre-positioning and spyware don't have to be reported if they don't immediately disrupt the provision of essential or digital services, despite those attacks having the potential to cause major disruption or compromise. Because of this, it is not correctly serving its intended purpose, and regulators and the NCSC have an incomplete picture of the threat landscape and are not equipped with the adequate

information needed to take corrective and/or preventative measures. Amending the reporting framework to bring a greater range of incidents into scope would help regulators and NCSC ensure that businesses are taking appropriate action to mitigate the risks of their essential service being disrupted.

Maintaining the current position (i.e. doing nothing), where an incident might not be reported until 72 hours after an organisation becomes aware of it, would limit the opportunity for the NCSC and regulators to support the organisation and manage the impact of an ongoing incident. This is compounded by the fact that the NCSC would not receive notification of the incident at the same time as the regulator, which would further delay the NCSC's ability to support in incident response.

Under the current system, there is no requirement for RDSPs, RMSPs, or data centre operators to inform their customers of incidents that have, or could, adversely impact them. This means that those customers could be oblivious to their exposure to risk, and unable to take actions to mitigate that exposure, with potential knock-on effects for the provision of their own services.

We judge that the current system is feasible but ineffective in ensuring regulators and NCSC have the ability to fulfil their duties. By not addressing the problem of regulators not having thorough and reliable data, it undermines the strategic objectives of ensuring regulators are equipped to support those they regulate and monitor compliance with vital cyber security regulations. It fails to ensure a better understanding of how the cyber landscape is evolving in order to better protect our national security and public services.

Option 2: Encourage regulators to include voluntary reporting of a broader range of incident types within their sectoral guidance

Option 2 suggests encouraging reporting beyond what is necessitated under NIS, for example to include incidents that have the potential to cause a significant disruption to a service. This is already being pursued in most NIS sectors (e.g. the water sector), with regulators stating clearly, via guidance, that the companies would not be penalised for voluntarily submitting information. However, regulators have found that regulated entities still do not report these incidents. Given that there is no explicit legal obligation to comply, companies prefer not to share information about such incidents, possibly to avoid regulators from discovering vulnerabilities in the regulated bodies' systems and consequently asking the companies to take action. This option would therefore be ineffective in improving regulators' ability to fulfil their duties and, like option 1, it would undermine the government's strategic objective of equipping regulators to support their sector and monitor compliance, and get a better understanding of the evolving threat landscape to best protect our national security and public services. For these reasons, it is not included in the short list appraisal.

Option 3: Introduce the duty to report incidents that have impacted the operation or security of networks and information systems relied on to provide a regulated essential, digital or managed service, where the incident is having, *or could have*, a significant impact **(preferred option)**

It is vital for the resilience of our critical services that we have regulators that are well-equipped to support organisations to reach and maintain an appropriate level of cyber security. To do this, information is essential. As stated above, we consider that amending the

reporting framework is the best way to ensure that regulated entities are reporting incidents, and that regulators are able to obtain a clear picture of the extent and severity of cyber security incidents. This includes capturing incidents such as ransomware, pre-positioning and spyware, which have the potential to have a significant impact in the UK, through creating disruption to services or compromising sensitive information, but which might not have had a significant impact at the point at which they are discovered.

Option 3(a) Additional requirements for data centre operators (recommended)
In addition to the thresholds specified above, data centre operators would also be expected to report:

In this regulation, "data centre incident" means an incident which could have had, has had, is having or is likely to have—

a) a significant impact on the operation or security of the network and information systems relied on to provide the data centre service provided by the OES in the UK,
b) a significant impact on the continuity of the data centre service provided by the OES in the UK, or
c) any other impact in all or any part of the UK which is significant.

Including an explicit reference to service continuity in the Bill reinforces the core function of data centres, whose primary role is to host network and information systems and support cyber resilience. It ensures that incidents affecting the continuity of data centre services, even if they don't directly impact the network and information systems themselves – remain within scope, preserving the integrity of oversight.

Similarly, including incidents with potential impacts – those that could have caused disruptions – enhances the ability of the competent authority to detect emerging patterns, assess systemic vulnerabilities, and respond proactively. For data centres, this strengthens resilience against evolving risks and aligns with international best practice, such a near-miss reporting under the EU's NIS2 directive. The existing 'significant' threshold provides a natural filter, ensuring that relevant events are captured without overwhelming operators.

Further steps to strengthen the incident reporting regime should also be considered. This includes updating incident reporting times, ensuring reports made to the regulator are shared with NCSC at the same time and enhancing transparency requirements for digital services and data centres.

Updating incident reporting times to introduce a two-stage reporting structure (an initial notification within 24 hours of becoming aware of the incident, followed by a report within 72 hours) would bring incidents to the attention of the regulator sooner, allowing more time to assess what action is needed (if any). The initial notification would be light touch, ensuring the regulated entity can direct their resources to mitigating the effects of the incident as best as possible in the crucial early stages. The regulated entity could then be required to share more information after 72 hours, as under the existing regime, once its understanding of the incident has developed. The two-stage model would be more cost effective for businesses (ensuring feasibility) than requiring one full report within 24 hours, which would divert resources away from the crisis at hand.

Currently, entities are required to provide a report to their regulator, who then shares this with the NCSC. Streamlining reporting, so that the NCSC received information at the same time as it was reported to the regulator, would facilitate prompt engagement and enable the NCSC to provide earlier support to the entity responding to the incident. Requiring a copy of incident reports to be provided to the NCSC will create minimal resource burden to regulated entities, who could simply copy the NCSC into incident reports that they send to their regulators.

Finally, introducing new transparency requirements for digital services, managed services and data centres would ensure customers who may be affected by significant incidents are alerted to those incidents, encouraging openness within the sectors and enabling customers to take steps to mitigate the effects of an incident. This approach is proportionate and consistent with the approach taken by the EU, fulfilling the strategic fit of international alignment where appropriate.

Option 4: Introduce a duty for regulated entities to report all incidents affecting their networks and information systems.

Requiring all incidents to be reported to regulators would, in theory, give regulators and the NCSC the fullest picture of the threat facing the UK, enabling them to plan and prepare most effectively to protect the UK's essential and digital services. However, given the sheer number of incidents facing the UK, regulators would be unlikely to be able to process the information that they would receive, making it unfeasible. The majority of the reporting would likely relate to low-level incidents that were successfully managed by the entity, which could distract from the more important reporting of more sophisticated or successful incidents, therefore reducing the effectiveness of the policy. This option would also be unfeasible for entities in scope as it would present an exceptionally high reporting burden, which is deemed disproportionate, especially given the difficulties that this option would also cause regulators.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable option suitable for shortlisting, alongside the 'do nothing' baseline. A 2022 consultation found support for this measure with 68% of respondents in favour of proposals to expand incidence reporting duties including 67% of organisations currently covered by NIS Regulations 2018.[29] Therefore, option 3 is the preferred option for taking this measure forward. This option has been taken forward to short list appraisal as it is effective, feasible and has a strong strategic fit. It was announced as part of the package of measures in the 2024 King's Speech.

5.6 Measures to strengthen information sharing provisions, such as by enabling regulators to share information with each other and public authorities, and vice versa

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the	Effectiveness - Does it improve the ability of regulators to fulfil their	Effectiveness – Does it ensure that the NIS Regulations themselves	Feasibility

[29] Proposal for legislation to improve the UK's cyber resilience - GOV.UK

		most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	duties in respect to the Network and Information Systems regulations?	are appropriate in an ever-changing cyber landscape?	
Option 1 - Do nothing	Low	N/A	Low	N/A	High
Option 2 – amendments to info sharing provisions	High	N/A	High	N/A	High

Option 1: Do nothing

The NIS Regulations 2018 include some provisions that enable information sharing to support the functioning of the regulatory regime. However, concerns have been raised by NIS regulators, industry and central government departments about whether these provisions are sufficient. There are significant ambiguities and limitations to the extent that data can be shared between key entities involved in implementing the NIS Regulations, informing associated policy (for example, on cyber resilience and national security) and evaluating the regulatory framework. Engagement with regulators has shown that a lack of legal clarity on sharing certain types of information with particular entities has put regulators at risk of legal challenge from regulated entities.

To do nothing would mean these shortcomings would remain, limiting the sharing of information that supports the effective functioning of the NIS Regulations. This means information required to ensure the NIS Regulations function properly and meet their objectives would not be shared across key actors in the regulatory regime. Regulated entities are reluctant to share information with regulators, and the government would not have the information required to get an accurate insight into the impact of the NIS Regulations, or a better understanding of the evolving threat landscape to best protect our national security and public services. There is also a risk of regulatory overlap and duplication if regulators cannot coordinate with other regulators outside of the NIS regime.

Option 2: Make targeted amendments to information sharing provisions in the NIS Regulations to address the shortcomings identified **(preferred option)**

This option seeks to make the four following changes to address the shortcomings in information provisions that have been identified, in order to improve the ability of regulators to fulfil their duties:

- Ensure NIS regulators can share information with UK public authorities (and vice versa) by explicitly referencing UK public authorities in the NIS Regulations;

- Expand the purposes for sharing information, to enable sharing between government and regulators to inform policy development related to the NIS Regulations and support their evaluation;
- Improve safeguards on how information can be used once it has been shared under the NIS Regulations by clarifying and restricting onward sharing provisions;
- Improve NCSC's access to information on RDSPs and RMSPs by requiring the Information Commission to share certain information more easily with NCSC. For example, the lists of registered RDSPs and RMSPs.

These changes would improve the effectiveness of NIS by providing greater certainty on what information can be shared, and by and with whom. They would ensure that UK public authorities and regulators have a clear mechanism to share information, which would ensure that the regulatory regime functions effectively. We deem this a feasible option for regulators because it will provide clarity on what information can be shared and via which pathways. Finally, there are safeguards on how the information would be used and shared onwards once it has been provided. This would give regulated entities confidence that once they have shared their information with regulators, their data is being protected, shared and used appropriately, and there are proportionate limits on how this data is shared onwards. These contained and targeted changes would strengthen information sharing provisions in the NIS Regulations whilst also ensuring safeguards are robust.

Information sharing is fundamental to the effective functioning of the NIS Regulations. All four changes are required under the measure to make holistic improvements to the current information sharing regime, whilst ensuring appropriate safeguards on how information is shared and used. They will improve the ability for regulators to access and exchange information to more effectively fulfil their duties. Government will have better access to information to inform policy development, and receiving greater information on RDSPs and RMSPs will support the NCSC to carry out its functions, such as providing more targeted support to regulated entities. Pursuing one or two of the changes outlined (rather than all four) would result in a limited set of changes, which would undermine the objectives in this space. Therefore, this option (with all four measures) has been carried forward to short list appraisal.

5.7 Measures to improve the Information Commission's information gathering powers

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility

		stability are in scope of?			
Option 1 - Do nothing	Low	N/A	Low	N/A	High
Option 2 – duty to provide certain info	High	N/A	High	N/A	Medium

Option 1: Do nothing

To do nothing, the Information Commission would have to rely on current information notice powers under regulation 15, or individual voluntary requests for information. This method of data collection, as well as the current scope under regulation 15, is considered insufficient to collect the data required to form an adequate picture of the risk. Without an adequate assessment of risk, the Information Commission is constrained to regulating cyber incidents reactively, rather than being able to be proactive in their regulatory functions to prevent and mitigate against attacks.

Option 2: Allow for a duty to require RDSPs and RMSPs to provide specific information to the Information Commission at registration, and allow the Information Commission to collect further information post-registration through Information Notices (INs) **(preferred option)**

This option would allow for a duty to require RDSPs and RMSPs to provide relevant information at registration, such as the type of service being provided and specific contact details, for the purpose of assessing risk.

As an example, RDSPs and RMSPs may be required to provide details such as company information regarding headcount and turnover, and customer information such as the sectors they supply – i.e. as whether they offer services through any government procurement frameworks and whether they supply CNI sectors. The requested information is basic and would not add any significant burden to organisations. This type of registration information is currently not in place; however, it is prevalent for other infrastructure and non-infrastructure businesses (e.g. telecoms providers' registration with Ofcom).

Additionally, the Bill would broaden the power for the Information Commission to request additional information after registration to determine risk through Information Notices.

The objective of this measure is to support the Information Commission to proactively identify cyber risks and take appropriate steps to prevent attacks. We deem this option to be an effective way to ensure the Information Commission can properly fulfil its duties under NIS. This option would enhance the Information Commission's capability to identify and mitigate cyber risks before they materialise, thus preventing attacks and strengthening the digital services sector against future threats.

This option has been taken forward to short list appraisal because it will be effective in improving the Information Commission's ability to fulfil its functions. By taking a proactive approach with RDSPs and RMSPs, this option is a strong strategic fit with the government's

objectives of protecting more digital services and supporting economic growth through a stable business environment.

5.8 Measures to improve regulators' cost recovery mechanisms

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	Low	N/A	Medium
Option 2 – expand recovery mechanisms	Medium	N/A	Medium	N/A	High
Option 3 – expand recovery mechanisms **and** enable recovery of enforcement costs	High	N/A	High	N/A	High

Option 1: Do nothing

Doing nothing would make no changes to the existing cost recovery provisions in the NIS Regulations, which allow for the recovery of specific costs associated with the regulation of individual entities but not the recovery of more general costs associated with the discharge of NIS regulatory functions, such as preparation of guidance or organisation upskilling, or the recovery of enforcement costs. It would likewise make no changes to the methods of cost recovery available to regulators, meaning that regulators will continue to rely on direct invoicing. Both of these aspects are undermining their ability to properly fulfil their roles.

Maintaining the status quo is feasible but not effective due to the rules around what activities' costs can and cannot be recovered.

Doing nothing will mean a continuing risk of non-compliance costs being passed unfairly to the taxpayer and constraints in regulators' ability to carry out their functions to their full extent. This is a poor strategic fit with the government's aims to reduce the cost of regulation for the taxpayer. The status quo leaves open an incentive for regulated entities to delay complying with actions required by regulators, where they anticipate that regulators may be constrained in their ability to undertake enforcement action. Again, this is a poor strategic fit for the government's objectives to strengthen the UK's cyber resilience.

Maintaining the reliance on direct invoices would also lead to an ongoing lack of clarity for regulated entities, who will be unclear whether they are to be charged and how much, and perpetuate the administrative burdens associated with invoice-based cost recovery mechanism for regulators.

Option 2: Expand the scope of existing cost recovery mechanisms to cover general NIS function costs but not enforcement costs, and create option for charging fees.

This option would enable regulators to recover general costs associated with the discharge of the NIS functions, such as costs associated with creating guidance or upskilling, while retaining the current exemption on recovering enforcement costs. Additionally, it would create options for regulators to recover those costs through charging fees instead of, or alongside, direct invoicing. This mechanism would require the regulator to develop a charging scheme, which they would consult upon with their regulated sector, and publish an end-of-period statement. This is feasible for the regulators because it is simpler and enables them to implement the most appropriate cost recovery regime for their sector.

This option would ensure that regulators were less reliant on other sources of funding for a greater proportion of their regulatory activities (albeit not enforcement activities) and would allow for greater certainty in how they approach and plan for the discharge of their duties. It would likewise reduce the likelihood of some costs being passed on to taxpayer, and – through the provision to charge fees – would also create more transparent and predictable regulatory environment for regulated entities. This option is therefore more effective in improving the ability of regulators to fulfil their duties, but only partly, as enforcement, a key duty of regulators, remains an activity unfunded by the sector itself.

This option would be an improvement on the 'do nothing' scenario in that it would ensure regulators are better resourced to fulfil their duties, but it would still mean that the costs of enforcement were not recovered. This is a detrimental omission, as it fails to address the risks of constraining the regulators' ability to discharge the full extent of their enforcement duties and the associated risks of costs being passed on to the taxpayer. It would also leave open the incentive of delayed compliance. This option is therefore an improvement to the strategic objectives of the government but, due to the fundamental issue of enforcement costs not being addressed, we have not carried it forward to a short list appraisal.

Option 3: Expand the scope of existing cost recovery mechanisms to cover general NIS function costs and enforcement costs; and create option for charging fees **(preferred option)**

This option would enable regulators to recover all the costs associated with the discharge of NIS functions, including the costs of enforcements activities and the other general regulatory

costs that are currently excluded, and would create options for regulators to recover those costs through charging fees rather than direct invoicing. It is vital that recovering enforcement costs is included in the shortlisted option. Without it, regulators would not be incentivised or indeed able to recover costs from enforcing the NIS Regulations. Without effective enforcement, compliance with the NIS Regulations may be limited, which could affect the implementation of cyber resilience for essential and digital services. This option is considered to align with the government's stated cyber objectives.

This option would most effectively and comprehensively enable regulators to fulfil their duties. It would enable regulators to have certainty about how they will fund all of their NIS-related regulatory activities, including enforcement, and would eliminate the need for costs to be passed on to the taxpayer through reliance on public funding, making it a strong strategic fit for the government's objectives. The mechanism would also be more transparent and predictable for regulated entities, and protected by safeguards whereby fees can only cover costs associated with their duties relevant to the NIS Regulations, and regulators cannot make a profit. Additionally, while it will lead to additional costs being borne by the regulated entities due to the inclusion of enforcement costs, this would be offset by the enhanced transparency and predictability of the charging of fees. It is feasible for regulators, who would have discretion to assign costs to regulated entities in a proportionate way which is most suited to their sector through the methodology underpinning their fees – for example, by tailoring to turnover.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable option suitable for shortlisting, alongside the 'do nothing' baseline. Therefore, option 3 is the preferred option for taking this measure forward. This option has been taken forward to short list appraisal due to its feasibility, effectiveness is ensuring regulators can fulfil their duties and strong strategic fit with the government's objectives of reducing regulatory burden on the taxpayer. It was also announced as part of the package of measures in the 2024 King's Speech.

5.9 Measures to enable government (Secretary of State) to designate a statement of strategic priorities

Policy Option	Strategic fit	Effectiveness - Does it appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility

Option 1 - Do nothing	Low	N/A	Low	N/A	High
Option 2 - Statement of Strategic Priorities	High	N/A	High	N/A	Medium

Option 1: Do nothing

Doing nothing would not be effective in ensuring regulators fulfil their duties consistently across NIS sectors. Implementation of the NIS Regulations by regulators has been inconsistent in approach. For example, regulators have mandated different cyber assessment tools and different frequencies of cyber assessments, despite the NCSC's advice that regulators should be using the Cyber Assessment Framework as the basis for guidance issued to regulated entities. Regulators have also had varied consistency in enforcement, with some regulators taking a more proactive approach as advised by DSIT, and other regulators continuing with a more reactive approach. The inconsistency of NIS enforcement means that different sectors adopt different security measures and have different degrees of protection against malicious cyber activity. Maintaining the status quo is therefore a poor strategic fit with the government's objectives for cyber, such as proactive implementation of the recommended guidance. Efforts by DSIT and NCSC to resolve these problems by issuing guidance and creating fora to collaborate have been unsuccessful, as the guidance is discretionary and may therefore be disregarded. As such, we do not believe further discretionary guidance is an effective solution.

Option 2: Grant the Secretary of State the power to designate a 'statement of strategic priorities' **(preferred option)**

The failure of discretionary guidance to guarantee consistency of approaches across sectors, as described above, suggests that there is a need for a direct and specific intervention from government to ensure the consistency and effectiveness of enforcement. The statement of strategic priorities would detail objectives which the regulators would have a duty to seek to achieve. This would provide better consistency in approach between regulators and sectors, as all would be required to work towards the same outcomes, and aligns with the government's overall approach to ensuring regulators are aware of government priorities and therefore able to service them effectively. This option is therefore a strong strategic fit as it allows government to set the direction for regulators, ensuring consistency and alignment with broader government objectives.

To maintain regulatory autonomy, statements of strategic priorities would be drafted in consultation with the regulators, and regulators would be free to seek to achieve the objectives in whichever way they thought was most appropriate. The current policy aim is for statements of strategic priorities to be produced every three to five years to provide regulators a long enough timeline to plan effectively. These processes will ensure the statement is feasible for regulators to implement. The Bill will allow the statement to be amended within

the three-year period where necessary, to ensure the statement is relevant and workable for regulators in a fast-moving environment. To provide opportunity for public scrutiny, the Secretary of State would be required to publish an annual report on steps taken toward the goals of the statement of strategic priorities, and may request information from the regulators to inform this.

Further long list options are not possible in this measure as it is a binary decision. Option 2 has been taken forward to short list appraisal alongside the 'do nothing' option because it is a strong strategic fit and will enable the regulators to fulfil their duties effectively and consistently. The requirements to consult and fair implementation periods will ensure the options is feasible for the regulators expected to adhere to the statement of strategic priorities.

5.10 Measures to strengthen the enforcement mechanisms in the NIS Regulations

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	N/A	Low	Medium
Option 2 – Introducing a new fine maximum	Medium	N/A	N/A	Medium	Medium
Option 3 – Introduce a new fine maximum and simplifying the penalty bands	High	N/A	N/A	High	High

Option 1: Do nothing

Doing nothing will maintain the sanctions regime under the NIS Regulations, which regulators report to be ineffective. This was highlighted in the PIR, where it was outlined as an area for a future consideration, noting the limitations in the grounds for enforcement, overall lack of clarity around the sanctions regime, and restrictions to the use of regulatory powers. These reports have since been further substantiated by internal assessments of the NIS enforcement and sanctions regime.

An effective sanctions regime is one that is meaningful, proportionate and enforced with confidence and certainty. Currently, we consider that the financial penalty levels are disproportionate to the emerging cyber risk landscape and are too low to deter non-compliance across all NIS sectors. In some sectors, the maximum penalty can be cheaper than the cost of compliance, with £17m representing less than 1% of the annual turnover of regulated organisations. This disincentivises large companies from complying. When compared to the substantial impact a failure could have on the economy and society, such penalty levels fall behind comparable regimes, and do not offer sufficient deterrent effect. We also know that fines are not confidentially enforced. The 2022 PIR showed that no fines had been levied by regulators since the Regulations came into effect in 2018. Since then, through engagement with regulators, we know that very few fines have been levied and the issues highlighted in the PIR persist.

Doing nothing would maintain the existing maximum fines, leading to less deterrence across sectors in the long-term and creating no further incentives to increase cyber resilience of vital services that the UK economy and society relies on. We consider that this option would lead to a regime that is less effective, and reduce the ability for regulators to address critical risks in our nation's infrastructure, as it will not increase deterrence, especially in circumstances where the cost of compliance is higher than the potential sanction. It would potentially allow regulated organisations to absorb the cost of a fine as 'the cost of doing business' and provide no additional incentives to comply. In this sense, both individual deterrence (in the sense of lowering repeat contraventions) and public deterrence (understood as the overall incentive to comply across the sectors) will not increase, and the overall success of the regime could stagnate or be lowered in the long term.

The current penalty band structure is also unclear, which means that regulators are not enforcing penalties in a confident and consistent manner, and regulated entities do not have the necessary clarity and transparency to be able to predict potential sanctions for non-compliance. In particular, the current requirement to determine penalties in relation to the impact, or the potential impact, of breaches on the continuity of services does not provide a sufficient indication of how fines would be levied, and introduces unnecessary complexities and costs for both regulatory authorities and regulated entities. As this option would not encourage compliance and consistent enforcement penalties, it would be a poor strategic fit for the government's objectives for an effective and transparent regulatory regime.

Option 2: Amending fine maximum only, with no reforms to the penalty structure

This option would enable regulators to issue higher penalties by amending the maximum fine level to include a measure based on percentage turnover. Under the current regulations, authorities are able to issue a financial penalty only up to £17 million, which represents a small proportion of turnover for large entities. This means that regulated entities are more incentivised to accept financial penalties as the cost of doing business, and the regime is not equipped to address non-compliance, especially in circumstances involving intentional or malicious breaches.

Enabling regulators to issue higher penalties based on percentage turnover would serve to shift the cost-benefit analysis towards compliance and clearly signal the societal and normative expectations for compliance for services that are critical to the UK economy and society. It would create a stronger deterrence effect, which we expect would directly contribute to the success of the regulatory framework and the policy objective of managing risks to national infrastructure and vital services. At the same time, it would reduce the likelihood of excessive fines for smaller organisations by calibrating fines in relation to turnover.

This option, however, does not include reforms to the penalty structure, which would maintain substantial limitations in the legislation, and makes the enforcement of financial penalties much more onerous and subject to interpretation. This increases the likelihood of unnecessary litigation and provides little clarity for regulated entities in terms of what consequences may follow non-compliance. It is generally accepted that an effective sanctions regime is comprised of three aspects: proportionate to the offence, the confidence with which the sanction is applied and the swiftness of the enforcement. As this option increases severity of the regime, but without also addressing the challenges in the structure of the framework (which would be concerned with making the regime more certain and swifter), it would only have medium impact in creating an effective sanctions framework.

Option 3: Amending the fine maximum and simplifying the penalty bands **(preferred option)**

This option would involve simplifying and rationalising the three-band penalty structure under the NIS Regulations, alongside amending the fine maximum fine to include a measure based on a percentage of turnover. It would address the lack of clarity associated with the current band structure by creating two new penalty bands with clearly defined parameters, and with all significant contraventions subject to the higher tier of penalties (one of the problems with the current penalty band test).

This option would deliver the most effective enforcement regime by simultaneously enhancing the proportionality of fines and the confidence and certainty with which they are applied. It would give regulators greater confidence and clarity in issuing penalties at the appropriate level for specific contraventions, meaning that it is more feasible that they will take meaningful enforcement actions, while simultaneously enhancing the incentives for regulated entities to comply with the regulations by enabling higher maximum penalties, thereby driving up security and resilience standards across the UK's most important services.

This option therefore represents the best strategic fit for the government's objective to strengthen the UK's cyber resilience through strong and effective enforcement mechanisms. While Option 2 puts in place of one of the key conditions for effective enforcement, this is the only option which comprehensively addresses the limitations of the current enforcement regimes and ensure that penalties will be applied in an effective, predictable and consistent manner.

Measures to ensure that the NIS Regulations keep pace with the ever-changing cyber landscape and equip government to take decisive action to protect our national security

5.11 Measures to allow the government to update the NIS Regulations without an Act of Parliament

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	Low	Low	Low	High
Option 2 – non-legislative	Low	Low	Low	Low	Medium
Option 3 – proportionate delegated powers	High	High	High	High	Medium

Option 1: Do nothing

Doing nothing would restrict the government's ability to update the regulatory framework in a way that keeps pace with changing threats and ensure the regime remains effective. This would leave the UK exposed to changing and emerging cyber threats, and behind international counterparts.

The cyber threat has evolved and the subsequent issues have not been addressed, as set out in Section 2 of this impact assessment. For instance, market forces and voluntary guidance has not effectively increased the cyber security of essential and digital services enough to reduce the threat it poses to business confidence, the economy, and the ongoing provision of services the public rely on every day, as can be seen in the case of MSPs. While these sectors are often governed by the General Data Protection Regulations (GDPR), this has only increased the security around personal data, and not for the systems that relate to the operation of the essential services.

This option is a very poor strategic fit with the government's objectives of ensuring our cyber security and resilience can tackle the threats facing our national security and essential services.

Option 2: Encourage better cyber practices by a wider pool of organisations through guidance and other non-legislative means

This approach has proven to be ineffective thus far. OESs and RDSPs often do not have a comprehensive understanding of the costs or benefits of cyber security to their operations. As a result, investment and voluntary action to improve cyber security and resilience is often deprioritised.

Recent reports highlight the continuing level of cyber resilience of businesses operating across the UK. In 2024, while seven in ten large business (70%) had a formal cyber security strategy in place, significantly fewer medium businesses (57%) had a formal cyber security strategy in place.[30] Fewer businesses are deploying security monitoring tools (30% in 2024[31] vs. 33% in 2023[32]), while the percentage of businesses undertaking any form of user monitoring (30%[33] [34]) is unchanged. This only highlights the necessity for government intervention for the regime to remain effective and fit for purpose.

HMG provides general guidance to help drive better cyber security practices amongst industry. Industry guidance (such as the NCSC's Cyber Essentials) is largely not tailored to specific sectors and industry can apply the guidance as best for their organisation. It also does not provide advice for specific threats for a certain sector.

The NIS Regulations apply to designated sectors and regulators work collaboratively with regulated entities to assess their security of network and information systems, their vulnerabilities, and provide specific advice to manage and mitigate those risks. If a sector would be deemed to be important enough to merit inclusion in the NIS Regulations, then generic guidance without active supervision and tailored advice is not sufficient. Due to the high cost of implementing some of the cyber security improvements, firms are unlikely to act on guidance alone, even if it was sector-specific. Therefore, a non-regulatory approach is not viable if we truly are committed to protecting British consumers from the disruption of their essential services. Therefore, this option has not been carried forward for short list appraisal.

Option 3: Introduce delegated powers with appropriate safeguards to ensure the NIS Regulations can remain relevant and effective **(preferred option)**

This measure would enable the government, after any appropriate consultation, to update the regulatory framework without requiring an Act of Parliament. This would allow the regulations to bring more entities into scope and improve the ability for regulators to fulfil their duties by updating their functions and duties. In turn, this would enable the NIS Regulations to remain relevant to the evolving cyber threat. These powers would be subject to certain restrictions and safeguards. For example, they would be limited to ensure that amendments operate within specific boundaries related to the regulation of services that are critical to the functioning of the UK economy or society. The powers may be used to make changes such

[30] Cyber Security Breaches Survey 2025
[31] Cyber Security Breaches Survey 2025
[32] Cyber Security Breaches Survey 2024
[33] Cyber Security Breaches Survey 2025
[34] Cyber Security Breaches Survey 2024

as introducing new requirements and duties for regulated entities and making changes to the responsibilities and functions of NIS regulators. The Bill also allows for the publication of a Code of Practice, which will set clear guidelines and good practice to follow, to support regulated entities in scope to comply with requirements imposed by the regulations.

The EU has also identified that more sectors need to be covered by the NIS Regulations. In the implementation of their NIS 2 Directive, the EU has extended the sectors under the NIS Regulations to include eight additional sectors. This shows that, internationally, countries are recognising the growing threat to other sectors, making this option a strong strategic fit and consistent with approaches taken internationally. Delegated powers in the Bill would allow the UK to expand the application of the NIS Regulations in the future, if there is a strong case to do so.

In the 2022 consultation, the majority (88%) of respondents agreed with the UK government having the power to amend certain elements of the NIS Regulations through secondary legislation, and in addition the majority (81%) of respondents agreed with the government's proposal for a delegated power that would allow the government to amend the NIS Regulations to add new sectors.[35]

This option best ensures that the government can react quickly to address any market failures, making it a strong strategic fit with the government's objectives to strengthen the UK's cyber resilience against hostile actors. This option has therefore been taken forward for short list appraisal.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable option suitable for shortlisting, alongside the 'do nothing' baseline. Therefore, option 3 is the preferred option for taking this measure forward.

5.12 Measures to enable government to update Security and resilience requirements in the regulatory framework

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility

[35] Government response to the call for views on proposals to improve the UK's cyber resilience - GOV.UK

		stability are in scope of?			
Option 1 - Do nothing	Low	N/A	N/A	Low	Medium
Option 2 - Security and resilience requirements	High	N/A	N/A	High	Medium

Option 1: Do nothing

The NIS Regulations set out minimum security requirements for RDSPs to meet in order to increase their cyber resilience. There is a strong indication from the PIR that, without NIS, cyber security improvements across digital and essential services in the UK would have proceeded at a much slower pace.[36] However, under the current NIS Regulations, we are unable to update security requirements and adapt these to new and upcoming threats and vulnerabilities. This leaves the UK with security requirements which prioritise minimised regulatory burdens on organisations in scope, but may not sufficiently tackle the cyber threats facing the UK in 2025. This option is therefore ineffective in ensuring the NIS Regulations are appropriate in an ever-changing landscape. This also poses the risk of the UK falling behind international precedent, including the EU, making it a poor strategic fit with international progress.

Option 2: Grant the Secretary of State powers to update security and resilience requirements via secondary legislation **(preferred option)**

This option would provide Secretary of State with the power to update the security and resilience requirements via secondary legislation. This was previously referred to as technological and methodological security requirements, with the name changed to security and resilience requirements providing stakeholders with a clearer understanding of their purpose. The Secretary of State would be provided with powers to:

- Set security requirements by regulation that would apply to RDSPs; and
- Extend these requirements beyond RDSPs, if appropriate and proportionate.

These requirements would enable the government to update the existing security requirements for RDSPs. One option would be to use the power to adjust the security requirements to reflect elements of the Cyber Assessment Framework Basic Profile, which sets baseline expectations around, for example, cyber governance, asset management, risk management and incident response. The CAF is an effective, outcome-based risk assessment tool which relies on tailored advice to operators in scope. It has allowed for the regulators to review an organisation's cyber security arrangements and ensure appropriate actions are in place, improving plans that have effectively reduced the vulnerabilities in key organisations' systems and could have otherwise been exploited. These requirements could build on the existing security requirements already outlined in NIS for RDSPs, while reflecting elements of the CAF Basic Profile and aligning, where appropriate, with the security

[36] Second PIR of the Network and Information Systems Regulations 2018 - GOV.UK

requirements set out in the EU NIS 2 regulations for all regulated entities. This option is therefore a strong strategic fit with international precedent.

Granting powers to set security and resilience requirements via regulations would be effective in enabling the current NIS Regulations to be more flexible and adaptable to the ever-changing cyber environment and new threats, allowing for amendment against future threats.

Option 2 has been carried forward to short list appraisal because of its effectiveness in ensuring the regulations remain appropriate and a strong strategic fit.

5.13 Measures to improve supply chain security

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	N/A	Low	High
Option 2 – voluntary guidance	Low	N/A	N/A	Low	Medium
Option 3 – supply chain duties	High	N/A	N/A	High	Medium

<u>Option 1: Do nothing</u>

The supply chains for our essential services are becoming increasingly complex and vulnerable to cyber attacks. Suppliers are an attractive target for malicious actors who can take advantage of weaker security somewhere in an organisation's supply chain, and cause huge disruption for an essential service without attacking the essential service itself. Despite the risk, last year just over one in ten businesses said they reviewed the risks posed by their immediate suppliers (14%), and under one in ten were looking at their wider supply chain

(7%).[37] This was higher for large businesses, with 45% looking at their immediate suppliers and 25% at their wider supply chain, but still insufficient to address the risks posed by vulnerabilities in large supply chains and the impact this can have on customers and service users. Doing nothing would not address these issues and would be a poor strategic fit with the government's objectives of strengthening the cyber resilience of supply chains to protect essential and digital services.

Doing nothing would be feasible, avoiding additional regulatory burden on OESs and RDSPs, allowing them to continue their operations without additional compliance costs or administrative requirements. However, it also means that the vulnerabilities and risks associated with supply chains would not be addressed and the NIS Regulations would not be appropriate for the level of cyber threat, leaving them susceptible to cyber threats and other security incidents. This could have broader implications for the security and resilience of essential services and CNI and, by extension, the people who use these services.

Option 2: Voluntary guidance

NCSC already provide a range of world-class voluntary guidance on supply chain security, which can be used by OESs and RDSPs as well as by suppliers. This includes voluntary cyber standards and products such as the Cyber Assessment Framework and Cyber Essentials.

This option would come at little cost to government and regulators, so it is feasible. The government recognises voluntary guidance, and cyber standards have not been sufficient to address the increasing security and resilience risks associated with the supply chain. This option would likely lead to uneven standards across the industry with some firms following guidance and others not, preventing a 'level playing field' from being established. This is therefore a poor strategic fit with the government's objectives of strong, consistent cyber regulations for essential and digital services. This option has therefore not been carried forward to short list appraisal.

Option 3: Enable the government to set stronger supply chain duties for OESs and RDSPs in secondary legislation, subject to consultation **(preferred option)**

By setting clear expectations on OESs and RDSPs to identify and manage supply chain security through enforceable duties, we expect to see greater levels of compliance across the supply chain than with voluntary guidance. The government's view is that a purely voluntary approach would see limited compliance with recommended measures, as has been evidenced by inconsistent levels of compliance with discretionary advice issued by the NCSC up to now.

This option would be effective in ensuring the NIS Regulations are appropriate for the increasing threat of unsecure supply chains. Enforceable expectations, set out in regulations, would drive improved use of contractual arrangements, enabling OESs and RDSPs to holistically manage risks across their broader supply chains. This should be feasible for OESs and RDSPs, who have the best understanding of their own supply chains and where vulnerabilities might be.

However, we recognise that certain critical supply chain risks, such as those arising from concentrated dependence on a small number of suppliers, may exceed what individual OESs

[37] Cyber security breaches survey 2025 - GOV.UK

or RDSPs can reasonably manage independently. In such scenarios, measure 5.4, which focuses explicitly on designating critical suppliers, should be employed. Measure 5.4 allows regulators to directly address vulnerabilities associated with these critical suppliers by bringing them within the scope of the NIS Regulations.

Together, these complementary measures will strengthen overall cyber resilience by both enhancing supply chain risk management practices and specifically targeting the most critical risks through regulatory designation.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 3 has been identified as the only viable option suitable for shortlisting, alongside the 'do nothing' baseline. Therefore, option 3 is the preferred option for taking this measure forward. Option 3 has been taken forward to short list appraisal due to its effectiveness in keeping the NIS Regulations appropriate, strong strategic fit (especially when taken together with measure 5.4) and feasibility for OESs and RDSPs.

5.14 Measures to enable the government to direct regulators, where necessary and proportionate in the interests of national security

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	Low	N/A	Medium
Option 2 – power to direct regulators, excluding government	High	N/A	High	N/A	Medium
Option 3 – power to	High	N/A	High	N/A	Low

direct all regulators					

Option 1: Do nothing

This option leaves the government unable to require regulators to respond to sudden changes in the threat environment which expose network and information systems of NIS-regulated entities to higher levels of risk. The current system requires regulated entities to undertake 'appropriate and proportionate' measures to secure themselves against cyber threats, and regulators issue guidance to their sectors to help them interpret this duty. However, the government lacks the ability to ensure that regulators update their guidance to reflect specific measures that could be necessary at times of heightened national security risk. Additionally, regulators do not have the same level or speed of access to vital intelligence as the government, which could hamper their ability to respond to imminent threats. This makes doing nothing less feasible for regulators. This creates national security vulnerabilities due to unmitigated risks of cyber disruption of the services provided by regulated entities. This option is a very poor strategic fit with the government's priority of strengthening national security and responding decisively to protect the public.

Option 2: Grant the Secretary of State the power to issue directions to regulators outside of government **(preferred option)**

This option ensures that the government can respond at pace to threats and incidents which pose risks to national security. Where action needs to be taken across one or more sectors, it would not be feasible to draft, issue, and monitor compliance with the required number of individual directions to regulated entities. It is therefore more feasible to issue a direction to a regulator, requiring them to update guidance for their sectors to reflect the heightened threat landscape.

This power would only be able to be used where necessary for national security, and where the impact of a direction is deemed to be proportionate. For example, following the Russian invasion of Ukraine in 2022, the government may have considered issuing a direction to regulators to update their guidance to encourage regulated entities across NIS sectors to take the action needed to respond to the heightened threat environment. This option is a strong strategic fit with the government's national security objectives.

We do not anticipate for this power to be used by the Secretary of State on a frequent basis, which means it is a feasible option for regulators. Directions would likely be informed by information from the NCSC, ensuring that sectors adopt the right measures to mitigate national security risk. This intelligence from government will enable regulators to fulfil their duties effectively.

This power would be limited so that it was not able to be used to direct a Minister of the Crown or a devolved government.

Option 3: Grant the Secretary of State the power to issue directions to all regulators

As with Option 2, this option ensures that the government can respond at pace to threats and incidents which pose risks to national security. Enabling the Secretary of State to issue directions to all regulators, including those that sit in government, would in theory provide a

greater ability to respond to a wider range of threats. However, this option is not feasible, as one Secretary of State cannot direct another Secretary of State to undertake specific actions. We also do not think that it would be feasible for the Secretary of State to direct a devolved government.

Option 2 has been carried forward to short list appraisal because of its very strong strategic fit with government objectives.

5.15 Measures to enable the government to direct regulated entities, where necessary and proportionate in the interest of national security

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness – Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Option 1 - Do nothing	Low	N/A	N/A	N/A	High
Option 2 – power to direct all regulated entities	High	N/A	N/A	N/A	Medium
Option 3 – power to direct only OESs	Low	N/A	N/A	N/A	Medium

Option 1: Do nothing

The NIS Regulations 2018 require entities in scope of the regulations to undertake 'appropriate and proportionate' measures to manage cyber security risks affecting their networks and systems. While regulated entities are under a duty to instate appropriate and proportionate measures to protect themselves against cyber risks, those measures are not always sufficient to protect the entities from sophisticated cyber attacks. Successful cyber attacks targeting regulated entities, particularly OESs, have profound impacts with implications for the UK's national security. In its annual review in 2024, the NCSC described

the cyber threat landscape faced by the UK as 'diffuse and dangerous.'[38] It noted that the number of cyber incidents was increasing, as was the impact of those incidents. The review also noted that nation state actors were increasing malicious activity targeting NIS sectors in the UK.

Doing nothing would leave the government unable to compel a NIS-regulated entity to respond to cyber threats and incidents relating to their network and information systems, even where this was judged to be essential for safeguarding national security. The growing threat posed by high-capability actors and hostile states means that it is more likely that this gap that could be exploited, leading to worsening disruption caused by malicious activity, putting the operation of the UK's CNI at risk. This option is a very poor strategic fit with the government priority of strengthening national security and responding decisively to protect the public.

Option 2: Grant the Secretary of State the power to issue directions to regulated entities **(preferred option)**

In light of the growing cyber security threat affecting the UK, this option addresses the existing national security vulnerability by ensuring that the government can respond at pace to threats and incidents affecting regulated entities. This option is a very strong strategic fit with the government's objectives of protecting the essential and digital services that the public rely upon every day. This power would only be used where necessary for national security, and where the impact of a direction is deemed to be proportionate. We do not anticipate for this measure to be used by the Secretary of State on a frequent basis as the power is designed to be used only in response to specific cyber security threats and where it is necessary for the UK's national security. This ensures that it is feasible for regulated entities. Directions would likely be informed by information from the NCSC.

Option 2 has been carried forward to short list appraisal because of its very strong strategic fit with government objectives.

Option 3: Grant the Secretary of State the power to issue directions only to OESs

This option would have similar implications to the preferred option, granting power to the Secretary of State to direct OESs to take action to address national security threats and incidents. However, this option would exclude RDSPs, RMSPs and designated critical suppliers. By targeting only the OESs, this option would significantly undermine the policy objective of mitigating national security risks, as threats to RDSPs, RMSPs and designated critical suppliers could reasonably risk disruption to OESs and therefore restrict the power it intends to grant. It is therefore a poor strategic fit with the government's priorities of protecting essential and digital services.

We do not recommend this option as it would restrict its intended power and ultimately would fail to address the need to intervene effectively on cyber threats of national security. It has therefore not been taken forward for short list appraisal.

After evaluating the long list of options against the critical success factors, as summarised in the above table, option 2 has been identified as the only viable option suitable for shortlisting,

[38] Annual Review 2024

alongside the ‘do nothing’ baseline. Therefore, option 2 is the preferred option for taking this measure forward.

6. Description of shortlisted policy options carried forward

Shortlisting using Critical success factors

As set out in the previous section, a long list of potential reform options was generated in each area where possible, with each option designed to tackle an identified issue. These were then assessed against the agreed critical success factors to shed light on their strategic fit, likely effectiveness and feasibility. This analysis left one viable intervention option under each area, which when taken together constitute the preferred option which has been taken forward to short list appraisal below. The ‘do nothing’ option has also been carried forward for short list appraisal, which is standard practice in options appraisal. However, as explained below, this is not the preferred option.

Option 1: Do nothing

Under the ‘do nothing’ scenario, the NIS Regulations 2018 are left unchanged in the UK from how they currently stand. It is a weak strategic fit with the government’s objectives to strengthen the cyber resilience of essential and digital services and protect the UK’s national security. This scenario acts as the counterfactual to the preferred option.

Under this option there would be insufficient powers to update the NIS Regulations and bring new entities and sectors into scope without primary legislation, making this option ineffective in ensuring the NIS Regulations remain appropriate in an ever-changing cyber landscape. In this scenario, whilst the EU progresses with NIS 2 and brings new entities into scope, and Australia updates its laws to include designation of critical supply chains, the UK would fall behind international partners on cyber security regulation. This makes option 1 a weak strategic fit with international precedents.

Hostile cyber activity in the UK has grown more intense, frequent, and sophisticated, with tangible impacts on public safety, the economy and national security. Without change to the NIS Regulations, cyber attacks are likely to cause more frequent disruption and operational downtime. This would be harmful for both the competitiveness of individual companies and for the overall business environment.

Furthermore, vulnerabilities in supply chains would continue to be exploited, harming UK citizens. In this scenario, the UK would continue to be insufficiently protected from cyber attacks similar to the 2024 ransomware attack on a key NHS supplier, which led to over 11,000 postponed outpatient appointments and elective procedures. Market power imbalances between OESs and ‘critical suppliers’ mean that this cannot be resolved through contractual means. As supply chains expand and become more complex, this gap in the NIS Regulations would become more likely to be exploited by hostile actors.

Without updating the NIS Regulations, the UK's national security would continue to be vulnerable to state sponsored threat actors. The NCSC's Annual Review 2024 describes the threat landscape as 'diffuse and dangerous', with persistent attacks from hostile states and organised crime.[39] The NIS Regulations 2018 are already outdated for the cyber threats faced by the UK today, and this vulnerability would only worsen as cyber criminals continue to develop their methods.

Option 2: Primary legislation

The preferred option is the primary legislation package of preferred option reforms outlined in section 5. This set of options is expected to meet the Government's objectives of increasing cyber resilience and future proofing the NIS Regulations 2018 in an ever-changing cyber environment, whilst maintaining an environment that is not overburdensome to businesses and essential services. Going forward in this impact assessment, the costs and benefits of the preferred option are assessed compared to the baseline 'do nothing' scenario. The table below shows how the two short list options perform against the critical success factors.

Table 6.1: Ranking of packages against CSFs

Policy Option	Strategic fit	Effectiveness - Does is appropriately ensure that entities vital to protecting the most critical national infrastructure which the public rely on and underpin economic stability are in scope of?	Effectiveness - Does it improve the ability of regulators to fulfil their duties in respect to the Network and Information Systems regulations?	Effectiveness– Does it ensure that the NIS Regulations themselves are appropriate in an ever-changing cyber landscape?	Feasibility
Do nothing	Low	Low	Low	Low	High
Primary legislation	High	High	High	High	High

[39] Annual Review, NCSC, 2024

7. Net Present Social Value (NPSV): monetised and non-monetised costs and benefits of each shortlist option (including administrative burden)

Costs

Table 7.1: breakdown of the costs by measure

Costs, Present Value, 2025, central estimate £m	Measure	Monetised? Non-monetised? Both?	Direct? Indirect? Both?	Followed by secondary legislation?
£796m	1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations.	Monetised	Direct	No
£149m	2. Bring data centre infrastructure into scope of the NIS Regulations.	Monetised	Direct	No
£40m	3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations.	Monetised	Direct	No
N/A	4. Enable regulators to designate critical suppliers.	Non monetised	Direct	Yes
£201m	5. Improving incident reporting.	Monetised	Direct	Yes
N/A	6. Strengthen information sharing provisions, such as by enabling regulators to share information with each other and public authorities, and vice versa.	Non-monetised	Direct	No
N/A	7. Enabling the Information Commission to collect information related to risk.	Non-monetised	Direct	No
N/A	8. Improve regulators' cost recovery mechanisms.	Non-monetised	Direct	No

N/A	9. Enable SoS to designate a statement of strategic priorities.	Non-monetised	Direct	No
N/A	10. Strengthen enforcement mechanism	Non-monetised	Direct	Yes
N/A	11. Delegated powers – ensure the regulatory framework is adaptable to emerging threats.	Non-monetised	Direct	Yes – in the future if needed
N/A	12. Security and resilience requirements.	Non-monetised	Direct	Yes
N/A	13. Enable government to improve supply chain security.	Non-monetised	Direct	Yes
N/A	14. Introduce a power for the SoS to direct a regulator, where it is necessary for national security.	Non-monetised	Direct	No
N/A	15. Introduce a power for the SoS to direct regulated entities, where it is necessary for national security.	Non-monetised	Direct	No

Wider Impacts

Table 7.2: breakdown of the wider impacts by category

Wider impacts £m	**Category**	**Monetised? Non-monetised? Both?**	**Direct? Indirect? Both?**
N/A	Small and micro enterprises (SMEs)	Non-monetised	Indirect
N/A	Small and Micro Business Assessment for data centre operators	Non-monetised	Indirect
NA	Impact on competition	Non-monetised	Indirect
N/A	Impact on equalities	Non-monetised	N/A
N/A	Impact on individuals	Non-monetised	N/A
N/A	Environmental impacts	Non-monetised	N/A
N/A	National Security impacts	Non-monetised	Direct
N/A	Sectoral impacts	Non-monetised	Indirect

N/A	Impact on trade	Non-monetised	Indirect

Despite the negative NPSV associated with some measures, significant non monetised benefits have been identified which centre on the expected reduction in the prevalence and impact of cyber attacks in comparison to the 'do nothing' option. This benefit will occur through bringing more entities in scope of the NIS Regulations, improving the enforcement of the regulation and facilitating greater sharing of information.

Assumptions, risks and methodology

The preferred package of reforms has been analysed and estimates of the potential costs and benefits can be found below. These are assessed over a period of 10 years from 2026 to 2035 and are discounted using the Green Book's suggested discount rate of 3.5%.

Where analysis has already been published for particular policies included in the Bill, this is referenced accordingly. This IA focusses on the additional impacts of these specific measures and does not assess the existing costs arising from the NIS regulations already in force.

The expected impact of the policies primarily will be on the organisations brought into scope of the NIS Regulations, the regulators tasked with implementing NIS, as well as the public who use the services of those regulated under NIS.

Where sufficient robust data is available, DSIT has estimated the monetary impact of the various reforms. Where this evidence is not yet available, DSIT has provided an in-depth outline of the potential costs and benefits and ensured that any evidence gaps will be addresses prior to relevant secondary legislation, or referenced in our monitoring and evaluation plan which can be found at the end of this impact assessment.

Due to the nature of the cyber area, evidence on the monetised benefits is currently limited. This section begins by looking at the direct non-monetised benefits of implementing the package of reforms when compared to the 'do nothing' option. This has initially been done qualitatively and with the help of relevant case studies that illustrate expected benefits. Some quantification to indicate the potential scale of benefits has also been provided.

The Bill will strengthen the cyber defences of essential and digital services and build resilience in the face of increasing and emerging threats to the UK which is essential for protecting long-term growth and the UK's national security. By setting clearer security standards and expectations, the Bill increases the UK's resilience to cyber incidents, reducing the costs incurred as a result of cyber attacks when compared to the 'do nothing' option. SMEs who might otherwise struggle to meet evolving threats may particularly benefit from the reforms.

An overview of the direct and indirect costs that could be faced by UK businesses and regulators as a result of these policies has been provided in the 'Costs' section.

8. Benefits

Summary – Do nothing option

The ‘do nothing’ option represents a continuation of business as usual and therefore does not provide any additional direct or indirect benefits.

Summary – Option 1

1. Direct benefits:
    a. Non-monetised:
        i. Security benefits
        ii. Reduce impact from cyber attacks
    b. Quantified
        i. Illustrative breakeven analyses
2. Indirect benefits
        i. Competition benefits

Direct benefits

Non-monetised

A secure and robust environment in which businesses can operate without fear of devastating cyber attacks is essential to economic growth. That is why, when compared to the ‘do nothing’ option, a key benefit of this Bill is to protect businesses from cyber attacks to foster an environment in which investment and innovation can thrive. Having better defences against cyber attacks, achieved by bringing more entities into scope and empowering regulators to better fulfil their duties, will reduce the time businesses must take to deal with cyber attacks, often halting their services to do so. When an attack does occur, improved incident reporting will allow regulators and NCSC to use this information to provide advice and guidance to, and to engage with, other businesses and organisations. This will enable them to take action to protect themselves and mitigate the wider impacts of the specific attack or type of attack.

More specifically, the measures together have the benefit of addressing the key market failures identified earlier in this impact assessment:

- **Externalities** – measures to improve the way the regulation is enforced, to bring more entities in scope and to update the standards set out in regulation will together have the benefit of reducing the prevalence and impact of cyber attacks and their spillover effects across the economy.
- **Imperfect information** – measures to enhance sharing of information across regulated entities and the government/regulator will reduce imperfect information, including information asymmetry, in the market, again improving security.
- **Coordination failure** – measures to bring more relevant entities into scope and encouraging information sharing, ensuring that a greater proportion of the network has heightened security.

It has not been possible to monetise the expected benefits of the Bill, but benefits have been explained qualitatively with the use of case studies, and indicative quantification of the scale of benefits has been provided using the concept of breakeven analysis.

The specific benefits of these measures stem from the expected outputs and outcomes as seen in the Bill’s Theory of Change (table 4.1):

Table 8.1: expected outputs and outcomes

Outputs	Outcomes
Improved cyber security and resilience of RMSPs	Protect essential services and businesses so that the public can get on with their lives
Improved cyber security and resilience of data centres	
Improved cyber security and resilience of large load controllers	
Improved oversight of supply chain risk	
Regulators across all sectors implement the NIS Regulations in a consistent manner	Ensure that regulators are well-equipped to implement the NIS Regulations, creating a stable environment which fosters economic growth
Firms have greater clarity on legislative requirements streamlining oversight from regulators	
Regulators and NCSC have a more comprehensive view of the threat landscape	
The Information Commission takes a proactive approach to identify and mitigate cyber risks	
Regulators have the resources to effectively perform their duties	
Improved ability of regulators to enforce the regulations through better penalty structures and more proportionate financial penalties	
Legislation remains relevant and effective	Strengthening the UK's national security and ensuring the NIS Regulations remain effective in the context of an evolving threat landscape
Regulated entities promptly address threats and incidents which pose a significant risk to national security	
Improved compliance with NIS duties as a consequence of the deterrent effect of higher and more proportionate maximum fines	
Sectors adopt more stringent security measures in periods of heightened risk	

Each individual measure brings an expected benefit set out below.

Table 8.2: summarised benefit of each measure and associated evidence.

Measure	Summarised Benefit	Evidence where applicable
Bringing more entities into scope of the regulatory framework.		
1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations.	Enhance the security of IT systems and reduce the risks of cyber attacks, therefore reducing the negative externality of	Operation Cloud Hopper: a campaign, conducted over years but ramping up in 2016, was perpetrated by a group known as group known as

	the harm attacks have on the clients of RMSPs. These investments will enhance the position of RMSPs as trusted and reliable partners in the digital economy.	APT10. It targeted MSPs) to access to the intellectual property and sensitive data of those MSPs and their clients globally.[40] The UK and its allies have publicly attributed APT10 as acting on behalf of the Chinese Ministry of State Security. The primary objective of this campaign was espionage and intellectual property theft, for longer term advantage and gain rather than immediate financial gain (as seen in ransomware attacks). Remediation efforts—such as removing persistent access, conducting forensic investigations, and implementing enhanced security controls—can take months or even years. When combined with the extensive staff hours required, **the financial cost can escalate into the millions.**
2. Bring data centre infrastructure into scope of the NIS Regulations.	Strengthen the protection of data centres and all they support and enable by reducing the risk of disruption or compromise and reducing ensuing impacts on the rest of the network. This measure will ensure that operators take appropriate, economy-wide resilience measures, aligning private incentives with public interest. Bringing data centres into scope will also place incident reporting requirements on them, reducing the information asymmetry that exists between data	In July 2022, two separate data centres serving Guy's and St Thomas' NHS Trust suffered failures associated with the heatwave. This took down most of the clinical IT systems at Guy's, St Thomas' and Evelina London hospitals and the related community services. The loss of IT systems caused massive and widespread disruption to the running of clinical services and patient care within the Trust, and further incurred £1.4m of out-of-plan spending on technology services to respond to the incident.[41]

[40] Operation Cloud Hopper
[41] Guy's and St Thomas' Hospital, Critical Incident Review

	centres and government/regulators.	
3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations.	Incentivise large load controllers to invest in robust defences by placing cyber security requirements on them. There will also be the benefit of improving information asymmetry by encouraging information sharing between load controllers and the government/regulators. In turn this will reduce the risk of cyber attacks and disruption to the wider grid. This will incentivise the use smart appliances, contributing to the government's broader Net Zero goals.	GDP losses from a cyber-physical attack on electrical distribution networks in London could range from £20.6m to £111.4m.[42] The 2024 IBM Cost of a Data Breach Report found that the average cost of a data breach in the energy sector reached $4.88 million.[43]
4. Enable regulators to designate critical suppliers.	By allowing designation of critical suppliers, this measure will improve security of essential services reducing the negative externalities associated with cyber attacks. It will improve visibility of key suppliers, ensure more consistent risk handling across sectors, and enhance national resilience aligning with the UK's strategic priorities on economic growth, national security and economic resilience.	The cyber attack on NHS pathology provider Synnovis led to an estimated loss of £32.7m, disrupting profits for 2024 and 2025. This compares to a reported profit of £4.3m in 2023. Significant broader costs were felt to patients and the broader supply chain.
Empower regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties.		
5. Improving incident reporting.	Increase the UK's resilience to cyber attacks by ensuring regulators and the NCSC	Reporting incidents is essential for minimising the damage of attacks. Incidents that are not reported or that are reported

[42] Based on conservative scenarios. "Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks", Oughton, E, 2019

[43] IBM, 2024

	are promptly informed about incidents in NIS sectors. This will reduce imperfect information in the market by ensuring that key stakeholders—such as regulators, the NCSC, and businesses—have the necessary real-time or complete data regarding evolving cyber threats. Users will be able to take mitigating action if response to service disruption or compromises to systems. In turn, transparency requirements will raise standards across service providers and customers will be better informed when the service they rely on could be affected.	too late are harder to recover from, according to ENISA.[44]
6. Strengthen information sharing provisions, such as by enabling regulators to share information with each other and public authorities, and vice versa.	Provide greater certainty on what information can be shared, and by and with whom. This will in turn support delivery of the regulatory functions of regulators, inform government policy development on national security, critical infrastructure and cyber resilience, and enable effective evaluation of the NIS framework and its implementation. Again, this will reduce the information asymmetries that currently exist in the market.	*These measures are required to facilitate an effective regulatory regime, to underpin the security benefits described in this section.*
7. Enabling the Information Commission to collect information related to risk.	Reduces the level of imperfect information that exists in the market, ensuring a more	

[44] ENISA, 2024

	proactive supervisory approach can be taken by the Information Commission. This will allow the Information Commission to better risk assess the digital and managed services that it regulates, better enabling them to proactively support organisations to take steps to secure their systems.	
8. Improve regulators' cost recovery mechanisms.	Addresses limitations in the regulatory costs which can be recovered and prevents the financial burden of regulation breaches from falling onto the taxpayer, thereby promoting a more transparent, robust, and reliable regulatory environment. This will make the provision of regulation of cyber security more sustainable and efficient, benefiting the public and economy.	
9. Enable SoS to designate a statement of strategic priorities.	Ensures insofar as appropriate and possible that the NIS Regulations are applied consistently and effectively across sectors. Working towards correcting the lack of consistent enforcement of the regime will improve the current under provision of good cyber security in some parts of the network of regulated entities. This will ensure regulation is more evenly distributed so that cyber security across the network has minimal gaps that could	

	otherwise be exploited by attackers.	
10. Strengthen enforcement mechanisms of the NIS Regulations	Facilitates an effective regulatory regime by allowing regulators to levy proportionate and consistent fines. This will improve compliance with the regulations and therefore UK cyber resilience.	
Ensure that the NIS Regulations keep pace with the ever-changing cyber landscape and equip government to take decisive action to protect our national security.		
11. Delegated powers – ensure the regulatory framework is adaptable to emerging threats.	Enables the NIS Regulations to be updated to stay relevant, robust and proportionate, ensuring the ongoing protection of essential services from cyber attacks, thereby benefiting both the government and the public.	*These measures are needed to enable the government to update the security requirements of regulated entities, ensuring they sufficiently defend against the cyber threats facing the UK now and in the future.*
12. Security and resilience requirements.	Enables the government to set clear expectations for firms that provide digital services, to ensure proportionate and up to date security requirements are in place, while providing a means to update these requirements in response to a changing threat landscape. It ensures that standards are aligned to present-day real-world risks, reducing uncertainty and improving cyber security. It will also improve transparency and reduce information asymmetries between firms, regulators, and the public, leading to better-informed decisions and a more secure digital market overall. Also	

	enables the government to extend these requirements beyond digital service providers (for example, to OESs), allowing for the opportunity to raise the threshold of cyber hygiene across a broader range of businesses.	
13. Enable government to improve supply chain security.	Ensures effective oversight of supply chains, reducing risk of significant disruptions to essential and digital services. In turn national cyber resilience will be enhanced, and trust in critical infrastructure will be bolstered.	Last year just over one in ten businesses said they reviewed the risks posed by their immediate suppliers (14%) and under one in ten were looking at their wider supply chain (7%).[45]
14. Introduce a power for the SoS to direct a regulator, where it is necessary for national security.	By empowering the government to direct regulators during heightened threats, this measure better supports regulators to take swift action to protect national security.	Events in recent history have demonstrated the cost of cyber attacks to the world economy during conflicts. It may be in response to such conflicts that the government may deem it necessary to issue a direction to minimise risk. The period following the annexation of Crimea by Russia was followed by sustained cyber attacks by Russia-linked groups. An attack in 2015 on the Ukrainian power grid left 230,000 customers without power and in 2017 a ransomware attack cost the global economy up to $10 billion, according to the Office for Budget Responsibility.[46]
15. Introduce a power for the SoS to direct regulated entities, where it is necessary for national security.	By empowering the government to mandate stronger security measures during heightened threats, this measure compels regulated entities to act on critical intelligence, thereby strengthening system-wide resilience. This will result in NIS-regulated entities being better protected from malicious cyber activity in periods of heightened tension, reducing levels of disruption to service.	

[45] Cyber security breaches survey 2025 - GOV.UK
[46] Cyber-attacks during the Russian invasion of Ukraine - Office for Budget Responsibility

Together these measures will strengthen the economy's resilience to cyber attacks and reduce the associated costs.

Security benefits

These measures are expected to facilitate greater understanding of and support for cyber security within organisations. This was a success of the NIS 2 Directive, with 71% of OESs stating that they have an increase in board support for cyber security, and 43% reported the regulations improving their understanding of organisations' aggregate risk.[47]

Reduce impact from cyber attacks

Reducing the frequency and impact of cyber attacks, when compared to the 'do nothing' option, not only benefits the economy at a macro level but also benefits in the individual organisations affected. 43% of businesses reported having any kind of cyber security breach or attack in the last 12 months. For medium and large businesses this figure rises to 67% and 74%. Among the 43% of businesses that identify breaches or attacks, approximately one in five experience a negative outcome, such as a loss of money or data.[48]

Moreover, cyber criminals are increasingly attacking CNI, seeing essential services as lucrative targets. An independent report commissioned by Bridewell consulting found that 86% of the CNI they interviewed have detected a cyber attack on their systems in the past 12 months. Of those 86%, 93% experienced at least one successful attack in the last 12 months.[49]

The case study below shows the devastating impact of cyber attacks on regular people and how these measures will help to reduce these impacts. Incidents have demonstrated that disruption to a supplier in a critical supply chain could have far reaching impacts on citizens in the UK.

Supply Chain Duties - Synnovis Ransomware Attack – June 2024

The cyber attack on NHS pathology provider Synnovis led to an estimated loss of £32.7m, disrupting profits for 2024 and 2025. This compares to a reported profit of £4.3m in 2023. The ransomware attack disrupted services in London for several months, with thousands of elective procedures and outpatient appointments postponed at Guy's and St Thomas' NHS Foundation Trust and King's College NHS Foundation Trust. The human impact of this attack is clear; over 11,000 acute outpatient appointments and elective procedures were postponed. The Bill will enable Government to impose duties on regulated entities to manage supply chain risk and enable regulators to designate a small number of critical suppliers.

Some of the measures set out in this impact assessment are designed to improve collaboration, incident reporting and information sharing. Greater information sharing on threats and vulnerabilities will help reduce the scale of impact, for example through implementing preventative measures in public organisations, and improving the function of

[47] NIS PIR 2022
[48] Cyber security breaches survey 2025 - GOV.UK
[49] CNI Cyber Report: Risk & Resilience, commissioned by Bridewell consulting.

regulators. Improved reporting will enable regulators, government and NCSC to better understand the evolving landscape, allowing assistance to be provided where necessary and informing future policy development.

Improved Incident Reporting – NHS Trust

In 2023, ransomware actions exploited a vulnerability on the file transfer platform MoveIt, affecting British businesses and the US Department of Energy. In the same year, cyber criminals put a ransom note on the dark web stating they had stolen personal data from an NHS Trust. Neither incident would have been reportable under the current NIS Regulations as they did not have a significant impact on the continuity of an essential service. The incidents would be reportable under the Bill, as they are capable of disrupting service continuity or affecting confidentiality, availability and integrity of the system. This would, for example, enable the regulator to understand and protect against tactics to disrupt the provision of NHS services in the future.

International incidents have demonstrated that state cyber actors have the ability to threaten national security. Providing Government with powers of direction will bring the crucial benefit of giving it the ability to act decisively when an imminent threat arises.

Powers of Direction – Volt Typhoon

Volt Typhoon, a state-sponsored Chinese cyber operation, has recently compromised US critical infrastructure. Volt Typhoon uses “living off the land” tactics, which allow attackers to operate discreetly, with malicious activity blending in with legitimate system and network behaviour making it difficult to detect. US intelligence assessed that the cyber actors were seeking to position themselves on IT networks for attacks on US infrastructure in the event of a major crisis or conflict with the United States. Under the Bill’s power of direction measures, SoS would be able to direct regulated entities to mitigate the potential impact of an attack. The power of direction could prevent or mitigate the effects of a harmful attack on our CNI, thereby protecting national security interests. This will reduce the risk of key services being disrupted or sensitive data compromised as a result of an attack on a regulated service.

Growth benefits

Secure and robust digital services create a stable and secure environment for businesses to thrive, attracting investment and encouraging the development of cutting-edge technologies. This stability not only enhances the competitiveness of individual companies but also drives overall economic progress by reducing downtime and operational disruptions.

Resilient cyber infrastructure is essential for encouraging innovation by providing a secure foundation upon which new ideas and technologies can be built, thereby maintaining the UK’s position at the forefront of global technological advancements. Increasing the uptake of essential cyber defences will protect more entities from cyber attacks and foster an environment in which investment and innovation can thrive.

Direct Benefits - Quantified

While compliance with the measures may incur a cost for businesses, it will bolster security and resilience, helping to reduce this estimated cost of cyber-attacks, when compared to the 'do nothing' option. However, it is not possible to estimate what proportion of this cost will be averted through these specific measures as it is not possible to estimate the number of avoided attacks. As set out in the NIS PIR, there has been insufficient evidence on the reduction in incidents directly attributable to NIS measures. Therefore, it is not possible to build a robust counterfactual position of the number of incidents that would have occurred had the NIS Regulations 2018 not been introduced or in the event that these further measures are not introduced.

The key benefit of the updated NIS Regulations outlined in the impact assessment is the expected improvement in security which would lead to a reduction in the risks posed to essential services, compared to the 'do nothing' option. This in turn would benefit the UK's economic prosperity as there is a reliance on these services to support economic output and societal wellbeing. It is 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.

Whilst formal monetisation of the specific benefits of this bill has not been possible, DSIT has worked with cross-government stakeholders through 2024 and 2025 to better understand how to quantify the economic cost of cyber-attacks and therefore the potential value of preventing them. These insights can be used to provide indicative quantified benefits from these measures.

DSIT has commenced this Cyber Quantification project[50] which will attempt to quantify the economic cost of cyber attacks against all entities, including consumers, government, and businesses. The final output of the project will provide an overarching view of the potential impact of cyber attacks to the UK economy. Early findings from this work draw from one initial report commissioned by DSIT:

- Economic Modelling of Sector Specific Costings of Cyber Attacks, KPMG, 2025 – findings from this report have been used to support the benefits to business analysis below.

Results are based on significant assumptions and therefore insights should only be treated as indicative. Estimated breakeven points below are based on an average annual snapshot and do not account for potential changes in the prevalence and cost of cyber attacks over the coming years.

Benefits to business

KPMG estimate that the average cost of a significant cyber attack for an individual business in the UK is £194,729 (in 2024 prices). When scaled based on the proportion of UK businesses estimated to experience a significant cyber attack,[51] the modelling estimates a total cost to businesses at the UK economy level of £14.7 billion, representing 0.5% of the

[50] https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk

[51] Uses figures from the Cyber Security Breaches Survey

UK's annual Gross Domestic Product (GDP).[52] However, it is noted that estimates of the total cost of cyber attacks to an economy vary widely, are based on a range of different methodologies and are highly sensitive to whether broader economic and welfare costs from the direct disruption and second order effects are taken into account.[53]

KPMG also estimate the average cost of a cyber attack to a business by sector and by firm size. The report contains information on all sectors, but three are most relevant to businesses currently covered by the NIS Regulations. These are utilities, transport and healthcare. The information sector is most relevant to the newly regulated businesses categorised as MSPs and Data Centres, whilst utilities remain most relevant to newly introduced large load controllers. SMEs are generally excluded from NIS, and therefore the most relevant firm size to focus on is large firms. The estimated cost per firm is shown in the table below:

Table 8.3: Estimated cost of a cyber attack on large firms within the Utilities, Transport and Healthcare sectors

Sector	**Estimated cost of a cyber attack on large firms in the sector**
Utilities	£436,443
Transportation	£951,443
Healthcare	£483,312
Information	£1,101,588

KPMG's work estimates that certain types of attacks can be particularly costly and these include scam/fraud, system failure and system intrusion. If these attacks are avoided, then the benefit per attack will be even larger. If wider avoided impacts, such as of water, energy or transport disruptions on people and businesses, or cancelled healthcare appointments, were also reflected in costs, the benefits per attack would be greater still.

Newly regulated firms

The majority of costs estimated in this impact assessment fall on businesses that are being brought within scope of the NIS regulations through this bill. The costs to three groups of businesses have been monetised in the cost section below; MSPs, data centres and large load controllers. The annualised direct cost to these businesses has been estimated at £125m. This consists of £120m in total to MSPs and data centres, and £5m to large load controllers.

However, the bill will produce significant benefits to these businesses through the reduced costs of cyber attacks they are expected to experience when compared to the 'do nothing' option. Although it has not been possible to monetise these benefits, a breakeven analysis can indicate the scale of benefits needed to justify the costs to these businesses:

[52] This figure uses GDP at market and current prices for 2024
[53] Cost of a Cyber Incident: Systematic Review and Cross-Validation

Breakeven point = Annual cost to business from adhering to regulations

/ Estimated cost of a cyber attack to an individual business

KPMG's estimates of the cost of attacks to relevant sectors can be used as a proxy for the cost of cyber attacks to newly regulated firms. For MSPs and data centres, the cost of an attack in the information sector can be used, whilst for large load controllers the cost within the utilities sector can be used. For both sectors, the estimated cost of an attack shown in table 8.3 is used as a central estimate, whilst a cost 20% greater is used for high estimate, and 20% lower used for the low estimate. The number of attacks that would need to be avoided to justify the cost can be estimated:

Table 8.4: Results of break-even analysis for newly regulated firms

MSPs and data centres

Scenario	**Cost per Attack**	**Number of avoided attacks (annual) to 'break-even'**
Low	£881,270	136
Central	£1,101,588	109
High	£1,321,906	91

Large load controllers

Scenario	**Cost per Attack**	**Number of avoided attacks (annual) to 'break-even'**
Low	£349,154	14
Central	£436,443	11
High	£523,732	9

Therefore, under the central scenario, if over 109 additional attacks were avoided a year for, MSPs and data centres, as a result of these businesses adhering to the regulations, then the cost of adherence would be outweighed by the benefits of adherence. For large load controllers, 11 attacks would need to be avoided. For context, there will be an estimated 863 newly regulated firms in the central scenario. In 2024, 6,000 large businesses across the UK economy experienced cyber breaches or attacks[54].

An alternative way to indicatively depict the scale of benefits from this intervention is to consider the potential costs under the 'do nothing' option of this impact assessment. In a hypothetical scenario in which if each newly regulated business experienced a cyber attack, the total costs can be estimated, shown below in table 8.5. When compared to an annual cost to these businesses of £125m from adhering to the NIS regulations, the theoretical potential benefit is clearly much greater.

[54] Cyber Security Breaches Survey, 2025

Table 8.5: Indicative annual total cost to businesses being brought in scope of the NIS regulations through this bill, under theoretical situation where each business experienced one attack, central estimate

Business Type (central estimate)	Number of Businesses	Cost per Attack (central estimate)	Total Cost (1 attack per business)
MSPs	788	£1,101,588	£868m
Data centres	64	£1,101,588	£71m
Large load controllers	11	£636,443	£4.8m
Total			**£943m**

Businesses already regulated

There are some additional costs falling on already-regulated businesses through this bill. Primarily, as explained in the 'Costs' section below, these costs originate from the new incident reporting timeline requirements. The estimated annual direct cost to already-regulated businesses is £12m across both the OESs and RDSPs. From the NIS PIR 2022 it is possible to estimate the number of regulated firms that fall into certain sectors. Taking these proportions, it is possible to estimate the cost to businesses within each sector which can be divided by the estimated cost of a cyber attack to businesses in these sectors to identify a break-even point for each firm.

Table 8.6: Break-even analysis for already-regulated businesses

Sector	Estimated number of firms	Estimated additional cost to these firms	Estimated cost of a cyber attack in this sector	Estimated break-even
Utilities (OESs)	210	£2.4m	£436,443	5
Transport (OESs)	171	£1.9m	£951,443	2
Healthcare (OESs)	132	£1.5m	£483,312	3
Information (RDSPs)	513	£6.8m	£1,101,588	6

In this analysis, if an additional 5 attacks a year are avoided by already regulated businesses in the utilities sector then the costs of the new reporting timelines will be justified. For the transport, healthcare and information sectors, the number of additional avoided attacks needed is 2, 3 and 6 respectively. While a stronger incident reporting approach is unlikely to prevent attacks in the year of implementation, it could support faster recovery (due to quicker reporting to both the NCSC and regulator) – which would reduce direct costs and broader second order impacts, and prevent future attacks by creating a

more comprehensive picture within and across sectors of successful attacks, regulatory compliance and the most impactful mitigation steps.

Benefits to total economy

It is worth noting that the above analysis only considers the benefits to UK businesses. In reality, the benefits from the Bill will be felt widely across the economy, not just by the businesses in scope of the NIS regulations. This is due to the negative externalities associated with cyber attacks. The negative impacts of attacks are felt more widely than just the organisations attacked, and the benefits of enhanced security are therefore felt across the whole economy.

Indirect benefits

Competition benefits

The Bill will provide a regulatory framework that fosters the right incentives to promote security and transparency among regulated entities. In turn, a more predictable and cohesive operating environment for these sophisticated players in this market might be conducive to encouraging more competitiveness on a quality basis and hence investment. Similarly, a more secure business environment might encourage digital businesses to operate in the UK. Consistent regulatory approaches with the EU and other countries will also allow greater investment in the UK.

9. Costs

Summary – Do nothing option

The do nothing option represents a continuation of business as usual and therefore does not provide any additional direct or indirect costs. Doing nothing is expected to result in no improvements to the significant costs associated with cyber attacks for in-scope organisations and to affected consumers. Some quantified estimates of the cost of cyber attacks to businesses and the wider economy are outlined in the benefits section above.

Summary – Preferred option

Analysis of the costs of the proposed package of reforms has been split in the following way, and further details can be found in the continuing sections.

Costs have explained and monetised where possible for each measure:

Contents

Bringing new entities into scope

1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations.
2. Bring data centre infrastructure into scope of the NIS Regulations.
3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations.
4. Enable regulators to designate critical suppliers.

Empower regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties.

5. Improving incident reporting.
6. Strengthen information sharing provisions, such as by enabling regulators to share information with each other and public authorities, and vice versa.
7. Enabling the Information Commission to collect information related to risk
8. Improve regulators' cost recovery mechanisms.
9. Enable SoS to designate a statement of strategic priorities.
10. Strengthen the enforcement and sanctions framework of the NIS Regulations.

Ensure that the NIS Regulations keep pace with the ever-changing cyber landscape and equip government to take decisive action to protect our national security.

11. Delegated powers – ensure the regulatory framework is adaptable to emerging threats.
12. Security and resilience requirements.
13. Enable government to improve supply chain security
14. Introduce a power for the SoS to direct a regulator, where it is necessary for national security
15. Introduce a power for the SoS to direct regulated entities, where it is necessary for national security.

Totals

Table 9.1: Total monetised cost per measure, where applicable.

This combines one off costs and annual costs over 10 year appraisal period in the form of a total present value of the cost in 2025 prices.

Measure	Total cost (£m) Present Value Low scenario	Total cost (£m) Present Value Central scenario	Total cost (£m) Present Value High scenario
1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations	£552m	£796m	£1,058m
2. Bring data centre infrastructure into scope of the NIS Regulations	£118m	£149m	£214m
3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations	£27m	£40m	£64m
4. Improving incident reporting	£58m	£201m	£384m

Please note all incident reporting costs for RMSPs, data centres and large load controllers are captured in the incident reporting measure.

Table 9.2: Costs per type

	Explained	Applies to
One-off		
Familiarisation	Costs associated with reading and understanding the new measures. DSIT have used a time-cost approach to estimate the administrative costs of reading the updated NIS Regulations	All newly regulated entities Regulators
Additional physical security costs	One-off additional physical security costs to business. The one-off additional security costs are attributed to the first year the measures are implemented as these are costs associated with meeting the additional security	All newly regulated entities

	requirements of the NIS Regulations.	
Contract change costs	Cost of changing contracts to reflect any relevant aspects of the NIS Regulations for clients.	All newly regulated entities
Ongoing costs		
Incident reporting	Costs to new firms from having to report incidents and the costs to existing regulated firms due to the expanded scope of incident reporting introduced by the updated NIS Regulations.	All newly regulated firms All existing firms
Additional cyber security costs	Ongoing cost of additional cyber security spending by regulated entities with complying with the new measures	All newly regulated entities
Compliance costs	The cost associated with providing evidence of compliance to the relevant regulator, including completed a CAF and other documents. Requirements differ depending on the sector and relevant regulator and it is not possible to capture that nuance in the monetised costs.	All newly regulated entities
Costs to regulators	Ongoing cost to regulators of having to regulate the new entities	Regulators

In scope organisations

A number of the monetisation analyses in this section rely on estimates of the total number of relevant organisations in scope. This section provides a summary of number of businesses in scope for each measure, along with highlighting the evidence informing the estimates in each scenario.

Table 9.3: Total number of organisations in scope for each measure in first year of implementation. See below the table for an explanation of these estimates.

Organisation group	**Number of orgs - Low scenario**	**Number of orgs - Central scenario**	**Number of orgs - High scenario**	**Evidence informing scenarios**
Relevant Managed Service Providers	556	788	1019	Frontier Economics 2025

Data centres	64	64	64	Commissioned research by DSIT's data policy team
Large load controllers	8	11	22	DSIT internal estimate
Critical Suppliers - relevant digital service provider (RSDP)s	N/A	N/A	N/A	
Critical suppliers - 'operators of essential services' (OESs)	56	93	130	Based on the estimates provided by two regulators
Incident reporting	1,756	1,991	2,223	This is a sum of estimates across all groups of firms already regulated and newly regulated
Regulators	13	13	13	There are 12 regulators for the NIS Regulations 2018. The addition of data centres, regulated jointly by Ofcom and DSIT, adds an additional regulator (DSIT).

Managed Service Providers

Frontier Economics estimate that there are 12,867 MSPs active or registered in the UK. SMEs are excluded from NIS therefore Frontier estimate that there are between 977 and 1,214 MSPs that employ at least 50 people in the UK and have a turnover exceeding 10m Euros. 658 of these organisations are estimated to be cloud service providers which are already in scope of the bill. Therefore, after removing these organisations, it is estimated that the number of MSPs in scope of the updated NIS Regulations is between 556 and 1,019. These numbers have been used for the low and high scenario while the midpoint of these estimates (788) has been used for the central scenario. For ongoing costs, the number of MSPs in scope is expected to grow over the period. Over the 10-year appraisal period the number of MSPs is expected to grow at a rate of 3.6% per annum in all scenarios. The average annual growth rate for the total number of businesses in the

information and communication sector over the previous 10 years is used to approximate this. It is assumed this sector best represents the likely growth rate of MSPs.

Data Centres

There are 64 data centres in scope of the measures. Due to the certainty of the number of data centres that will be in scope when this regulation is implemented this is the same in all scenarios. For ongoing costs, in the low scenario this is assumed to stay constant, in the central scenario a growth rate of 3.6% is assumed in line with other measures while in the high scenario a higher growth rate of 10% is assumed to account for the potential for increased growth in this sector.

It likely that the considerable growth in the capacity and number of data centres that is forecast in the UK will not itself lead to a significant increase in the number of businesses, since much of this growth is led by existing businesses, particularly large, foreign-owned ones. It is a highly specialised industry which, whilst they are welcome, further limits the potential for many new entrants.

Large Load Controllers

In the low scenario, 8 organisations are expected to be in scope, in the central scenario 11, and in the high scenario 22 for the first year of implementation. This is based on market analysis done internally in 2023, combined with the known number of load aggregators controlling above 300MW – 5 organisations. The number of large load controllers is expected to grow over the appraisal period whereas there is no growth expected for the number of load aggregators This is because load controllers are a nascent market, whereas the aggregators are large established organisations.

Designating Critical Suppliers

For this measure, critical suppliers may be designated in relation to OESs, as well as RDSPs and RMSPs. Critical suppliers are firms whose products or services are essential to the resilience of essential or digital services. Sector regulators will have the power to designate suppliers and impose proportionate cyber security duties to reduce the risk those suppliers posed to regulated entities. Designation will only be possible where statutory threshold criteria are met, ensuring that only a small number of the most important suppliers are captured.

Importantly, this includes certain small and micro MSPs and DSPs, such as smaller cloud providers, that were previously exempt from the NIS Regulations. If such providers meet the threshold criteria and are deemed critical to an essential service, they may now be designated as a critical supplier.

- Small/micro DSPs and MSPs are generally exempt from direct regulation due to size thresholds, but may still be designated where their disruption could significantly affect essential, digital, or managed services.

DPSs and MSPs (SMEs)

At this stage it has not been possible to estimate the number of small and micro-sized DPSs and MSPs that will be designated. This will be updated at secondary legislation stage.

OESs

In the low scenario there is expected to be 56 OESs, in the central scenario; 93, and in the high scenario; 130. These scenario expectations originate from estimates provided by two regulators, extrapolated by DSIT to all 13 regulators to produce total numbers of OESs to be that could be designated. The number of critical suppliers is not expected to change over the appraisal period as these organisations are well established in the supply chain.

This measure will be enacted once secondary legislation (setting the duties on critical suppliers) comes into effect. Ahead of this, DSIT will conduct a full analysis the expected number of critical suppliers to be designated and the cost of that designation per supplier.

Improved Incident Reporting

The number of firms in scope is the sum of the number of organisations in scope of the NIS Regulations 2018 and those that have been bought into scope via this Bill. In the first year, for the low scenario this is 1,756, in the central scenario is 1,991 and for the high scenario this is 2,233. For ongoing costs, the number of MSPs are expected to grow at a rate of 3.6% as explained previously. The number of RDSPs and OESs currently in scope remains the same and the number of critical suppliers is assumed to remain constant.

Regulators

There are currently 12 regulators in scope of the NIS Regulations. This will increased to 13 once the Bill comes into force because data centre infrastructure will be regulated jointly by Ofcom and DSIT – the latter of which is not currently a NIS regulator.

---

1. Bring relevant managed service providers (RMSPs) into scope of the NIS Regulations.

This measure brings all managed services provided by large and medium providers in scope of the NIS Regulations via the Bill. Small and micro businesses would be exempt, unless designated as a critical supplier by a regulator. By bringing RMSPs into scope of the NIS Regulations, they will be required to uphold standards of cyber security corresponding to those of RDSPs currently in scope, deterring cyber attackers and minimising the impacts should an incident occur.

Direct costs

Monetised direct costs

One-off costs

Familiarisation costs

Quantifiable impacts to RMSPs include familiarisation costs associated with the implementation of the new measures. DSIT have used a time-cost approach to estimate the administrative costs of reading the updated NIS Regulations.

DSIT identified the relevant number of MSPs as identified by commissioned research, which has provided a range of 556 to 1,019, with a mid estimate of 788. DSIT assumes that

familiarisation costs are experienced in year one as all organisations read the new guidance. Evidence was drawn from the NIS PIR 2022 which updated cost estimates by building on analysis within the 2018 NIS Impact Assessment. The original 2018 Impact Assessment's estimate was calculated using hourly earnings for legal professionals (£26) and IT and telecommunication directors (£37) from the 2018 ONS Annual Survey of Hours and Earnings (ASHE) Survey.[55] These were then multiplied by the average hours for each occupation to familiarise with the updated NIS Regulations and the number of firms in scope of the measure, 12 for legal professionals and 6 for directors, based on conversations with the department's internal legal department. An overhead charge of 22% was also applied as was used in previous NIS impact assessments. The 2022 PIR analysis takes this and also assigns a weighted average cost, provided by survey respondents, to the 12 respondents who disagreed with the original NIS Impact Assessment's estimation of familiarisation costs. The PIR then combines these two estimates to produce one composite familiarisation cost per organisation which is calculated as £1,133 (adjusted to be in 2025 prices). For this IA, this was then multiplied by the number of MSPs in scope as seen in table 9.4 below.

Table 9.4: Familiarisation cost calculation for MSPs (2025 prices)

	Low	**Central**	**High**
Number of MSPs	556	788	1019
Cost per MSP	£1,133	£1,133	£1,133
Total familiarisation cost	**£0.63m**	**£0.89m**	**£1.15m**

Additional physical security costs

DSIT has also modelled one-off additional physical security costs to MSPs. The one-off additional security costs are attributed to the first year the measures are implemented. These are costs associated with meeting the additional security requirements of the NIS Regulations.

The one-off additional security cost for MSPs is estimated by applying the investment in physical security for each digital service provider. DSIT were not able to update the cost per business of physical security cost updates during the 2022 PIR process because of low response rates from organisations surveyed. Therefore, the best estimate for the cost to MSPs is to take the cost per RDSP identified in the 2020 PIR (£58,012) through a survey of relevant organisations, and update this to 2025 prices (£70,281). This is then multiplied by the number of MSPs in scope in each scenario.

Table 9.5: Additional physical security cost calculation for MSPs (2025 prices)

	Low	**Central**	**High**
Number of MSPs	556	788	1,019
Cost per MSP	£70,281	£70,281	£70,281

[55] Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics

Total additional physical security costs	**£39.08m**	**£55.38m**	**£71.76m**

Contract change costs

DSIT assumes that RMSPs will spend a set amount of time in changing contracts to reflect any relevant aspects of the updated NIS Regulations for clients. This is expected to be a one-off cost as contract updates are expected to be incorporated going forward as BAU. DSIT assumes that organisations will only incur the cost of drafting one contract change that will be implemented across all clients.

This is calculated using the hourly salary and time spent by legal professionals for changing contracts to reflect the relevant requirements from the updated NIS Regulations. Using data from the 2023 ASHE Survey the hourly wage of a legal professional was approximately £29,[56] updated to 2025 prices (£34). The length of time legal professionals took to change the contracts for all measures has been assumed to be 1 day (8 hours) in the low scenario, 1 week (40 hours) in the central scenario and 2 weeks (80 hours) in the high scenario.

To calculate the total cost of one-off contract changes for MSPs the hourly salary of a legal professional is multiplied by the length of time to change the contracts in each scenario. This cost is then multiplied by the number of MSPs in scope for each scenario. An uplift of 22% has also been applied to account for overheads.

Table 9.6: Contract change cost calculation for MSPs (2025 prices)

	Low	**Central**	**High**
Number of MSPs	556	788	1,019
Hourly salary (2025 prices)	£34	£34	£34
Number of hours	8	40	80
Cost per MSP	£270	£1,348	£2,695
Total contract change costs	**£0.15m**	**£1.06m**	**£2.75m**
Total contract change costs including 22% overheads	**£0.18m**	**£1.30m**	**£3.35m**

Ongoing costs

Ongoing costs are costs to business and regulators associated with ongoing compliance with the NIS Regulations. These are appraised over the entire 10-year appraisal period.

Incident reporting

Incident reporting costs are explained in the incident reporting sub section 5 below.

Additional cyber security spending

[56] Employee earnings in the UK - Office for National Statistics

Additional cyber security spending refers to the ongoing cost of additional cyber security spending by businesses with complying with the new measures.

RMSPs will have to take on additional cyber security spending as they seek to comply with the NIS Regulations. This includes internal and external staff costs which were estimated in the 2022 PIR using survey data. This estimate already included a 22% uplift for overheads.

For RDSPs the internal cost per organisation was estimated at £64,460 in all scenarios while the external cost per organisation was estimated to be £28,175 in the central scenario, £26,297 in the low scenario and £30,054 in the high scenario.[57] This is the most appropriate estimate for MSPs, so this was then multiplied by the number of MSPs in each scenario to calculate an overall cost. Over the 10-year period the number of MSPs is expected to grow at a rate of 3.6% per annum in all scenarios, using the business growth rate in the information and communication sector.

Compliance costs

Compliance costs are ongoing costs of reporting compliance to the regulator. This could include processes such as completing a Cyber Assessment Framework (CAF) report or other reporting requirements. Requirements differ depending on the sector and the relevant regulator, so this analysis can be treated as potentially an over estimate as not all organisations in scope will need to incur this cost.

The total ten-year compliance cost for RMSPs is estimated from multiplying the average compliance cost per firm per year as found in the 2022 PIR by the number of MSPs that are expected to be brought into the regulation for each scenario. The average compliance cost per firm each year ranges from £429 to £644, with £519 in 2025 prices, being the central scenario estimated. This estimate already included a 22% uplift for overheads. These estimates were produced in the 2022 PIR by combining survey responses with estimates using ONS ASHE 2018 data. The latter assumed compliance activities would need 10 hours of legal professionals' time at £26.07 and 14 hours of corporate managers' time at £22.58. Time estimates were calculated by conversations with the department's internal legal team during the creation of the 2018 IA.

Over the 10-year period the number of RMSPs is expected to grow at a rate of 3.6% per annum in all scenarios, using the business growth rate in the information and communication sector.

Non monetised direct costs

There are no additional non monetised direct costs associated with this measure.

Indirect costs

There are no additional monetised or non-monetised direct costs associated with this measure.

---

2. Bring data centre infrastructure into scope of the NIS Regulations.

[57] Second PIR of the Network and Information Systems Regulations 2018 - GOV.UK

Designating data centres at or above 1MW capacity and enterprise data centres at or above 10MW capacity under the NIS Regulations would bring these facilities into the regulatory framework, ensuring that they adhere to specific security and resilience standards.

Direct costs

Monetised direct costs

One-off costs

Familiarisation costs

Quantifiable impacts to data centre operators include familiarisation costs associated with the implementation of the new measures. DSIT has used a time-cost approach to estimate the administrative costs of reading the updated NIS Regulations.

Due to the certainty of the number of data centres that will be in scope when this regulation is implemented, the total familiarisation cost for data centres is expected to be the same in each of the low, central and high scenarios. There will be 64 data centre operators, each with at least one data centre that meets the requirements, coming into scope of NIS. The total familiarisation costs for data centre operators were estimated by multiplying the expected familiarisation cost for each organisation by the number of data centre operators with a data centre in scope of the measures. An uplift of 22% has already been applied to account for overheads. The estimate used in the 2022 PIR of £1,133 (adjusted to be in 2025 prices) is again used. As explained in the previous section on RMSPs, as this applies to all newly-regulated businesses.

Table 9.7: Familiarisation cost calculation for data centres (2025 prices)

	Low	**Central**	**High**
Number of data centre operators	64	64	64
Cost per data centre operator	£1,133	£1,133	£1,133
Total familiarisation cost	**£0.072m**	**£0.072m**	**£0.072m**

Additional physical security costs

DSIT has also modelled one-off additional physical security costs to data centre operators. The one-off additional security costs are attributed to the first year the measures are implemented. These are costs associated with meeting the additional security requirements of the updated NIS Regulations.

The total physical security cost for data centre operators is estimated by applying the average cost of physical security investment for OESs and then applying this figure to the number of data centre operators expected to have at least one data centre in scope when the measure is introduced. This was estimated during the 2022 NIS PIR based on survey results as £86,973, £94,474 and £101,976 in the low, medium and high scenarios respectively. They have been uplifted to 2025 prices and set out in table 9.8 below. As the

number of data centre operators is constant across all the scenarios, the only deviation amongst the scenarios comes from the average cost of investment.

Table 9.8: Additional physical security cost calculation for data centres (2025 prices)

	Low	Central	High
Number of data centre operators	64	64	64
Cost per data centre operator	£105,356	£114,454	£123,542
Total additional physical security costs	**£6.74m**	**£7.33m**	**£7.91m**

Contract change costs

As with RMSPs, the cost of contract changes is calculated using the hourly wage of a legal professional from the 2023 ASHE survey. This is then uplifted to 2025 prices and multiplied by the length of time the legal professional took to change the contracts. An uplift of 22% has also been applied to account for overheads.

Table 9.9: Contract change cost calculation for data centres (2025 prices)

	Low	Central	High
Number of data centre operators	64	64	64
Hourly salary (2025 prices)	£34	£34	£34
Number of hours	8	40	80
Cost per data centre operator	£270	£1,348	£2,695
Total contract change costs	**£0.017m**	**£0.09m**	**£0.17m**
Total contract change costs including 22% overheads	**£0.021m**	**£0.11m**	**£0.21m**

Ongoing costs

Ongoing costs are costs to business and regulators associated with ongoing compliance with the NIS Regulations. These are appraised over the entire 10-year appraisal period.

Incident reporting

Incident reporting costs are explained in the incident reporting section 5 below.

Additional cyber security spending

To estimate the ongoing cyber security costs for data centre operators, DSIT has applied the external and internal security staff costs those operators of essential services incurred to comply with the previous NIS measures as found in the 2022 PIR which was gathered

using a survey. These costs combined for OESs range from £181,464 to £211,363 annually in 2025 prices. These costs are then multiplied by the number of data centre operators expected to be in each scenario over the next 10 years. This estimate already included a 22% uplift for overheads. Over the 10-year period the number of data centre operators is expected to grow at a rate of 3.6% per annum in all scenarios, using the business growth rate in the information and communication sector. Data centre operators are to become OESs so the internal and external costs here are greater than for RDSPs as set out in the 2022 PIR.

Compliance costs

Compliance costs are ongoing costs of reporting compliance to the regulator. This could include processes such as completing a CAF or other reporting requirements. Requirements differ depending on the sector and the relevant regulator, so this analysis can be treated as potentially an overestimate as not all organisations in scope will need to incur this cost.

The total, 10-year compliance cost for data centres is estimated from multiplying the average compliance cost per business per year as found in the 2022 PIR by the number of data centre operators that are expected to be brought into the regulation for each scenario. This estimate already included a 22% uplift for overheads. The average compliance cost per firm each year ranges from £429 to £644, with £519 in 2025 prices, being the central scenario estimated. Over the 10-year period the number of data centre operators is expected to grow at a rate of 3.6% per annum in all scenarios, using the business growth rate in the information and communication sector. These estimates were produced in the 2022 PIR by combining survey responses with estimates using ONS ASHE 2018 data. The latter assumed compliance activities would need 10 hours of legal professionals' time at £26.07 and 14 hours of corporate managers' time at £22.58.

Non-monetised direct costs

There are no additional non-monetised direct costs associated with this measure.

Indirect costs

There are no additional monetised or non-monetised direct costs associated with this measure.

---

3. Bring a new energy essential service for the electricity sector (load control) into scope of the NIS Regulations.

This option will require large load controllers to demonstrate that they are implementing effective measures to prevent and mitigate a cyber attack, providing assurance to government regarding the sector's resilience against the evolving threat landscape.

Direct costs

Monetised direct costs

One off costs

Familiarisation costs

Quantifiable impacts to load controllers include familiarisation costs associated with the implementation of the new measures. DSIT have used a time-cost approach to estimate the administrative costs of reading the updated NIS Regulations.

The total number of large load controllers that will come in scope of NIS have been estimated over the low, central and high scenario. The total familiarisation costs for these organisations were estimated by multiplying the expected familiarisation cost for each organisation by the number data centres in scope of the measures. The estimate used in the 2022 PIR of £1,133 (adjusted to be in 2025 prices) is again used and this is the same across each scenario. An uplift of 22% has already been applied to account for overheads.

Table 9.10: Familiarisation cost calculation for load controllers (2025 prices)

	Low	**Central**	**High**
Number of load controllers	8	11	22
Cost per load controller	£1,133	£1,133	£1,133
Total familiarisation cost	**£0.009m**	**£0.012m**	**£0.025m**

Additional physical security costs

DSIT has also modelled one-off additional physical security costs to load controllers. The one-off additional security costs are attributed to the first year the measures are implemented. These are costs associated with meeting the additional security requirements of the updated NIS Regulations.

The total physical security cost for load controllers is estimated by applying the average cost of physical security investment for operators of essential services, which is the most appropriate estimate for this group of newly regulated organisations. These were estimated for the 2022 PIR based on survey results as £86,973, £94,474 and £101,976 in the low, medium and high scenarios respectively and have been updated to 2025 prices. This was then applied to the number of data centres assumed to be in scope when the measure is introduced.

Table 9.11: Additional physical security cost calculation for data centres (2025 prices)

	Low	**Central**	**High**
Number of load controllers	8	11	22
Cost per load controller	£105,356	£114,454	£123,542
Total additional physical security costs	**£0.84m**	**£1.26m**	**£2.72m**

Contract change costs

As with MSPs, the cost of contract changes is calculated using the hourly wage of a legal professional from the 2023 ASHE survey. This is then uplifted to 2025 prices and multiplied by the length of time the legal professional took to change the contracts. An uplift of 22% has also been applied to account for overheads.

Table 9.12: Contract change cost calculation for load controllers (2025 prices)

	Low	**Central**	**High**
Number of load controllers	8	11	22
Hourly salary (2025 prices)	£34	£34	£34
Number of hours	8	40	80
Cost per load controller	£270	£1,348	£2,695
Total contract change costs	**£0.0022m**	**£0.015m**	**£0.059m**
Total contract change costs including 22% overheads	**£0.0026m**	**£0.018m**	**£0.072m**

Ongoing costs

Ongoing costs are costs to business and regulators associated with ongoing compliance with the NIS Regulations. These are appraised over the entire 10-year appraisal period.

Incident reporting

Incident reporting costs are explained in the incident reporting section 5 below.

Additional cyber security spending

Additional cyber security spending refers to the ongoing cost of additional cyber security spending by load controllers on complying with NIS.

To estimate the ongoing cyber security costs for load controllers, DSIT has applied the external and internal security staff costs OESs incurred to comply with the previous NIS measures as found in the 2022 PIR which were gathered using a survey. These costs combined range from £181,464 to £211,363 annually in 2025 prices. This estimate already included a 22% uplift for overheads. These costs are then multiplied by the number of load controllers expected to be in each scenario over the next 10 years. Over the 10-year period the number of load controllers is expected to grow in all scenarios, using the business growth rate in the information and communication sector. Load controllers are to become OESs so the internal and external costs here are greater than for RDSPs.

Compliance costs

Compliance costs are ongoing costs of reporting compliance to the regulator. This could include processes such as completing a CAF or other reporting requirements. Requirements differ depending on the sector and the relevant regulator, so this analysis

can be treated as potentially an over estimate as not all organisations in scope will need to incur this cost.

The total ten-year compliance cost for load controllers is estimated from multiplying the average compliance cost per firm per year as found in the 2022 PIR by the number of load controllers that are expected to be brought into the regulation for each scenario. This estimate already included a 22% uplift for overheads. The average compliance cost per firm each year ranges from £429 to £644, with £519 in 2025 prices, being the central scenario estimated. Over the 10-year period the number of data centres is expected to grow at a rate of 3.6% per annum in all scenarios, using the business growth rate in the information and communication sector. These estimates were produced in the 2022 PIR by combining survey responses with estimates using ONS ASHE 2018 data. The latter assumed compliance activities would need 10 hours of legal professionals' time at £26.07 and 14 hours of corporate managers' time at £22.58. The time estimates were informed by conversations with the department's internal legal team ahead of the 2018 NIS IA.

Non monetised direct costs

There are no additional non monetised direct costs associated with this measure.

Indirect costs

There are no additional monetised or non monetised direct costs associated with this measure

---

4. Enable regulators to designate critical suppliers

This gives regulators the power to designate critical suppliers to regulated entities. Statutory threshold criteria will need to be met in order for a supplier to be designated, ensuring that only a small number of the most important suppliers are captured. Small and micro RDSPs, previously exempt from the NIS Regulations 2018, will be capable of being designated as 'critical suppliers' if they meet the threshold criteria (and are therefore deemed critical to an essential or digital service).

Designation of critical suppliers cannot take effect until the Government sets out duties on designated critical suppliers in secondary legislation at a later date. The analysis below sets out an estimate of what the costs to a designated critical supplier is likely to be and gives an indication of how many suppliers could be designated at secondary legislation. However, due to the uncertainty around the exact number of firms the costs have not been monetised, are not included in the headline figures for this IA and this analysis will be updated ahead of secondary legislation.

Direct costs

DSIT does not expect this measure to produce any direct costs at primary legislation phase. This measure will be enacted once secondary legislation (setting the duties on critical suppliers) comes into effect.

Non monetised costs

Cost per organisation

At this stage it is possible to say that each designated critical supplier will have to incur the following one-off costs:

- **Costs of familiarising themselves with the NIS Regulations** which is estimated at £1,133 per firm in 2025 prices
- **Additional physical security costs in the first year in which they are designated**. These organisations will be designated as a category of their own and will have similar obligations to OESs and RDSPs. Specific duties will be set through secondary legislation so the exact cost of security measures is not possible to estimate. Taking the costs to OESs as identified in the NIS PIR 2022 as the closest proxy, the central estimate of this cost per firm will be £114,451. In this impact assessment, costs to OESs has been estimated to be higher than for RDSPs, so the higher cost has been chosen here for caution.
- **Contract change costs** are estimated at £329 to £3,288 per form, with a central estimate of £1,644 in 2025 prices. As with measures 1-3, the cost of contract changes is calculated using the hourly wage of a legal professional from the 2023 ASHE survey. This is then uplifted to 2025 prices and multiplied by the length of time the legal professional took to change the contracts. An uplift of 22% has also been applied to account for overheads.

They will also incur the following annual ongoing costs:

- **Incident reporting** which is explained under measure 5 below.
- **Additional cyber security spending** associated with NIS. As previously explained, these organisations will be designated as their own category. Again taking the cost to OESs as a cautious proxy would provide a central estimate of cost to each individual business of £190,435.
- **Other costs of compliance** for with the updated NIS Regulations with an estimated cost per firm each year ranging from £429 to £644. £519 in 2025 prices is the central scenario estimated, in line with the other newly regulated firms.

Number of organisations designated

DSIT has evidence from two regulators regarding the number of firms they will likely designate as critical suppliers. Extrapolating these estimates out to all 13 regulators identifies in a low case scenario, 56 will be designated, 130 in a high case scenario and 93 in a central case scenario.

DSIT is not able to estimate at this stage the number of SMEs or SME DSPs that will be designated as critical suppliers. These will be small and micro businesses that are not automatically captured by NIS and the new measures brought in by this bill. However, regulators will follow strict guidelines on which organisations can be designated to ensure that only critical suppliers are included. Any cost to SMEs is therefore necessary to ensure the security of key supply chains.

These estimates will be updated ahead of secondary legislation.

5. <u>Improving incident reporting</u>

This measure involves amending the reporting framework to ensure that businesses are reporting incidents, and that regulators are able to obtain a clear picture of the extent and severity of cyber security incidents.

Updating incident reporting times to introduce a two-stage reporting structure (an initial notification within 24 hours of becoming aware of the incident, followed by a report within 72 hours) will bring incidents to the attention of the regulator sooner, allowing more time to assess what action is needed (if any). The initial notification will be light touch, ensuring the regulated entity can direct their resources to mitigating the effects of the incident as best as possible in the crucial early stages.

Incident reporting produces costs in two ways:

- Existing regulated entities will incur just additional costs from the new incident reporting requirements brought in through this measure.
- Organisations that are being brought into the updated NIS Regulations through this bill incur the full costs of incident reporting. This includes RMSPs, data centres and large load controllers being bought into scope. Critical suppliers will also bear this cost, but the cost to these entities has not been monetised at this stage.

Direct costs

Monetised direct costs

One off costs

Table 9.13: Number of firms in scope

	Low	Central	High
MSPs	556	788	1,019
Data centres	64	64	64
Load controllers	8	11	22
Total newly regulated entities	628	863	1,105
Existing regulated entities	1128	1128	1128
Total	**1,756**	**1,991**	**2,233**

Familiarisation costs

All firms in scope including newly regulated entities will have to familiarise themselves with the incident reporting requirements set out in the updated NIS Regulations. For newly regulated firms this cost is captured in the familiarisation costs under RMSPs, data centres and load controllers. For entities already in scope, DSIT has estimated familiarisation costs based on the median wage for legal professionals (£29) and IT and telecommunication directors (£43) in the 2023 ASHE survey. The number of hours for each occupation to familiarise with the updated NIS Regulations as 3 for legal professionals and 1.5 for IT and

telecommunication directors. The median wage is multiplied by the number of hours and by the totals of firms. An uplift of 22% has already been applied to account for overheads.

Table 9.14: Familiarisation cost calculation for incident reporting for existing regulated firms (2025 prices)

	Low	**Central**	**High**
Number of existing regulated firms	1128	1128	1128
Cost per firm	£380	£380	£380
Total cost for existing firms (£m)	**£0.43m**	**£0.43m**	**£0.43m**

Ongoing costs

Ongoing costs are costs to business and regulators associated with ongoing compliance with the NIS Regulations. These are appraised over the entire 10-year appraisal period.

Cost of reporting incidents

For existing regulated firms there is no additional cost from having to report incidents as they are already required to. The additional cost comes from the new reporting timeline and definition covered below.

All newly regulated firms will likely experience the below cost of having to report incidents. Due to a difference in scope of definition for reportable incidents, the cost of reporting incidents for data centres is considered separately.

The reporting cost of each incident is calculated by using the hourly wage in the 2023 ONS ASHE survey for 1 IT and telecommunication professionals (£27.20), 1 legal professional (£29.08) and 1 corporate manager and director (£32.66). This is multiplied by the amount of time DSIT expects them to spend addressing the incident. This is 0.75 hours for IT and telecommunications professionals and legal professionals and 0.33 hours for corporate managers and directors. These are the same assumptions as were used in the NIS Regulations 2018 impact assessment and the 2022 PIR. The average wages are assumed to grow over the appraisal period at a growth rate calculated using the average annual growth rate in wages for these three occupations per year between 2013 and 2023.

The wage time estimate is then multiplied by the number of incidents per organisation; estimated at 2, 7 and 16 for the low, medium and high scenarios. These were calculated by taking the number of incidents per year under the NIS Regulations 2018 divided by the total number of regulated organisations. This is then multiplied by the number of newly regulated firms in each scenario. This produces an estimate of the total cost of incidence reports for newly regulated firms excluding data centres. An 22% uplift for overheads has been applied.

Table 9.15.1: Total annual cost to newly regulated firms (excluding data centres) for reporting incidents in 2026, which is expected to grow year on year due to wage growth.

	Low	**Central**	**High**

Cost per incident (including 22% overheads)	£89	£89	£89
Number of incidents a year	2	7	16
Total number of newly regulated firms (excl. data centres)	564	799	1,041
Total incident reporting costs for newly regulated firms (excl. data centres)	**£0.10m**	**£0.50m**	**£1.6m**

The number of incidents per organisation for data centres has been uplifted to account for the expanded definition of reportable incidents. Therefore, the number of incidents per organisation for data centres is estimated at 7, 16, and 25 for the low, central and high scenarios. The revised low and central scenarios were taken from the baseline central and high scenarios set out above. The revised high scenario was calculated by applying to the revised central estimate absolute increase between the baseline central and high scenarios. This produces an estimate of the total cost of incident reports for data centres. A 22% uplift for overheads has been applied.

Table 9.15.2: Total annual cost to data centres for reporting incidents in 2026, which is expected to grow year on year due to wage growth.

	Low	**Central**	**High**
Cost per incident (including 22% overheads)	£89	£89	£89
Number of incidents a year	7	16	25
Total number of data centres	64	64	64
Total incident reporting costs for data centres	**£0.04m**	**£0.09m**	**£0.14m**

Aggregating costs across all newly in-scope organisations (including data centres), the total estimated cost for reporting incidents in 2026 is £0.14m, £0.60m, and £1.7m for the low, central and high scenarios respectively.

Incident reporting timeline

The improved incident reporting measure also makes changes to the incident reporting timeline. The new measure which requires a notification within 24 hours and a full report within 72 hours may require organisation to have staff on weekends to deal with the

incident. DSIT has assumed that all organisations will require one member of staff to deal with an incident.

To calculate the costs of this change, DSIT estimated the cost of a weekend shift and the proportion of businesses that will have on-call staff and weekend workers as well as the proportion of firms that will pay overtime. If firms did not have either weekend workers or on-call workers, then they had to pay for a full overtime shift. For medium and large firms 59% had on call staff, 13% had weekend workers and 63% paid overtime. For small and micro firms 61% had on call staff, 28% had weekend workers and 56% paid overtime. The proportions used were estimates from the 2024 NIS survey. If firms have weekend workers, there was no additional cost. If firms did not have weekend workers but did have call workers, then firms paid the on-call salary. The cost to businesses with on-call staff was calculated as £50.57.

Based on the proportions of firms with weekend and on call workers and the number of firms in scope of the NIS Regulations the appropriate the total cost for a weekend day is calculated. This is then multiplied by the number of weekend days in each given year. An uplift of 22% for overheads is also applied.

This cost applies to both existing regulated firms and newly regulated firms.

The total annual cost in 2026 for all firms will be £17.4m (£9,000 per firm on average) in the best estimate scenario, rising to £29m (£14,000 per firm on average) by 2036.

Non-monetised direct costs

Incident reporting costs to designated critical suppliers has not been monetised due to uncertainty in the number that will be designated. It is expected that they will experience the same costs as the RMSPs, data centres and large load controllers that are being brought into scope of NIS through this Bill.

Indirect costs

There are no additional indirect costs.

---

6. Strengthen information sharing provisions, such as by enabling regulators to share information with each other and public authorities, and vice versa.

To strengthen and expand information sharing provisions under the NIS Regulations to provide greater certainty on what information can be shared, and by and with whom. This option seeks to make four changes to address the shortcomings in information provisions that have been identified.

This measure is not expected to have any direct or indirect costs to businesses. However, there will be some familiarisation costs to regulators assessed below in the cost to regulator section.

---

7. Ensuring that the Information Commission has the appropriate information related to risk

This option would allow for a duty on RDSPs and RMSPs regulated by the Information Commission to provide additional specific information at registration through the NIS Regulations (such as the type of service being provided and specific contact details).

This is expected have no direct cost to business. There will be some familiarisation costs for the Information Commission set out in the costs to regulator section.

---

8. Improve regulators' cost recovery mechanisms.

This will allow regulators to properly fund all of their activities under NIS, including enforcing against breaches, and enable them to recover costs in the most appropriate way for their sector.

This may increase costs to regulated entities due to the inclusion of enforcement; however, it would have a positive impact for transparency and predictability of costs. Under the current model of invoicing, it is unclear for businesses whether they will be charged by the regulator and how much. The new duty on regulators to consult on any new charging scheme would ensure regulated entities are able to share their views and be made aware of the expected costs going forward. Additionally, this presents opportunities for regulators to put in place more tailored and proportionate cost recovery mechanisms, whilst facilitating a consistent approach across sectors through the criteria regulators will have to meet when designing their cost recovery regime.

This will lead to direct costs to business but it is not possible to calculate them at this stage due to lack of certainty on how each regulator will design their cost recovery regime. The NIS Regulations already contain cost recovery provisions under which most of the costs of exercising the regulators' functions under the NIS Regulations are already recoverable. The costs recovered vary from regulator to regulator, partly due to the cost recovery powers being inconsistently utilised by regulators.

---

9. Enable SoS to designate a statement of strategic priorities.

The statement of strategic priorities would detail outcomes which the regulators would have a duty to seek to achieve. This would provide better consistency in approach between regulators/sectors, as all would be required to work towards the same outcomes. To maintain regulatory autonomy, statements of strategic priorities would be drafted in consultation with the regulators, and regulators would be free to seek to achieve the outcomes in whichever way they thought was most appropriate. The current policy aim is for statement of strategic priorities would be produced every three to five years to provide regulators a long enough timeline to plan effectively, whilst allowing regulators and government to adjust approach as needed, such as the shift in guidance from reactive to proactive enforcement of the NIS Regulations. To provide opportunity for public scrutiny, the Secretary of State will be required to publish an annual report on progress made toward the goals of the statement of strategic priorities and may request information from the regulators to inform this.

This is not expected to lead to any cost to business. Regulators will be required to familiarise themselves with the statement of strategic priorities, as explained in the cost to regulators section.

---

10. Strengthen the enforcement mechanism of the NIS Regulations

This measure will enable regulators to levy higher and more proportionate fines for non-compliance with the regulations. It will also serve to simplify the financial penalty structure, providing increased clarity and predictability to fines, while at the same time enabling regulators to consider a wider range of circumstances when determining the appropriate level of a fine.

There are not any costs associated with this measure because full compliance is assumed.

---

11. Delegated powers – ensure the regulatory framework is adaptable to emerging threats.

This measure will enable the government, after any appropriate consultation, to update the regulatory framework without an Act of Parliament. These powers will be subject to certain restrictions and safeguards, for instance they will be limited to ensure that amendments are restricted to certain purposes in relation regulating services critical to the functioning of the UK economy or society. The powers may be used to make changes such as, introducing new requirements and duties for regulated entities, and making changes to the responsibilities and functions of NIS regulators. Any costs to businesses associated with changes to the NIS Regulations will be assessed before such secondary legislation is laid.

---

12. Security and resilience requirements.

We intend to provide Secretary of State with the power to update security and resilience requirements via regulations. The Secretary of State will be provided with powers to:

- Set security requirements by regulation that will apply to RDSPs.
- Extend beyond RDSPs, if appropriate and proportionate.

These requirements would replace the existing security requirements for RDSPs. The expectation is that Secretary of State will use the power to adjust the security requirements to reflect elements of the Cyber Assessment Framework Basic Profile – which sets baseline expectations around cyber governance, asset management, risk management and incident response for example.

At this stage this measure is not expected to have a direct cost to business. Any updates will take place via secondary legislation at which point the government will make an assessment of any costs to business.

13. Enable government to improve supply chain security

By setting clear expectations on OESs and RDSPs to identify and manage supply chain security through enforceable duties, it is expected that greater levels of compliance across the supply chain will be seen than with voluntary guidance. Clear, legal expectations will improve the use of contractual arrangements with suppliers to manage supply chain risk.

It is expected that this will have a direct impact on business but it is too early to estimate what these would be. Future duties will be set out in secondary legislation for which the government will make an assessment of the costs to business.

---

14. Introduce a power for the SoS to direct a regulator, where it is necessary and proportionate in the interests of national security

15. Introduce a power for the SoS to direct regulated entities, where it is necessary and proportionate in the interests of national security.

At this stage these two measures are not expected to have a direct cost to business. Should it be necessary to issue a direction to a regulator or regulated entity, there could be a cost to business depending on what that direction contains. Since this power is expected to be used infrequently and in exceptional circumstances where national security is threatened, it is not possible to predict the requirements in the directions or the cost to business incurred by complying with the direction. The government will make an assessment of any costs to the relevant businesses when deciding whether to issue a direction and how far reaching the direction should be.

Costs to regulators

There are currently 12 regulators in scope of the NIS Regulations, although this will raise to 13 once the Bill comes into force.

Direct costs

Monetised direct costs

One off costs

Familiarisation costs

DSIT assumes that familiarisation costs are borne in year one as all regulators read the new legislation. Evidence was drawn from the NIS PIR to inform the amount of time needed to familiarise the legislation. Familiarisation costs for regulators are estimated using hourly earnings for legal professionals (£26) and IT and telecommunication directors (£37) in the 2018 ONS Annual Survey of Hours and Earnings (ASHE) Survey. This was then multiplied

by the average hours for each occupation to familiarise with the legislation and the number of authorities in scope of the measure, 12 for legal professionals and 6 for directors. An overhead charge of 22% was also applied as was used in previous NIS impact assessments. This was calculated as £1,133 (adjusted to be in 2025/26 prices) for each competent authority. This was then multiplied by the number of regulators in scope.

Table 9.16: Familiarisation costs for regulators

	Low	**Central**	**High**
Number of regulators	13	13	13
Cost per regulators	£1,133	£1,133	£1,133
Total familiarisation cost	**£0.01m**	**£0.01m**	**£0.01m**

Ongoing costs

Cost of regulating

Ongoing cost to a regulator of regulating an organisation is estimated at £1,411 per firm in 2025 prices, as set out in the PIR 2022. This was based on the cost estimates provided by the Information Commission to inform the 2022 PIR and is the most appropriate estimate to apply for all competent authorities. This includes 22% uplift for overheads. Total number of new organisations regulated across MPSs, data centres and large load controllers over the 10 year appraisal period results is multiplied by this cost per organisation to estimate a total cost to regulator. Present value estimation of this cost is £18m over 10 years.

Costs of updated reporting timelines

Regulators will experience the costs associated with the new reporting timeline requirements for regulated entities. The new measure which requires a notification within 24 hours and a full report within 72 hours may require organisation to have staff on weekends to deal with the incident. DSIT estimated the cost to the regulator of the weekend work associated with dealing with incident reports. This cost has a present value of £1.99m in 2025 prices over 10 years.

Non monetised direct costs

Measures 13 and 14 (powers of direction) will lead to costs but at this stage it is not possible to monetise these costs. Regulators may also undertake costs involved with identifying and designating critical suppliers, however this Bill does not compel regulators to do that, so this cost is indirect.

Sensitivity Analysis

Throughout the analysis, low, central and high estimates have been provided to indicate a range where there is uncertainty in the assumptions used.

In addition, sensitivity analysis has been conducted on the highest costs estimated in the impact assessment. The most significant cost is the estimated ongoing additional cyber security spending needed by newly regulated entities to be compliant with the regulations. A change in the estimated cost by 20% would result in a 15% change in the estimated NPSV and EANDCB.

Of the newly regulated entities, RMSPs are the largest contingent. Therefore, changing estimates on the number of RMSPs that will be brought into scope has a significant impact on the estimated costs. A change in the estimated cost by 20% would result in a 13% change in the estimated NPSV and EANDCB.

To a lesser extent, the analysis is sensitive to the estimated incident reporting costs associated with the new reporting timeline. 20% changes to these costs would result in a 3% shift in the NPSV and EANDCB.

10. Wider impacts

Impact on small and micro businesses

There is currently minimal impact of the NIS Regulations 2018 on small and micro businesses because small and micro digital service providers (DSP) are exempt, whilst it is unlikely that many small and medium sized OESs are in scope – the 2022 PIR found that only one small and micro-OES was in scope.[58] The Bill proposes that the exemption be modified so that small and micro DSPs and MSPs can be designated as being in scope of the NIS Regulations by their regulator if they are deemed a critical supplier. This will ensure proportionate regulation of high-risk suppliers.

It is considered that this modification is necessary because all critical suppliers, regardless of size, can pose a risk to CNI, essential services and the UK economy. Research conducted by the Federation of Small Businesses in 2019 found that small businesses are subject to almost 10,000 cyber attacks every day. The same report estimated the annual cost of such attacks to the small business community to be £4.5bn.[59] The Cyber Security Breaches Survey 2025 found that 41% of micro businesses and 50% of small businesses reported having identified breaches or attacks in the past year.[60] These findings highlight the need to mitigate the potential risks posed by small and micro businesses which form part of our CNI and essential services supply chains.

There is significant support for the chosen approach. In response to the 2022 government consultation on cyber resilience legislation, 70% of respondents agreed that the exemption on small and micro DSPs should be modified to allow a small number of the most critical organisations to be regulated by the NIS Regulations. In addition, 100% of micro and 75% of small businesses agreed with modifying the exemption.[61] DSIT has conducted discussions with small and micro MSPs who were broadly supportive of some small and micro DSPs/MSPs being brought into scope of the Bill. There is considered to be little risk

[58] Second Post-Implementation Review of the Network and Information Systems Regulations 2018 - GOV.UK
[59] 'Small firms suffer close to 10,000 cyber attacks daily' FSB (2019) 10k cyber-attacks a day on small firms - CPA | The Credit Protection Association
[60] Cyber security breaches survey 2025 - GOV.UK
[61] Proposal for legislation to improve the UK's cyber resilience - GOV.UK

of raised prices of goods and services provided by SMEs due to increased regulation. Evidence from the 2022 PIR showed that 93% of NIS regulated entities did not raise the price of their goods or services as a result of the NIS Regulations 2018.[62]

DSIT will ensure that appropriate guidance is designed for small and micro businesses, working closely with the regulators on the implementation of this measure.

SAMBA for Data Centre Operators

SAMBA was carried out separately for data centre operators (DCOs). From research commissioned last year there are 68 DCOs operating in the UK, 64 of which have at least one data centre that is equal to or above the 1 MW threshold for bringing them into scope (confirmed by the Secretary of State). Employee counts were obtained from two sources:

- Primarily Beauhurst, which sources much of the information from Companies House data. Employee counts were found for 45 DCOs.
- Employee counts were obtained for an additional 8 DCOs from The Data City web-scraped data obtained in 2023.

49 of these meet the threshold for inclusion in scope.[63] According to this sample, the number of SMEs estimated to be in scope, out of these 49 businesses, are as follows.

Table 10.1:

	Number of SMEs in scope	Percentage of 49	95% confidence interval (percentage points)
SMEs (<500)	38	78%	13%
Small and micro (<50)	21	43%	21%
Medium (≥50 and <500)	17	35%	23%

There are a number of caveats to these estimates:

- The confidence intervals underrepresent the scale of the real error in the estimates, as this is simply the sampling error. The inaccuracy of the employee counts is unquantifiable but is likely to be significant given a) their basic nature and b) ownership structures.
- The figures themselves overstate the true measure of the burden on SMEs, for several reasons:
    - The data centre sector has a low employment density, whilst generating relatively high revenues. If the administrative burden of registration and incident reporting requires an additional employee, it is expected that the majority of DCOs would be able to meet the associated cost (not forgetting

[62] Second PIR of the Network and Information Systems Regulations 2018 - GOV.UK

[63] If we did not apply a threshold to MW IT capacity, an additional 2 SME DCOs (in the sample of 49 for which we have employment count estimates) would be included (along with an additional 2 non-SMEs). The percentage would change only slightly however – to 79% – because the total number of DCOs in the sample would be 53 instead of 49.

that the reason they do not currently do this is only that they are an exception which this Bill intends to address).

- The employment numbers represent only those employed by businesses registered in the UK. In many cases, these businesses are owned by much larger businesses – often large, US tech companies. Some of these businesses were created specifically for the purpose of operating a particular data centre, and the associated employee counts are thus a somewhat artificial representation of the true employment of the enterprise. 75% of relevant companies found on Beauhurst are not the ultimate parent.
- Where there is an expectation that DCOs meet certain standards, the burden is expected to be minimal, since the industry has made it clear to the Department that they already meet any relevant standards, without suggesting that smaller operators are an exception.

Impact on competition

A more predictable and cohesive operating environment for these sophisticated players in this market might be conducive to encouraging more competitiveness on a quality basis and hence investment. Similarly, a more secure business environment might encourage digital businesses to operate in the UK.

The Bill is expected to have a positive impact on competition by ensuring that all businesses, regardless of size or sector, adhere to consistent minimum cyber security standards. This reduces the ability of less secure firms to gain cost advantages by underinvesting in resilience, thereby promoting fairer market conditions lowering the barriers for entry for smaller businesses. The Bill will also improve trust across the digital economy, encouraging innovation and enabling smaller firms to compete more effectively by reducing the complexity and uncertainty associated with varying cyber security expectations. Furthermore, by strengthening supply chain security, the Bill supports more stable and competitive digital services.

Environmental impacts

The measures in the Bill are primarily focused on digital infrastructure, regulatory compliance, and risk management, rather than physical operations or environmental resources. As such, they are expected to have no direct environmental impact.

National security impacts

The Bill aims to mandate stronger cyber security practices across key sectors such as energy, transport, healthcare, and telecommunications. These sectors can be targets for cyber attacks; enforcing resilience minimises the risk of national-scale disruptions. By setting clear obligations for incident response and resilience planning, the Bill boosts national readiness to detect, respond to, and recover from cyber incidents. This reduces the strategic advantage of hostile states or cybercriminal groups aiming to exploit weak points in national systems.

The Bill seeks to ensure that third-party suppliers also meet security standards. This strengthens the entire ecosystem, preventing attackers from infiltrating sensitive systems through less secure contractors.

Sectoral impacts

The Bill is expected to be especially beneficial for digital businesses by providing a more secure and reliable digital operating environment. Mandatory cyber security standards will reduce vulnerabilities across sectors, which benefits all digital businesses by lowering systemic risk. Competitive businesses that rely on complex supply chains and digital infrastructure will benefit from knowing partners are also secure.

Compliance with the Bill's standards could serve as a trust signal to customers and investors. Businesses that demonstrate resilience are more likely to retain clients and contracts, especially in business-to-business environments where cyber security is a major factor in procurement.

Encouraging and enforcing resilience measures can help minimise business disruptions from cyber incidents. This is especially valuable to digital businesses where downtime equals direct revenue loss, like e-commerce, SaaS platforms, and fintech firms.

Impact on trade

High resilience standards can make UK digital firms more appealing to international clients and partners, especially in regulated industries. It aligns UK businesses with evolving global norms on cyber security, helping them export services or attract international investments.

11. Regulatory scorecard for preferred option

Part A: Overall and stakeholder impacts

(1) Overall impacts on total welfare		**Directional rating** **Note: Below are examples only**
Description of overall expected impact	The non monetised benefits aptly describes the welfare impact of these measures taken together. Reducing the negative effects of cyber attacks has a benefit to business and society as a whole.	**Positive** **Based on all impacts (incl. non-monetised)**
Monetised impacts	Total NPSV, 2025 present value: Best estimate: -£1,203m Low estimate: -£768m	**Negative** **Based on likely £NPSV - benefits not monetised**

	High estimate: -£1,741m	
Non-monetised impacts	Significant non monetised benefits have been identified which centre on the expected reduction in the prevalence and impact of cyber attacks. This will occur through bringing more entities in scope of the NIS Regulations, improving the enforcement of the regulation and facilitating greater sharing of information.	**Positive**
Any significant or adverse distributional impacts?	No	**Positive**

(2) Expected impacts on businesses		
Description of overall business impact	While compliance with the measures may incur a cost for businesses, it will bolster security and resilience, helping to reduce this estimated cost of cyber attacks. However, it is not possible to estimate what proportion of this cost will be averted through these measures as it is not possible to estimate the number of avoided attacks. The key benefit of the updated NIS Regulations outlined in the impact assessment is the expected improvement in security which would lead to a reduction in the risks posed to essential services. This in turn would benefit the UK's economic prosperity as there is a reliance on these services to support economic output and societal wellbeing. It is 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.	**Positive** Negative impact due cost of regulation however businesses impact from the prevention of cyber attacks is expected to be significant.
Monetised impacts	Business NPV: 2025 present value Best estimate: -£1,186m EANDCB: £137.7m, 2025 present value	**Negative** **Based on likely business £NPV**

		and lack of benefits
Non-monetised impacts	The benefits of these measures have not been monetised as it is not possible to accurately estimate the number of avoided cyber attacks. However, this measure will result in 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.	**Positive**
Any significant or adverse distributional impacts?	No	**Positive**

(3) Expected impacts on households		
Description of overall household impact	Households will not be directly impacted by the updated NIS Regulations. Households will experience the indirect benefit from the enhanced prevention of cyber attacks and their negative spillover effects on individuals.	**Positive**
Monetised impacts	N/A	**Neutral** **No impact to households**
Non-monetised impacts	Reduction in negative spillover effects from cyber attacks – indirect benefit	**Positive**
Any significant or adverse distributional impacts?	No	**Neutral**

Part B: Impacts on wider government priorities

Category	Description of impact	Directional rating
Business environment: **Does the measure impact on the ease of doing business in the UK?**	We expect the long term impacts of the Bill to be positive for the UK's business environment. Cyber attacks are disruptive and costly to business, creating an unstable environment in which to grow and innovate. The Bill seeks to reduce cyber attacks by bringing more entities into scope and empowering regulators to better enforce the security requirements, as well as reduce the impacts of any cyber attacks that do succeed by strengthening the intelligence available to regulators and government so that services can recover quickly. By stabilising the environment so that businesses can feel confident to expand and innovate without fear of a devastating cyber attack, this Bill will contribute to the Government's number one priority of growing the economy to the benefit of all.	**Supports**
International Considerations: **Does the measure support international trade and investment?**	The NIS Regulations 2018 were always intended to apply to any entity providing regulated services whether or not that entity is established within the UK. This remains the case, however, this Bill will bring more entities into scope across MPSs, data centres and large load controllers, some of which will be non-UK businesses. Therefore, for non-UK based businesses across these three groups, there may be additional costs associated with having to comply with regulations which could affect their willingness to operate in the UK. However, high resilience standards can make UK digital firms more appealing to international clients and partners, especially in regulated industries. It aligns UK businesses with evolving global norms on cyber security, helping them export services or attract international investments. Adverse impacts on trade are not expected.	**Supports**

Natural capital and Decarbonisation: **Does the measure support commitments to improve the environment and decarbonise?**	Load control plays a crucial role in supporting decarbonisation by optimising energy usage and integrating renewable energy sources more effectively. Requiring cyber security requirements in the load control market will increase consumer confidence in a nascent sector and encourage the adoption of smart, flexible energy solutions. This will go towards supporting decarbonisation and HMG's goals of Clean Power 2030 and Net Zero. Additionally, a secure, resilient load control market and wider UK grid will further encourage investment in smart energy accelerating growth in the sector and the adoption of sustainable energy practices.	**Supports**

12. Monitoring and evaluation of preferred option

The Bill will update the NIS Regulations 2018 to bring more entities into scope, better empower regulators to fulfil their duties and include proportionate powers to enable government to respond to emergency cyber threats. The NIS Regulations 2018 have been evaluated via two PIRs in 2020[64] and 2022.[65] These analysed how effective the NIS Regulations 2018 have been in achieving the original objectives to date, whether those objectives remain appropriate, as well as how the NIS Regulations 2018 had been implemented and the costs and benefits incurred. These reviews demonstrated that the NIS Regulations 2018 were largely working successfully in achieving in the objective "to prevent (where possible) and improve the levels of protection against network and information systems incidents". However, areas for improvement were set out, including recommended improvements to the NIS Regulations themselves. The PIRs also set out that whilst improvements to security were being made, organisations were not taking adequate steps to protect their systems from cyber attacks. In response, the previous Conservative Government conducted a consultation and subsequent analysis on proposed legislative measures to address the challenged identified in the PIRs and in response to the cyber landscape at those times.[66] The proposed legislative measures have formed the basis of the Bill, although they have been developed further and expanded upon to ensure that the Bill addresses the distinct challenges faced by the UK in 2025 and looking ahead to the future. Costs and benefits of the original legislative measures were set out in the consultation in 2022. However, since the conclusion of the 2022 consultation, further evidence gaps have been identified that will need to be monitored going forward, including the cost of compliance activities, how they vary by organisation (including for SMEs) and the time spent by businesses familiarising themselves with the legislation. Work is already underway to capture this. Through the process of putting this impact assessment together,

[64] PIR of the Network and Information Systems Regulations 2018
[65] Second PIR of the Network and Information Systems Regulations 2018 - GOV.UK
[66] Proposal for legislation to improve the UK's cyber resilience - GOV.UK

key metrics have been identified that can be tracked and measured going forward that will be able to gauge the success of the proposed measures.

There is a statutory duty for the Secretary of State to carry out a review of the NIS Regulations in intervals not exceeding five years. The next PIR of the NIS Regulations 2018 is currently due to take place in 2027. DSIT is reviewing whether this timing is appropriate to ensure the Bill has been fully implemented and had time to take effect once it has received Royal Assent. The next PIR will include carrying proportionate and appropriate research including:

a. **Process evaluation**: to assess the implementation of the measures and identify any unintended consequences. This will also inform how changes are being made to improve implementation of future reforms.

b. **Impact evaluation**: to establish causal links between the intervention and its outcomes compared to initial ambition of the measure in order to assess the scale of effects caused by the planned changes.

In preparation for future PIRs, and to support the ongoing implementation of the Bill and its evaluation, DSIT will undertake regular engagement with the NIS regulators through standing forums, and with industry and industry bodies (including, but not limited to, techUK and the Federation of Small Businesses). DSIT will conduct formal surveys to gather data and insights, which will then be analysed to inform evaluation which will contribute to future PIRs.

Under the proposed Bill measures, the Government will have the power to designate a statement of strategic priorities for NIS regulators. The Secretary of State will be required to report annually on regulators' progress in seeking to achieve the outcomes included in the statement of strategic priorities and will be able to require provision of information from the regulators to inform this report. The Secretary of State's annual report will be published in an appropriate manner to ensure that interested parties are sighted on regulators' progress at implementing the NIS Regulations. These annual reports will support monitoring and evaluation of the Bill and the NIS Regulations and will inform any future interventions from the government to improve the effectiveness of the regime.

The basis of both the impact and process evaluations will come from a more detailed version of the Theory of Change that was presented earlier in the assessment (Table 4.1).

As outlined in Table 4.1, below are the expected long-term outcomes and impacts of the preferred package of reforms:

- Outcome 1: Protect essential services and businesses so that the public can get on with their lives
- Outcome 2: Ensure that regulators are well-equipped to implement the NIS Regulations, creating a stable environment which fosters economic growth
- Outcome 3: Strengthening the UK's national security and ensuring the NIS Regulations remain effective in the context of an ever evolving threat landscape

The table below details the proposed methodologies and resources required in order to accurately and efficiently measure the success of the proposed policies within the Bill.

Table 12.1: Long run impacts of the package of reforms and how these will be monitored and evaluated.

Long Run Impact	**How this will be monitored and evaluated**
Protect essential services and businesses so that the public can get on with their lives	NIS PIRs Statement of Strategic Priorities annual reporting. Analysis of aggregate NCSC Cyber Assessment Framework returns data (demonstrates how well entities are managing cyber risks and meeting regulatory requirements in a particular sector).
Ensure that regulators are well-equipped to implement the NIS Regulations, creating a stable environment which fosters economic growth	NIS PIRs Statement of Strategic Priorities annual reporting. Regular surveys of NIS regulators Regular engagement with NIS regulators Analysis of aggregate NCSC Cyber Assessment Framework returns data
Strengthening the UK's national security and ensuring the NIS Regulations remain effective in the context of an ever evolving threat landscape	NIS PIRs Statement of Strategic Priorities annual reporting. Total NIS incidents – cyber incidences inc. Voluntary reports

Many of the impacts will rely on DSIT and others developing new data sources or new modelling that will fill current evidence gaps. In the risks and assumptions section of this Impact Assessment it is highlighted that the modelling assumptions have been made due to a lack of existing evidence. Where this is the case DSIT will ensure that there is a strategy for recording these going forward. The table below summarises these assumptions and the proposed ways forward in terms of their monitoring and evaluation:

Table 12.2: Evidence gaps and proposed monitoring and evaluation approach

Long run impact	Evidence gap	Proposed monitoring and evaluation
Increased supply chain resilience to cyber attacks	Understanding of the number of enterprise data centres in the UK which fall in the scope of regulation	Deep-dives into the UKBDS
Strengthening the UK's national security and ensuring the NIS Regulations remain effective in the context of an ever evolving threat landscape	Understanding of the counterfactual and current impacts of cyber attacks	Cyber Quantification project quantifies the economic cost of cyber attacks Cyber Assessment Framework review

		Reviewing annual informal and internal review of data by DSIT
Number of critical suppliers	Understanding the number of critical suppliers within each section that should be designated and brought in scope of NIS	Annual reporting from regulators on the suppliers they have deemed critical within their sectors

This monitoring and evaluation strategy relies on the use of the NIS PIR and analysis of aggregate NCSC Cyber Assessment Framework returns data. Should changes be made to these sources of data, any evidence gaps will be attempted to be filled, and access gained to the information and data necessary by the proportionate allocation of existing DSIT resources for evaluation, or through a competitive tender for new primary data collection, and synthesis of existing secondary data sources, to be done by an independent research agency.

As outlined in the benefits section of this Impact Assessment, a reduction in cyber incidents or cyber risk has not been possible to review given lack of a well-founded counter-factual position. Top-down metrics, such as the number of incidents, are still important to collect, however they are not good measures of the NIS Regulations' performance alone. An improvement in cyber security can lead to an increased number of incidents detected by an organisation, instead of a fall in incidents, as organisations with poor cyber security may not realise they are being breached. Both the 2020 and the 2022 PIRs collected information that allowed the assessment of whether the NIS Regulations 2018 were working to improve the cyber security of OESs through measures such as improvement plans.

DSIT currently has a plan to collect key performance indicators from regulators annually across 4 different areas:

1. Assurance and understanding
2. Improvements
3. Incidents
4. Capability

Assurance and understanding will focus on the Cyber Assessment Framework reviews and the number of organisations that meet the baseline and enhanced (if applicable) profiles. This will help assess the understanding that both regulators and organisations have as a result of the NIS Regulations. It will also assess whether regulators have a good understanding of their sectors' or geographical regions' cyber risk profile.

Improvements will focus on when organisations will meet the Cyber Assessment Framework profiles and whether improvement plans are being implemented and finished. Enforcement action will also fall under this section, to see if changes have been enforced upon organisations through the NIS Regulations. Successful enforcement activity which leads to additional compliance would be counted as a success for the purposes of overall improvements. It will also provide more insight as to the reason for the failure, enabling better monitoring of the sources of non-compliance in the future.

Incidents will look to capture total NIS incidents but also the number that are specifically related to cyber incidents. DSIT would also like to see an increase in voluntarily reported cyber incidents.

Finally, capability will capture the ability of regulators to carry out their regulatory function. This will allow DSIT to understand which regulators are struggling with resources and why this might be.

This annual informal and internal review of data by DSIT will highlight if there is a need to do a formal review in sooner timelines. DSIT may also consider evaluating the implementation of the NIS Regulations sooner if advice is received from the NCSC or the regulators that the NIS Regulations are not working as intended.

In addition to this annual data collection of key performance indicators, DSIT needs to capture the impact of separate areas in its monitoring plan, these are:

a. Costs
b. Benefits
c. Interaction with other regulations (Telecommunications (Security) Act 2021, Data Protection Act 2018, Online Safety Act 2023 and 'Secure by design')
d. Impact on innovation
e. Impact on trade
f. Impact on competition

Costs

DSIT already has good data on costs through the previous two PIRs and speaking directly to organisations that are regulated under the NIS Regulations 2018. The costs of the additional requirements need to be captured in the next PIR. Questions should be selected that allow DSIT to state what the costs have been from the original NIS Regulations 2018 and what the cost has been from the changes introduced by subsequent amending of the updated NIS Regulations. Some costs that need to be better understood:

- The costs (if any) of contract change as a result of being designated by the NIS Regulations.
- The costs of reporting an incident by organisations. Further data should be collected in the future to better understand both the costs of reporting an incident by organisations as well as estimates of optimism, taking into account the new reporting timelines.
- The number of critical suppliers that are to be designated and the costs to these entities.
- The costs incurred by organisations as a result of regulators recovering the costs of enforcement activities. This will involve engaging with regulators to understand how this power is used, as well as collecting data from organisations on the magnitude of the costs incurred and the impact of this.

The methodology for assessing the costs of the NIS Regulations will be similar to previous PIRs. It will need to consider the number of new organisations that were designated as a result of these measures, how many incidents have been reported as a result of these

measures and whether the set-up costs of the critical suppliers measure were accurate. The costs will be split out on a measure-by-measure basis.

As previously stated, it is difficult to understand the monetary value of the benefits of the NIS Regulations, however, DSIT is looking to overcome these issues. DSIT has worked with cross-government stakeholders to better understand how to quantify the economic cost of cyber-attacks and therefore the value of preventing them.

The Cyber Risk Quantification project seeks to quantify the economic cost of cyber attacks against all entities, including consumers, government, and businesses. The output of the project provides an overarching view of the potential impact of cyber attacks to the UK economy, including those sectors covered by the NIS Regulations.[67]

Interaction with other regulations

The number of regulations in the digital space is increasing, requiring organisations to comply across different areas. The increase in regulation reflects how pivotal they have become to daily life. How these regulations interact with each other should be monitored to establish whether they are overburdensome, even to large organisations.

In order to do this, regulations that may or do overlap with the NIS Regulations will be mapped out. DSIT will ensure that the views of the organisations that have an overlap with other regulations are captured. Costs will need to be reviewed as to whether the regulatory overlap creates an increase in costs above what they would cause separately or whether there will be some savings by only being required to meet one standard of cyber security.

Impact on innovation

DSIT has already collected information on the impact on organisations' ability to innovate and it will continue to collect this in subsequent reviews. The questions should probe on different areas of innovation to test whether the NIS Regulations have an impact on the ability to innovate on cyber security and more generally the offering that an organisation provides.

Impact on trade

DSIT will continue to collect information to inform the potential impact of the regulations on prices, which will in turn serve to understand the potential impact on UK suppliers' competitiveness. In addition to this, subsequent reviews should also seek to collect information on whether organisations have perceived an impact on their ability to trade as a result of the NIS Regulations. This will help in assessing whether trade activities have been impacted through channels other than prices.

Impact on competition

DSIT will collect information on the concentration of the markets that will be impacted by the changes suggested in the Bill over the next year to baseline the competition review. This will then be collected every year to monitor whether there are big changes in the market

[67] https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk

and if they are, DSIT will do a deep dive to understand whether this change has been because of the NIS Regulations.

Collecting information on whether the NIS Regulations have an impact on the prices that organisations change will help to assess whether the NIS Regulations have had any impact on an organisation's ability to compete in the market. If businesses don't increase costs or only have small increases, it is unlikely that the Regulations are having a large impact on competition.

Impact on households

In order to assess the impact of the Regulations more broadly, DSIT will consider the evidence on the impacts of the NIS Regulations to trade, innovation, and competition to evaluate the extent to which households are impacted.

13. Minimising administrative and compliance costs for preferred option

Cyber attacks are costly to businesses and operators of services, as set out above in the 'benefits' section. A primary purpose of the Bill is to decrease the number of cyber attacks and, where a cyber incident does occur, minimise the impacts of the attack on individuals and businesses. In the longer term, the Bill's measures seek to save businesses money and stabilise the environment in which they can grow and innovate. This in turn seeks to grow the economy to the benefit of working people.

In the shorter term, the government recognises that the Bill's measures will expand regulator responsibilities and require more action to be taken by businesses and essential services to secure their networks. There is expected to be some administrative burden on organisations as they familiarise themselves with the updated NIS Regulations and participate in an expanded incident reporting framework. For those organisations being brought into scope of the NIS Regulations (e.g. data centre operators), they will be required to take the steps already being taken by those in scope of the NIS Regulations 2018 to secure their networks and assess their cyber security measures. Where appropriate, the government will produce guidance to help organisations comply and it will continue to work closely with the sector to monitor the implementation of the updated NIS Regulations. An implementation period will be set during Bill passage to ensure that affected organisations have sufficient time to prepare for the changes. The length of the implementation period will be decided on in consultation with stakeholders and it will consider the impacts on small and micro businesses. Furthermore, the measures to be set via secondary legislation (including updated supply chain security measures) will be formally consulted on it, within which the costs to businesses will be carefully considered.

In sum, government will seek to minimise any costs to business via an implementation period, guidance and formal consultations where appropriate. The Bill's measures have been designed to strike the right balance between urgently needing strengthen the security of a large range of regulated entities and ensuring that any regulation is not burdensome to business. Any cost to organisations to implement updated NIS Regulations are minor in comparison to the potential impact of a disruptive cyber incident, as demonstrated by recent instances of cyber attacks in the UK.

14. Declaration

Department:

Department for Science, Innovation and Technology

Contact details for enquiries:

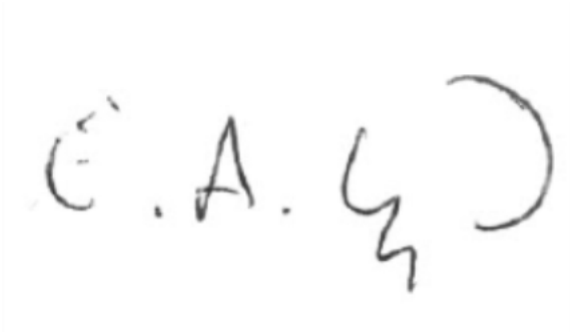
Kelly North, Deputy Bill Manager, kelly.north@dsit.gov.uk

Minister responsible:

Liz Lloyd, Parliamentary Under Secretary of State (Minister for Digital Economy)

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed:



Date: 31 October 2025

Annex A. Summary: Analysis and evidence

For Final Stage Impact Assessment, please finalise these sections including the full evidence base.

Price base year: 2025

PV base year: 2026

	1. Business as usual (baseline)	**2. Preferred way forward (if not do-minimum)**
Net present social value (with brief description, including ranges, of individual costs and benefits)	N/A	Best estimate: -£1,201m Low estimate: -£766m High estimate: -£1,740m There is a significant negative NPSV due to the lack of monetised benefits in the impact assessment, as justified throughout. The most significant costs stem from the new entities that are being brough under the NIS Regulations, and the ongoing cyber security costs they will experience to be coherent with the regulations.
Public sector financial costs (with brief description, including ranges)	N/A	There will be some costs for the 13 regulators, 12 of whom are already tasked with enforcing the NIS Regulations 2018. They will undergo the costs of familiarising themselves with the new legislation and some will face greater costs from having to regulate more entities. However, the measures here will empower regulators to drive compliance and ensure they have the resources and vital intelligence needed to fulfil their duties. Also, the measures will equip government to take decisive action to protect our national security. Additionally, public sector organisations falling in scope of the legislation will incur familiarisation and compliance costs. These have not been considered separately in the analysis and are include in aggregate cost figures to OESs.

Significant un-quantified benefits and costs (description, with scale where possible)	N/A	There are significant un-quantified and non-monetised benefits resulting from these measures. The key benefit of this Bill is to protect businesses from cyber attacks to foster an environment in which investment and innovation can thrive. Having better defences against cyber attacks, achieved by bringing more entities into scope and empowering regulators to better fulfil their duties, will reduce the time businesses must take to deal with cyber attacks, often halting their services to do so. When an attack does occur, improved incident reporting will allow regulators and NCSC to use this information to provide advice and guidance to, and to engage with, other businesses and organisations. This will enable them to take action to protect themselves and mitigate the wider impacts of the specific an attack or type of attack. While compliance with the measures may incur a cost for businesses, it will bolster security and resilience, helping to reduce this cost of cyber-attacks. However, it is not possible to estimate what proportion of this cost will be averted through these specific measures as it is not possible to estimate the number of avoided attacks.
Key risks (and risk costs, and optimism bias, where relevant)	N/A	The key risks stem from potential underestimation of costs within this impact assessment. However, assumptions have been informed through evidence gathering during the initial NIS Regulations 2018 IA development, and improved through the two PIRs that have taken place since the commencement of the regulations. A significant cost of this Bill falls on RMSPs as they will now fall in scope of the regulations. DSIT commissioned bespoke research to estimate the number of RMSPs that will come into scope, reducing the risk associated with incorrectly estimating the cost to these entities.
Results of sensitivity analysis		The most significant cost falls on the new entities being brought into the NIS regulations. These are RMSPs, data centres, large load controllers and designated critical suppliers. These are the costs of ensuring their cyber security is sufficient with the regulations, and the cost of reporting incidents. It was not possible to estimate accurately the number of critical suppliers that will be designated. The other three groups have been analysed, with costs provided in ranges through the use of a low, central and high scenario.

		Further sensitivity analysis outlined in the Cost section showed that the overall NPSV is particular sensitive to the estimated cost of annual additional cyber security spending for newly in scope firms. Changing the per firm assumption by 20% would increase or decrease the NPSV and EANDCB by 15%. To a lesser extent, the analysis is sensitive to the estimated incident reporting costs associated with the new reporting timeline. 20% changes to these costs would result in a 3% shift in the NPSV and EANDCB.