Department for
Science, Innovation
& Technology

Protecting and enhancing the security and resilience of UK data infrastructure

Public consultation

Closing date: 22 February 2024

December 2023

Any enquiries regarding this publication should be sent to us at: alt.formats@dsit.gov.uk

Ministerial Foreword

Data, and its associated infrastructure and services, are increasingly crucial to the UK's economy, future growth and security, and are therefore strategically important at a national and global level. Without functioning, secure and reliable data infrastructure, the UK will be unable to innovate or compete in the global economy.

Data infrastructure refers to data storage, processing, or transmission assets and services; including the physical, logical and virtual infrastructure that is the foundation of the digital service economy, and an increasing proportion of the whole economy. The data centre sector in particular is now of critical underlying importance to economic activity, delivery of public services and the everyday lives of millions of people in the UK.

The UK data centre market is amongst the most advanced and commercially and technologically sophisticated in the world. The government intends to continue to build the right business environment that encourages investment into the sector, allowing for its growth and continued innovation, and ensuring capacity can meet the UK's ambitions for economic growth, scientific progress and safe development of artificial intelligence and other new technologies.

However, the abundance, importance and value of data accumulating in or passing through such infrastructure makes it an attractive target to those who may have the intention or capability to threaten the UK's national security, economy, or ways of life, or seek access to

data for other malign or criminal purposes. Like any infrastructure, data centres can also be vulnerable to natural phenomena, especially extreme weather, which have the potential to disrupt continuity of data access.

Ensuring the security and resilience of data storage and processing infrastructure is of national interest. The UK government's unique position as steward of the economy and society, with sight across the entire system, means we have a responsibility to identify aggregate, emergent and national security risks that may not be a priority for any single organisation or sector. The Department for Science, Innovation and Technology (DSIT) - working with relevant departments and agencies across UK government - have identified and evidenced a range of risks to the security and resilience of data infrastructure in the UK.

This consultation sets out our proposals – developed through ongoing consultation with relevant industry stakeholders and experts – to improve and assure the ongoing security and resilience of UK data infrastructure. We propose to introduce a new, proportionate statutory framework, focused on data centres, to ensure all relevant operators in the UK are appropriately mitigating risks where they are relevant to the national interest, and national security in particular. This framework would be applicable in future where other risks emerge, especially as a result of new threats, technological developments and commercial models.

We look forward to constructive discussions with industry, experts and other interested parties.

Rt Hon John Whittingdale OBE MP

Minister for Data and Digital Infrastructure

Department for Science, Innovation and Technology

Contents

General information

Why we are consulting

This consultation will gather further views and evidence to inform development of proposals to improve and assure the security and resilience of UK data infrastructure. Proposals focus on third-party data centre services, which face:

- Security threats such as cyber attacks, physical attacks, and insider threats.
- Resilience risks resulting from hazards such as equipment malfunction and extreme weather.
- Poor information-sharing and cooperation across industry, and with HMG, which hamper our ability to appropriately identify and address risks.

The proposals focus on a new proposed statutory framework applying to UK-based data centre services provided to third parties, but potentially applicable in future where other risks are evidenced.

Following this consultation, we will carefully consider views and evidence, which will inform our response and any further proposals. This consultation will be complemented by continued engagement with industry, experts, across UK government departments and agencies, and with international partners to further inform policy development and implementation to address risks related to UK data infrastructure.

Consultation details

Issued: 14/12/2023

Respond by: 23:55 22/02/2024

Enquiries to: disr-consultation@dsit.gov.uk

Consultation reference: Protecting and enhancing the security and resilience of UK data infrastructure.

Audiences:

The government invites feedback from any interested party, but in particular:

- Data centre operators
- Data centre land and facility owners
- Cloud platform providers
- Managed service providers

- Customers and suppliers of the providers above
- Independent or academic experts on data storage and processing

Territorial extent:

All of the UK.

How to respond

Outline whether responses should be provided in a particular preferred format, where electronic responses should be emailed to, which address to send hardcopy responses to, whether to use different addresses for responses for the devolved administrations, etc.

Respond online at: https://dsit.qualtrics.com/jfe/form/SV_ea09NEjZX9XFVki

or

Email to: disr-consultation@dsit.gov.uk

A response form is available on the GOV.UK consultation page: www.gov.uk/government/consultations/protecting-and-enhancing-the-security-and-resilience-of-uk-data-infrastructure

This consultation will run until 23:55 on 22/02/2024. We welcome all forms of insight from any category of stakeholder. You can respond as an individual or on behalf of an organisation.

We particularly welcome input from data centre operators, cloud platform providers, managed service providers and other relevant market actors such as customers and suppliers, as well as independent or academic experts on data storage and processing. Please note which services your business or organisation provides or relation to the outlined proposals.

We would appreciate it if respondents can note their level of certainty for any factual statements and wherever possible provide evidence to support them. Where businesses express views, we would be grateful for responses from senior representatives responsible for security and resilience, or compliance. If responsibility for risks is shared across multiple roles, responses from the senior risk owner are preferred for each risk, where relevant. If organisations operate multinationally, we would prefer the leader responsible for security and resilience of UK-based operations to respond, but we welcome views reflecting experiences in other jurisdictions.

We ask that responses are submitted online at https://dsit.qualtrics.com/jfe/form/SV_ea09NEjZX9XFVki. If you would like to provide a response via email, please complete the consultation response form, on the consultation web page, and send it to us at disr-consultation@dsit.gov.uk. In exceptional circumstances, if you need to submit a hard copy, please contact us at disr-consultation@dsit.gov.uk and we will advise how to do this. Should you require another format (e.g. braille or large font) please contact disr-consultation@dsit.gov.uk.

When submitting your response, please state:

- which questions you are answering (there is no need to respond to all questions if they are not all relevant to you);
- whether you are willing to be contacted (if so, please provide contact details);

- whether you prefer for your response to remain confidential and non-attributable (if so, please specify).

Responses will be analysed by the Department for Science, Innovation and Technology (DSIT). The Department will process the information you have provided in accordance with the Data Protection Act 2018 (DPA).

The information you provide will be used to shape future policy development and may be shared between UK government departments, government-approved regulatory authorities, the National Cyber Security Centre (NCSC) and the National Protective Security Authority (NPSA) for this purpose. Personal information will be removed in such instances. Copies of responses, in full or in summary, may be published after the consultation closing date on the Department's website with personal data removed.

We will publish a formal response to this consultation following analysis of the responses.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@dsit.gov.uk.

Executive Summary

Purpose of consultation

The National Data Strategy (2020) set out the government's commitment to create a stronger risk management framework to protect the infrastructure on which data use relies. Subsequent government strategies have further emphasised the need to take such action, including the Integrated Review Refresh (2023), UK Government Resilience Framework (2022) and the National Cyber Strategy (2022).

This consultation builds on the views and evidence gathered through our Data storage and processing infrastructure security and resilience - call for views (2022), subsequent industry and expert engagement, and continued UK government and security agency assessment and analysis. It sets out and seeks views on the government's intention to introduce a new statutory framework to mitigate risks to the security and resilience of data stored and processed in the UK, focused on data centres, but potentially applicable in future to other existing or emergent 'data infrastructure'. It also outlines voluntary action and other measures to support this.

Rationale for intervention

The government recognises that the value and importance of data concentrated in and transmitted through data centres presents an attractive target for a range of malign and hostile actors. There are also vulnerabilities resulting from natural hazards, including extreme weather, as well as other events that may disrupt access to data that is crucial for our economy, public services and everyday lives. The government has identified and evidenced existing risks that are currently unmitigated, under-mitigated, or inconsistently mitigated.

Whilst commercial drivers often result in high security and resilience standards, corporate and commercial interests are not always aligned with, or do not go far enough to reflect, national interests, including protection of the UK's national security. The criticality of data centres to our economy means that the national harm resulting from significant security or resilience shocks could be far greater than commercial harm to any one operator, and thus commercial drivers are not sufficient to drive the level of security/resilience standards required in the national interest.

Whilst some oversight of risk mitigation exists through security and resilience-focused regulation of certain sectors within the economy which have a dependency on data centres within their supply chains, this does not account for systemic risk and cross-economy dependency on data centres. The government's assessment is that it provides insufficient security and resilience oversight of the data centre sector given its national importance. The range of risks and their potential impacts present a precautionary case for considered government action and intervention.

Government approach

The government intends to take a proportionate, sequenced and iterative approach to risk mitigation, including through a proposed new statutory framework and regulatory function.

This regulatory function would, at a minimum, have statutory regulatory oversight over organisations that operate date centres, in particular, those that provide colocation and co-hosting data centre services as a third-party provider (see Scope section for further detail). We refer to these data centres as “third-party data centres”. It would seek to establish a baseline level of mitigation against security and resilience risks by all UK third-party data centre operators.

This would be complemented and informed by continued work on voluntary measures and industry support structures. We envisage close working between government and industry to encourage better information-sharing, and exploring Critical National Infrastructure designation for critical systems, or data infrastructure more broadly. We will also seek to explore wider risks to the growth and resilience of the sector.

The statutory framework would be designed to include appropriate powers to adjust the scope and approach in response to the evolving risk landscape and rapidly developing technologies. We propose that additional or more reaching requirements could be set if industry does not sufficiently mitigate identified risks under the proposed ‘baseline’ approach.

Proposals have been designed modularly to allow implementation through various potential legislative mechanisms, including existing statutory frameworks.

Proposed statutory framework

Scope: third-party data centres, in particular, those being implemented to provide colocation and co-hosting data centre services.

It is intended that organisations that operate these data centres or provide these services, and so fall within the scope, would be required to undertake or comply with the following:

Registration: relevant data centre providers would be required to register with the designated regulator and provide relevant information regarding their UK operations.

Security and resilience measures: relevant data centre providers would have a duty to take appropriate and proportionate technical and organisational measures to manage risks to security and resilience of these services. Baseline measures may relate to:

- risk management;
- the physical and cyber security of facilities, networks and systems including measures targeted at specific areas or functions (for example, meet-me rooms);
- incident management;

- resilience and service continuity;
- monitoring, detection, auditing and testing;
- governance and personnel;
- supply chain management.

Standards, assurance and testing: standards, assessment frameworks and other tools can be used to improve and assure security and resilience mitigations. To enable this, the government would introduce a range of mechanisms which could be used by a regulator to mandate assurance of, and provide assurance beyond, baseline security and resilience measures.

Incident reporting: relevant providers would be required to report significant incidents to the regulator, and in some cases disclose incidents to customers or other affected parties.

Regulatory function: a regulatory function would be established with the appropriate remit, powers and capability to implement, manage and enforce the new framework. This function would take a risk-based, proactive approach, based on the principle of proportionality and with a duty to consider growth and innovation when exercising its functions.

We do not intend to identify an existing, or propose the establishment of a new, regulatory body until further views on the proposed framework have been received and assessed.

Next steps

The government will carefully consider views and evidence gathered through this consultation to inform our response and any further proposals. We will continue to engage closely with relevant stakeholders to inform the development of any statutory intervention and to address individual and collective risks outside this. We will also seek to engage further with governments of other jurisdictions to explore collective risk mitigation and joint action to address shared risks and threats.

Introduction

Context and purpose of consultation

Data, and its associated infrastructure and services, are increasingly crucial to the UK's economy, future growth and security, and are therefore strategically important at a national and global level. The UK and global economy have become increasingly digitised, and many businesses and organisations outside the digital economy now rely on data storage and processing to fulfil everyday functions. The infrastructure underlying this is therefore now a crucial part of the economy.

In addition, data use is opening new opportunities for businesses, services and citizens. Secure and reliable access to data is crucial to expand and improve our use of technology, drive innovation, analysis and decision-making. It is also a key prerequisite for boosting productivity, attracting investment, connecting communities and regions, establishing the UK as a science and technology superpower, and enabling UK authorities to fight crime and terrorism and protect our borders.

The UK data economy represented 6.9% of GDP in 2022, and 76% of UK service exports worldwide are data-enabled. As a greater proportion of our work and lives is digitised and the benefits of data innovation become clearer, the generation, collection and use of data grows, prompting further demand for data storage, processing and transmission capacity.

Data and the infrastructure it relies on therefore has a direct relationship to many of the UK government's priorities, and especially achieving our ambition for the UK to be recognised as a science and technology superpower by 2030.

The National Data Strategy (2020) set out our commitment to creating a stronger risk management framework to protect the infrastructure on which data use relies. Subsequent government strategies have further emphasised the need to take action to ensure security and resilience risks are robustly addressed, including:

- The Integrated Review Refresh (2023) which emphasises critical technologies, infrastructure and data access as priorities for UK government in national security and foreign policy thinking, and recognises the complexity of interconnected and network risks.
- The UK Government Resilience Framework (2022) which emphasises that regardless of the risk, pre-emptive action must be the foundation of the UK's resilience.
- The National Cyber Strategy (2022) call which seeks to improve cyber resilience and create better management of cyber risks across UK organisations to prevent and resist cyber attacks, as well as increase our ambition on cyber resilience for Critical National Infrastructure in the face of higher threat levels. This includes strengthening the protection of data when processed, in transit, or stored at scale.

The growing importance of data infrastructure has led DSIT to closely examine risks, dependencies and existing mitigations. Early assessment established that the primary unaddressed areas of risk were borne by data centres, and in particular third-party data centres.

This consultation sets out a series of proposals that the government considers will, together, enhance the security and resilience of third-party data centres, and provide a suitable statutory framework to allow for oversight of any further existing, emerging, or future technologies or commercial applications for data storage or processing where risks are deemed to be of sufficient national importance.

The data centre market in the UK

Data centre provision is fundamental to, and highly integrated into, the technology-stack, but it has also emerged as an important and distinct sector in its own right with its own commercial pressures, market models, public policy requirements, and need for highly skilled, professional personnel.

The UK has a dynamic, growing and developed data centre market. Whilst there are no current registration requirements to determine precise figures, DSIT estimates there are around 170 colocation data centre operators managing at least 250 colocation sites in the UK. Of these 170 operators, around 80 also provide Managed Service Provider (MSP) services. The total number of data centre operators in the UK is around 800, including MSP-only operators. Total revenue is estimated at £4.6bn per year (2021). The industry is concentrated, with 80% of this revenue being generated by the largest 10 operators.

The UK Business Data Survey 2022[1] indicates that 28% of all UK businesses use services housed in data centres (either directly or indirectly via the cloud). For large businesses (with at least 250 employees) this is 62%.

We estimate that current data centre outages cost the industry in the region of low single-digit billions per year. It is also estimated, based on research published separately, that the knock-on cost to customers as a result of a loss of productivity amounts to, for 2019, approximately £0.7bn. It is anticipated that this would be significantly higher during a prolonged or systemic outage in the sector. More information can be found in Annex A.

Risks

In recent years UK government has looked in greater detail at the data centre sector, whilst continuing to examine where other economic actors are subject to risks regarding the security and resilience of data that are not mitigated by existing oversight. We have:

[1] https://www.gov.uk/government/statistics/uk-business-data-survey-2022

- Issued a Call for Views on risks to data storage and processing infrastructure, the response to which affirmed and built upon the government's view and evidence of existing and emergent risks.
- Worked with the National Cyber Security Centre (NCSC) and National Protective Security Authority (NPSA) to assess, examine and test the security of a sample of data centres, including through voluntary audits. Prior to this, in March 2022, NPSA and NCSC released joint data centre security guidance for owners and users.
- Worked with Cabinet Office, industry and others to build a picture of critical dependencies and vulnerabilities.
- Engaged with the data centre sector, other relevant industry actors and experts to test our analysis of risk and explore potential mitigations.

This examination has identified and evidenced a range of existing security risks and vulnerabilities in UK data centres (potentially relevant to other or future elements of data infrastructure). These risks are related to technology, people and processes that can be exploited by malign actors, or result in disruption, and include:

- Vulnerabilities within data storage and processing infrastructure and the technologies that make it up, that may be exploited in a cyber attack.
- Physical attack or infiltration of data storage and processing infrastructure facilities and 'grey spaces'.
- Insider threats and human error: data storage and processing infrastructure staff, contractors or customers misusing privileged access or credentials.
- Equipment and system failures.
- Security and resilience vulnerabilities in supply chains.
- Ownership, influence, or control of data infrastructure by those seeking to do harm to the UK.

We have also identified natural hazards and externalities which present significant resilience risks, including in the longer term:

- Natural hazards such as fires, floods and extreme temperatures.
- Disruption to specific services provided to data storage and processing infrastructure, especially the electricity grid and equipment supply chain.
- Geographical and economic concentration of infrastructure, operators or the market, including site proximity and points of interconnection.
- Wider economic disruption, including where this may result in insolvency of data infrastructure operators or major customers, affecting overall supply and capacity, or severely reduce demand and revenue.

It is probable that the risk and frequency of many of these threats, hazards and vulnerabilities manifesting will increase over time, as the attack surface across sites and interconnected infrastructure grows, means of penetration evolve and become more sophisticated, and natural

hazards intensify with climate change. There are also likely to be new and evolving risks, including from emerging technologies such as quantum computing and artificial intelligence.

The government has engaged closely with relevant industry actors and experts to better understand these risks and how they are mitigated. Information-sharing and coordination between data storage and processing infrastructure operators and the government is facilitated informally, ad hoc or by trade bodies. In comparison to other areas of critical infrastructure, there is limited formal information-sharing between industry and government, and an absence of statutory regulatory oversight or independent testing of security and resilience risk management controls and management. Without a framework that puts appropriate information-gathering on a statutory footing, and a regulatory function with sufficient capability, expertise and levers to implement this, the UK government has limited ability to:

- support private sector operators;
- oversee and manage wider risks, some of which may not be in individual economic actors' direct control, across multiple sectors that provide critical national infrastructure.

Rationale for action and intervention

Since the publication of the National Data Strategy, the government has also taken steps to better secure our key digital services and associated data infrastructure through:

- Implementation of the National Security and Investment Act 2021, with data-related services and infrastructure represented across many sectors deemed critical enough to require mandatory notification of acquisitions.
- Implementation of the Telecommunications (Security) Act 2021, including the publication of its accompanying regulations and code of practice.
- Publication of proposals to update the Network and Information Systems (NIS) Regulations 2018.
- Publication of two calls for views on the security and resilience of data storage and processing infrastructure, and software for businesses and organisations.

Our examination of risks and threats to data infrastructure has indicated the speed of growth and evolution of relevant sectors and commercial applications and dynamism of the market in general, and in data centres in particular. It has also indicated the potential for new technologies to disrupt current commercial models and risk mitigations. For example, increased demand for low latency and trends towards the edge may lead to a greater geographical distribution of physical sites and assets, providing benefits, but also increasing the attack surface beyond regional data centre facilities, building the aggregate risk.

The UK data centre market is amongst the most advanced, developed, and commercially and technologically innovative in the world. The government intends to continue to build the right business environment that encourages investment into the sector.

The government recognises that the value and importance of data concentrated and transmitted through these sites presents a highly attractive target for a range of malign and hostile actors. More generally, currently unmitigated, under-mitigated, or inconsistently mitigated risks have been identified and evidenced.

We recognise that commercial drivers often result in high security and resilience standards; UK data centre operators are already incentivised to maintain good security standards for commercial reasons. However, corporate and commercial interests are not always aligned with, or do not go far enough to reflect, national interests. For instance, colocation data centres may rely on the explicit demands of their customers to put in place mitigations, rather than produce an independent assessment of what measures are commensurate to the aggregate risk to all supply chains to which they belong. They may introduce security and resilience measures to mitigate a certain level of risk, but deem any greater risk to be “force majeure” and therefore exempt of liability and not worth investing in mitigating. Or they may tolerate low impact threats and hazards, despite the aggregate impact of these being significant across systems or nationally. This is of particular risk to the national interest where there is a concerted attempt at disruption to or exfiltration from multiple sites, or climatic events such as heatwaves.

Furthermore, private sector operators do not have direct responsibility, remit, nor access to privileged information or relevant legal or operational levers to address such risks to the national interest or national security. And, given the rapidly evolving technological and threat landscape, even where commercial drivers and models may appear commensurate to perceived risks, these may change over time.

Commercially driven security standards and other risk mitigations are also inconsistent across operators and sites. Our voluntary reviews of UK data centres, whilst confirming generally high standards, also identified inconsistencies, limitations and gaps. The government recognises that some of these inconsistencies are in some cases intentional and by virtue of varying business models, but the level of inconsistency indicates that this goes beyond cost offerings and presents a strong case for harmonising standards and ensuring a baseline of risk mitigations.

Our public Call for Views collected a wide range of perspectives regarding the security and resilience of data centres, including assessments of the insufficiency of existing risk management and recommendations for government on how to address them. In particular, this analysis has identified that third-party data centres are exposed to significant risks. Whilst some oversight risk mitigation exists through regulation of specific sectors, that may be customers, or operate interdependent infrastructure, this is partial and does not account for systemic risk and cross-economy dependency on data centres themselves. This is deemed as insufficient supervision and protection of the sector, given its national importance.

There are further risks to resilience of data access with significant potential impacts. The dependence of the UK on data infrastructure generally (and the data centre sector specifically) implies a potentially catastrophic scale of impact in a reasonable worst case scenario outage for particular individual data centres, or a number of data centres at once.

The extent of risks and their potential impacts present a precautionary case for considered government action. Where such impacts have an unknown likelihood, the government has grounds to invoke the precautionary principle.[2] This means that the risk should be treated as sufficiently likely to warrant mitigation. The use of this principle is in line with HMG's recent refocus on proactive and preventative action to ensure resilience.[3] Third-party data centres are currently not directly regulated for security and resilience in the UK, unlike other similar sectors, and unlike the approach taken in some other major economies.

The government has concluded that third-party data centres are subject to a level of risk and potential impacts that warrants greater intervention. Unlike many critical sectors, at present there is an absence of oversight, assured testing, governance and statutory mechanisms to defend against threats to evidenced and serious security and resilience risks. The current regulatory landscape and market dynamics address some risks, but do not provide the information, tools, or levers required for the government to effectively manage risks presented to the national interest. Given the scale of risk and potential impact, it is appropriate to establish proportionate oversight and assurance to protect the UK's economic and national security, as well as its reputation for good governance and as a secure, stable and lawful place to innovate and do business.

Such action would be in line with intervention taken in a number of other countries with comparable economies. For example, Australia and Germany have legislated for a suite of obligations on critical national infrastructure operators including data centres. This includes reporting obligations, security and resilience requirements, government audits and a range of penalties for non-compliance.

Putting in place a considered and proportionate framework that balances compliance costs with strengthened security and resilience, complemented by other voluntary measures and support, would have benefits for investability for the sector and for the UK as whole.

Government approach

As well as mitigating risks and vulnerabilities, the government's intention is to build confidence in the stability and security of the UK data infrastructure and data innovation market. Our desired outcome is to increase UK competitiveness in the global digital economy, and more broadly deepen assurances around the exportability of the UK services economy which at its foundation is reliant on data centres.

The government proposes to take a proportionate approach to mitigating the risks we have identified, carefully considering commercial and wider economic realities and sensitivities. This includes consideration of laws that businesses may be subject to globally and in other jurisdictions. Where possible, we would adopt alignment or interoperability with these

[2] RPC guidance note on 'using the precautionary principle'
[3] See the UK Government Resilience Framework

requirements and processes to minimise burden. Although, where warranted, by risk or operating context, we would take a UK-specific approach.

DSIT (and relevant government agencies) intends to work with relevant industry actors to explore further collective voluntary mechanisms to build on individual actions, whilst developing a statutory framework and function that would assure a baseline level of security and resilience across the sector. Any such intervention would be mindful of commercial and market pressures and dynamics.

We anticipate UK data centre operators will take a responsible and accountable approach to this work, as they have through their close engagement during the exploration and development of these proposals. Operators should not hold back on taking appropriate action to further mitigate risks now – we expect them to take individual and collective action. This includes participating in improved government-industry fora, and in the development of relevant industry codes of practice with the UK government and its agencies, in advance of any statutory implementation.

The nature of threats to security and resilience do not allow for complete and comprehensive risk prevention. There is also a need to carefully balance the trade-offs between security and resilience against innovation and investment, as well as costs to the taxpayer in implementing interventions.

We have carefully examined risks, mitigations and market dynamics and have built an evidence base supporting a case for intervention. Data and evidence in regard to risks and mitigations is not always consistently available or fully representative in sample size. This is largely the result of an absence of legal reporting obligations, or a statutory regulatory function to oversee and engage with relevant market operators with the backing of information-gathering powers.

As part of the proposed statutory framework, the government therefore proposes to empower a regulator with the appropriate remit and levers to supervise and enforce, but also to continuously monitor, and work with others to monitor, the risks and the market (see Framework overview). This function would initially have supervisory responsibility over data centres that provide services to third parties, for which there are already evidenced risks. It would have a further responsibility to gather evidence on other relevant activity in relation to data storage, processing and transit services to assess if similar risks to the security and resilience of data exist in other commercial sectors, applications, or functions.

The proposed regulatory function would be complemented in parallel by continued work on voluntary measures and industry support structures. This will include exploring Critical National Infrastructure designation for critical systems or data infrastructure more broadly, and close working between government and industry. We will also seek to explore wider risks to growth and resilience of the sector.

In the meantime, a lack of certainty is not grounds to avoid carefully considered statutory intervention, and we propose to empower and instruct a regulator to supervise baseline security and resilience requirements, with the potential to set further or more reaching

requirements if necessary and if industry does not sufficiently mitigate identified risks under the proposed ‘baseline’ approach (see Security and resilience measures).

Requirements would be appropriate, proportionate and, wherever possible, outcome-based and standards-aligned. They would be designed based on modern good practice to level the playing field and raise the bar where there are individual vulnerabilities, deficiencies and inconsistency across the sector.

We also propose incident reporting obligations, as found in similar statutory frameworks for critical infrastructure, that would facilitate better understanding and management of significant incidents. This would be carefully calibrated and adjusted by the regulator to avoid over- or under-reporting (see Incident reporting).

Given the rate of technological and market development, it is important that any framework is flexible and therefore future-proofed. We therefore propose to design a power to allow the government to adjust the scope of this statutory framework, to be exercised where new developments result in new risks to security and resilience of relevant physical or virtual data infrastructure. Within that scope, the framework itself would grant flexibility to the regulator in how it manages risk, and appropriate flexibility to industry in how it implements mitigations.

We intend to keep options open in regard to a statutory vehicle to deliver these proposals, where legislation is required.

We welcome views on these proposals and look forward to continuing to work with relevant industry actors, experts and others to ensure design and implementation serves both commercial realities and the national interest.

Voluntary measures and industry support structures

Critical National Infrastructure status

Advances in technology are changing the way essential services are supported and delivered across the UK. The increasing use of digital systems will, over time, increase the criticality of third-party data centres. Some data infrastructure is already considered by the UK government to be critical, due to the way the systems support Critical National Infrastructure assets (CNI).

The UK currently has 13[4] critical national infrastructure sectors, of which some sectors can be further broken down into subsectors. For instance, Communications is split into Broadcast, Internet and Telecommunications, and Postal services.

Within these sectors, CNI is determined as "the critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

- major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
- significant impact on national security, national defence, or the functioning of the state."

Working closely with industry, the UK government uses the CNI framework to identify the most critical systems which need enhanced security protection and resilience measures.

Each CNI sector has a Lead Government Department responsible for working with industry to identify CNI assets, understand risk within the sector and ensure appropriate assurance and mitigations are in place to reduce the vulnerability – either through policy, guidance, or sectoral legislation.

The UK government is considering how the data infrastructure sector fits into the CNI framework and whether third-party data centre infrastructure should be determined as a subsector of CNI in its own right due to the increasing reliance on these services by the UK.

We expect that some parts of the data centre sector will meet the definition of CNI.

[4] Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water

Implications of CNI Sector Designation

By definition, Critical National Infrastructure and systems are fundamental to UK society, and it is imperative that the government works in partnership with industry to ensure CNI assets and supporting systems are appropriately identified and protected. As part of this:

- Owners and Operators of CNI systems will receive enhanced levels of support and scrutiny from their designated CNI Lead Government Department, NCSC, NPSA and UKNACE where applicable, in order to ensure risks and threats to these critical systems are mitigated.
- CNI assets are being mapped onto a secure tool[5] which is used by appropriately cleared government officials to identify interdependencies and potential areas of cascading risk.
- Sector-specific security and resilience frameworks may be introduced, where adequate provisions are not already in place.

This section is not a confirmation of an intention to designate the third-party data centre sector as CNI. Instead, following on from last year's call for views, we are collecting comments to inform a future decision.

Government is currently undertaking research into the third-party data centre and digital service sectors to determine if they contain critical systems which meet the CNI thresholds for inclusion in the CNI framework, either as supporting systems to existing CNI assets, or as part of expanding the CNI sector framework to include data infrastructure more generally.

We have a number of questions for stakeholders that can inform any future decision on whether and how we might implement CNI designation:

Questions

1. What forms of digital or data-related infrastructure should the government the government consider for potential CNI designation?
2. How would you compare the expertise required to appropriately risk manage the colocation data centre sector to other critical sectors, such as Communications?
3. Are there particular benefits, opportunities, or risks to CNI designation for the colocation data centre sector that you would wish to draw our attention to?

[5] https://www.ncsc.gov.uk/files/Criticalities-and-CNI-Knowledge-Base-Industry-Flyer.pdf

Other voluntary measures and support structures

As described above, the government is aware of the wider challenges the data infrastructure sector is facing, and that, to some extent, underpin the security and resilience risks we have identified in this consultation.

In the UK, industry has organised itself into productive policy fora, including the techUK Data Centre Council. The government recognises that there is more work to do to reach the full breadth of data centre operators, and to ensure the government has appropriate oversight in anticipation of any legislative measures being introduced. The government is considering mechanisms to improve government-industry information-sharing and dialogue on security and resilience risk management, as well as further measures to benchmark risk management in the interim.

The telecommunications sector offers useful precedents in this respect. For example, the Electronic Communications Resilience & Response Group (EC-RRG). This is a government-industry telecoms industry forum to ensure the telecoms sector remains resilient to threats and risks to services. As another example, Ofcom's TBEST[6] offers a threat intelligence-led penetration testing scheme which simulates a well-resourced cyberattack from a nation state or large organised crime groups. Finally, the Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible, and has been largely successful as a mechanism to drive up the standard, where it is used.

The government recognises that some risks can be mitigated sufficiently by improved government-to-industry information sharing, or other voluntary means of benchmarking risk for the sector. Pursuing the right initiatives will equip industry stakeholders to prepare well for any statutory intervention, in those areas where legal requirements may be deemed necessary.

The government invites views on which industry-to-industry and industry-to-government forms of cooperation would be most valuable to the sector, as well as any other security and resilience measures the government should consider to support the sector.

Questions

4. What forms of intra-sector and sector-to-government voluntary cooperation would be most useful for the sector?

5. What voluntary cooperation mechanisms, if any, have you experienced in this or other sectors that demonstrate improvement to risk management?

[6] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work

6. Which issues lend themselves to intra-sector cooperation, and on which issues would industry welcome further government involvement?

Statutory Framework

Framework overview

The government proposes a statutory framework to protect and enhance the security and resilience of the infrastructure on which the UK's data use relies.

As set out in the Introduction section, there are a range of risks that can lead to disruption of continuity of service or unwanted access or compromise of data; this proposed framework would seek to ensure relevant providers and supervisory authorities are empowered – and where necessary obliged – to mitigate these.

The desired outcomes of these proposals, which would be applied UK-wide, are to:

- establish appropriate regulatory supervision of data centres and data centre services within scope;
- ensure that there is a baseline of security and resilience risk mitigations in place;
- ensure that incidents are detected, managed and, where significant, reported;
- ensure that the government and regulators have the information, capability and levers to address local and systemic risks to current and emergent data infrastructure, and that customers have sufficient visibility of risks and mitigations where appropriate.

We have set principles for the design and implementation of this framework:

- **Appropriate precaution:** putting in place the levers necessary to manage and mitigate risks before they become serious incidents.
- **Effective and proportionate:** meeting our objectives while minimising unnecessary costs or restrictions.
- **Flexible and futureproof:** utilising mechanisms and setting outcomes that allow for the policy to keep pace with emergent technologies and risks.
- **Targeted but interoperable:** centred on the needs of the sector but with an awareness of wider stakeholders and policies it may interact with.
- **Evidence-based and testable:** using rigorous analysis and clear argument where empirical evidence is limited, and ensuring interventions can be effectively measured and evaluated for impact.
- **Collaborative and transparent:** engaging honestly and working with the sector and associated experts to understand the most suitable path forward that meets societal objectives while considering commercial interests.
- **Pro-innovation and growth:** creating the right environment for disruption and market entry, while promoting the UK as a trusted jurisdiction for investment and trade.

- **Internationally-minded:** considering our positioning alongside peer countries and minimising cross-border operating costs and, where necessary and effective, promoting a fresh approach in response to our new realities.

The proposals have been designed in line with developing good practice, including innovation-friendly regulation, as set out by the Regulatory Horizons Council, and the Better Regulation Framework.[7]

Whilst this framework would focus on security and resilience challenges faced by third-party data centres, we would also ensure that any intervention is coherent and consistent with the existing regulation of other relevant infrastructure and services, in pursuit of closing gaps, rather than layering legal requirements. This is explored in further detail in later sections.

We have sought to apply the most relevant and effective elements of existing regulations for adjacent or connected sectors and infrastructure – and in particular the Network Information Systems Regulations and Telecommunications (Security) Act – with a view to ensuring interoperability (especially where operators might be in scope of more than one regulation). International comparators and cross-border standards have also been carefully considered through the design process, and we will continue to engage with our partners.

Detail on the proposed framework is provided through the following sections:

- Scope
- Organisations within the scope
- Registration
- Security and resilience measures
- Standards, assurance and testing
- Personnel
- Incident reporting
- Regulatory model and function
- Monitoring and evaluation
- Statutory vehicle

DSIT has taken an open and collaborative approach to the development of this proposed framework through its 2022 call for views and subsequent engagement with industry, experts and academics. We have also engaged closely with relevant UK government agencies, authorities and existing regulators. To help shape these proposals further, we would welcome feedback and evidence on individual elements, and the framework as a whole.

For the benefit of stakeholders who have already engaged with these proposals, and for those interested in contextual information and technical detail of how the proposals could be implemented, supplementary details are included throughout this document. This can include

[7] Innovation friendly regulation; Better Regulation Framework

suggested technical wording, potential material for supplementary guidance and possible measures. These are separated from the main body of the text in boxes or tables, such as the below:

Box X – example information box

Please note that the following details are indicative, that this is an example of a possible approach and has not been finalised. The final legal implementation of the proposed framework would be determined as part of the legal drafting process and influenced by the shape of any introduced or adopted statutory vehicle.

Scope

Rationale

The unrestricted access to internet-based information demanded by the information economy has led to extremely rapid growth in the volume of data and the need to process, store and transport it. Demand is also accelerating from businesses and organisations innovating with data within closed systems and networks. Data centres house, support and rely upon the information technology, operational technology and network telecommunications that meet these demands. The ecosystem is complex and interconnected, and interdependencies are only increasing as technologies and services develop.

The attack surface scales with these developments and the system is only as secure as its weakest link. Points of failure may exist and widespread outage is possible if the system is compromised. The complexity of the system and the presence of information silos compound this risk as there are few people or organisations who deeply understand the networks and systems.

Data centres are a valuable target for threat actors, who continue to innovate and use new or adapted tools and techniques. They are also exposed to non-malign risks to resilience and continuity of service, particularly supply chain risks and natural hazards. Taken together, this risk landscape presents a significant cumulative risk to a crucial sector that underlies much of the UK's economy, and to datasets that have significance for the UK's national security. These proposals seek to play a part in ensuring that risks are minimised and mitigated as far as is possible and proportionate, through transparency of information and adherence to best security and resilience practices.

Data centres often serve multiple customers and represent a concentration of dependencies, and consequently additional or heightened security and resilience risks. Compromise or disruption to continuity of service could have cascading impacts on other interdependent infrastructure (some of which is CNI), business customers and, ultimately, the public. Valuable, sensitive and sometimes critical data is also highly concentrated in these facilities, some of which also house equipment or network interconnections which are targets for interception and exfiltration, or could be exposed to non-malign incidents. Illegitimate access to such data by hostile actors at these facilities constitutes a risk to the UK's national security, and interruption to operations could have knock-on effects for thousands of UK businesses and millions of citizens.

Data centres provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. The growth in demand for artificial intelligence and Large Language Models are just one recent example of this; providers are evolving their services to offer higher rack densities to meet compute needs. Environmental management and energy consumption of data centres also continues to be

critical in order to provide reliable operations while also balancing efficiency to minimise environmental impact and costs.

There are commercial pressures for data centre providers to maintain physical and cyber security and resilience. Incidents and attacks nonetheless regularly occur that challenge this, potentially highlighting a dynamic and evolving threat landscape.[8] Third-party data centre services are currently not directly regulated for security and resilience in the UK, unlike other similar sectors, and unlike the approach taken in other major economies.

Data centres and data centre services

The design and management of a data centre varies in relation to: a) purpose; b) security level; c) physical size; and d) accommodation (permanent, temporary and mobile constructions).

Delineated by purpose or function, there are a number of common “types” of data centre:

- **Colocation data centre**
    - Data centre in which one or more users rent space in the same site from a third-party provider.
- **Cloud or hyperscale data centre**
    - Data centre operated (and sometimes owned) by a Cloud Service Provider (CSP) in order to provide a cloud service.
- **Managed services data centre**
    - Data centre operated (and sometimes owned) by an MSP in order to provide managed services through the network(s), servers and storage equipment. Not all managed services involve the operation of a data centre, but some do.
- **Enterprise and on-premise data centre**
    - Data centre that is owned and operated by a company with the sole purpose of the delivery and management of services for that company.
- **Network operator data centre**
    - Data centre that has the primary purpose of the delivery and management of telecommunications or internet services to the operator's customers.

Data centres can also be delineated by their size and accommodation (which can be linked to their intended use-case):

- **Regional data centre**

[8] Evidence related to the prevalence of incidents/attacks includes the Uptime Institute Data Report 113, Oct 2023, and the Uptime Annual Outage Analysis 2023.Due to methodological and data challenges, data relating to attacks and outages should be treated with caution and are subject to uncertainty.

    - These data centres are often large and serve entire regions, they are usually situated in or near a major metropolitan area.

- **Edge data centre**
    - Smaller and sometimes ‘micro’ data centres geographically closer to the “edge” of a network where data is generated, processed, or consumed. Their main purpose is to reduce latency for applications and services that require real-time processing.
- **Modular data centre**
    - This refers to a portable collection of all the components needed to supply data centre capacity (servers, storage, networking equipment, etc). The most common type is known as a containerised data centre or portable modular data centre. Other examples of modular data centres can include prefabricated data halls and prefabricated power and cooling modules.

Understanding the data centre landscape is complicated by the interconnected and interdependent nature of the physical, logical and virtual layers of data infrastructure, and the fact that the reality of organisations’ data centre service provision does not always neatly fall within discrete definitions of types of data centre. This is exacerbated by varied use of terminology and innovations in data centre services, that sometimes leave categorisation open to debate even where there is expert understanding of the technical reality.

Multiple services can be offered through a single data centre, meaning they may not have one “purpose”. The organisations that operate data centres and offer these services often offer multiple services through their, or others’, data centres, from colocation, to hosting, to managed services, to various forms of cloud (private, public, hybrid), with certain data centre services potentially sitting between or across these categories.

Cloud services can be provided through dedicated cloud or hyperscale data centres but can also be provided through and housed in any of the data centre types listed above. Managed services are much the same in this respect. Public electronic communications networks or services (telecommunications) can have their own data centres, but parts of telecommunications infrastructure also connect to and sit inside other types of data centres, such as colocation data centres.

To accurately capture the organisations in scope – data centre providers – the government aims to take account of the reality of service provision by focusing on the provision of certain data centre services.

By taking a service-orientated definitional approach, rather than attempting to refer to “types” of data centres, the boundaries of responsibility can be identified appropriately. Importantly, responsibilities can then be set in line with the boundaries of services offered by data centre providers, responsibility which may stop at the room, the rack, through to the servers and virtualisation, or beyond. While the security and resilience of third-party data centre infrastructure remains the core focus here, the scope of security and resilience risk

management responsibility extends in line with the service provision, and this is important clarity for those in scope of the framework and any designated regulator.

Data centre services within the scope

The proposed framework is intended to initially capture organisations that operate data centres, in particular, those that provide colocation and co-hosting data centre services as a third-party provider.

Box 1 – data centre services within scope

Colocation. Providers typically rent out space within a physical facility in which a customer, or multiple customers, can locate their own network(s), servers and storage equipment.

The support infrastructure of the building (such as power distribution, environmental control, network connectivity and security) is provided as a service by the operator. These third-party data centres may also provide services that connect telecommunications and network service providers to other telecommunication and network service providers. This is commonly known as interconnection/peering.

Co-hosting. Providers typically rent out space to customers within a physical facility, but unlike colocation, both the network(s), servers and storage equipment and the support infrastructure of the building are provided as a service.

Co-hosting is intended to cover services such as bare metal hosting, hardware-as-a-service and dedicated servers/hosting, where these are not cloud services. Co-hosting providers can sometimes also provide virtualisation or containerisation environments for their customers.

These services can be provided through dedicated data centres. However, it is also possible for colocation services to be provided through data centres that have other purposes and provide other functions or services. Likewise, co-hosting services can also be provided through data centres that have other purposes, including colocation data centres. The proportion of such services provided through data centres and by organisations with multiple-service provision models is likely to vary and evolve over time and with market demand. If a colocation or co-hosting provider were also to provide other services through a data centre they operated, this would not preclude their being in scope.

Definitional approach

The government intends to adopt or align with existing definitions where they exist and are fit for purpose. This includes definitions of a data centre and its various types, which have been

established through globally recognised standards like ISO/IEC 22237 and BS EN 50600. Substantive elements of these definitions have also been adopted and adapted in some other jurisdictions.

The government intends to define a data centre and relevant data centre services. Organisations will be in scope of legal duties as a relevant data centre provider where they provide a relevant data centre service. This would ensure that organisations responsible for the management and operation of specific data centre implementations are in scope, even when it may only form part of a wider data centre facility.

Any formal definitions would be determined through a legal drafting process, to help to inform this, the government would welcome feedback on the structure of the scope approach, and whether the following could work to adequately define a data centre and relevant data centre services.

Box 2 – definition of a data centre

A structure, or group of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructure for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability.

Note 1: *A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function.*

Note 2: *The boundaries of the structure or space considered the data centre, which includes the information, operational and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building.*

Box 3 – definition of relevant data centre services

colocation

A service that provides a data centre or space within a data centre in which a customer or multiple customers can locate their own network(s), servers and storage equipment.

co-hosting

A service that provides a data centre or space within a data centre in which a customer or multiple customers are provided with access to network(s), servers and storage equipment on which they operate their own services/applications.

Note 1: *These definitions are intended to capture retail and wholesale applications of these services.*

Note 2: *Data centres of any size, including edge data centres that are operated by the above service providers to provide these services, are seen to be in scope of this definition.*

Note 3: *Where necessary, and pending the response to this consultation, amendments and explicit exemptions could be made to these proposed definitions to minimise regulatory overlap or any unintended over or under reach.*

Services and infrastructure outside the scope

The following services or infrastructure, and so any data centre services or parts of data centres that solely fall under these categories, are proposed as outside the scope of these proposals, as outlined and explained in box 4.

Box 4 – services and infrastructure proposed as outside the scope

Public electronic communications services and networks (telecommunications) are regulated under the Communications Act 2003 (as amended by the Telecommunications [Security] Act [TSA]) and its accompanying secondary legislation. Network operator data centres and any infrastructure provided by public electronic communications providers connecting to or inside data centres are therefore regulated.

Digital infrastructure, including key elements of internet infrastructure, are regulated under the UK's Network and Information System (NIS) Regulations 2018, including internet exchange points (IXP), top-level domain name registry (TLD name registry) and Domain Name Systems (DNS) service provider.

Submarine or subsea fibre optic cables (SFOC), which, like some digital infrastructure, can interconnect with data centres. SFOC are part of longstanding government policy work focusing on improving the security, resilience and regulatory coverage of internet infrastructure, including cable landing sites, to minimise disruption and compromise. This area is under continual monitoring and review.

Enterprise data storage and processing and storage operated by a company with the sole purpose of the delivery and management of services for that company. These data centres are out of scope as they are subject to regulation through their use by a respective business or sector. For one example, through the NIS Regulations as Operators of Essential services (OES) subsectors. Additionally, they do not provide services directly to third-parties, even if the enterprise may ultimately provide one, meaning risks associated with a concentration of dependents are reduced.

While the government proposes the above are outside the scope of this proposed framework, proposed mechanisms to adjust the scope could allow for services or infrastructure to be brought into scope in the future (for example, enterprise data storage and processing).

Box 5 sets out services that are proposed as outside the scope but where the feedback to this consultation will particularly help to inform the government's approach.

Box 5 – services proposed as outside the scope, pending feedback to this consultation

Cloud services from providers above a certain threshold are regulated through the NIS Regulations. CSPs are considered a Relevant Digital Service Provider (RDSP).

Managed services that meet a defined set of characteristics are proposed to be regulated through the NIS Regulations. MSPs are proposed to be added as an RDSP.

Given the close relationship between cloud and data centres, and some managed services and data centres, the section (Data centres and Cloud and Managed Service Providers) covers this interaction in more detail and requests views on their regulatory treatment.

Questions

7. Please share any views you may have on the definitional approach, and on the proposed indicative definitions for:

    a. data centre

    b. relevant data centre services

        i) colocation

        ii) co-hosting

8. Please share, and explain, any views you may have on the proposed scope of third-party data centres, the operation of which are part of colocation and co-hosting services.

9. Of the services and infrastructure that are indicated as outside the scope of the proposed framework, are there any that you feel should be included, or that you feel require a different treatment? Please explain the reasons for your answer.

10. Please share any information that you consider might help to inform the government's scope approach. This might include, for example, information on the taxonomy of and terminology used to describe the data centre and data centre services landscape and market.

Data centres and Cloud and Managed Service Providers

In the UK, many CSPs currently provide their services through data centres they do not own, which they either lease wholesale, or occupy as tenants in a multi-tenant retail facility. MSPs also offer their services in these ways and can own their own data centres.

As stated, the government proposes that cloud services would be out of scope of these proposals. All managed services would also be out of scope of these proposals, should they become regulated under the NIS Regulations. This is due to their existing or forthcoming coverage under the NIS regulations[9] and a desire to ensure that regulatory regimes are complementary rather than duplicative, and have minimal overlap.

Importantly, this would not mean that all data centres would be out of scope where cloud or managed services are provided through them; only data centres that are solely owned and operated by a cloud or managed service provider to provide a cloud or managed service (and are therefore already required, or are expected to need, to meet security and resilience requirements under existing or forthcoming regulation).

However, the government would like to receive views to inform its approach to data centres that are owned and operated by CSPs and MSPs (with a view to ensuring they receive appropriate protections). This will help to inform future decisions around how to best treat dedicated cloud and managed services data centres from a regulatory perspective.

The risks posed to the security of network and information systems of cloud services (and, in the future, managed services) are within the scope of the NIS regulations. Where they form part of the network and information systems relied upon to provide a service that is within the scope of the NIS regulations, this would include:

- risks posed to data centres that are owned by CSPs and MSPs;
- risks posed to data centres that are leased and operated by CSPs and MSPs (to the extent it is appropriate and proportionate for the CSP/MSP to manage these risks);
- risks posed to spaces within data centre facilities that CSP and MSPs lease or occupy as tenants (to the extent it is appropriate and proportionate for the CSP/MSP to manage these risks).

In the last two scenarios the organisation who leased the data centre, or space within a data centre, to a CSP or MSP, would be in scope of this proposed framework as a data centre provider, and would be responsible for the security and resilience of the data centre to the extent it is appropriate and proportionate. The boundary of responsibility may be appropriately drawn up to the point of a CSP or MSP's contractual responsibility as customers, or tenants.

[9] CSPs (and in the future, MSPs) will be subject to the NIS Regulations where the organisations are above the regulation's small and micro exemption –more than 50 staff and an annual turnover or balance sheet above €10 million.

The government would welcome views on whether data centres that are owned and operated by cloud or managed service providers, should be:

- **A:** Kept as they are (or are set to be). That is, excluded from this framework and covered under the RDSP category in the NIS Regulations as part of the relevant managed service or cloud services network and information systems.
- **B:** Bought within the scope of this proposed framework. To implement this, there would be two main options:
    - **B(1):** Cloud and/or managed service data centres could be included within the scope of this framework, with relevant CSPs and MSPs being made relevant data centre providers on the one hand, while remaining a RDSP within the UK NIS Regulations, on the other. This framework would cover data centre infrastructure security and resilience, and the RDSP provisions in the NIS Regulations would retain coverage of these organisations as digital service providers, including the services they offer, the platforms and the virtual and logical layer.

      In other words, this would mean a separation between the data centre facility and operations, and everything beyond the rack, the storage and processing equipment, software and service layer.

      This is similar to the split in responsibility that occurs between a typical colocation data centre provider and a customer.
    - **B(2):** Cloud services and/or managed services (that own and operate a data centre) could be brought entirely within the scope of this framework as data centre providers, and those that met these criteria could be removed from the RDSP category in the NIS regulations.

      This would ensure that third-party data centres, relevant CSP and MSP data centres and their services that rely on these data centres would be regulated together.

      The measures within this framework would then cover the security and resilience of a CSP or MSP data centre, and the rest of their digital service. Any adaptations or tailoring to ensure appropriate regulation of these digital services would be made to this framework, or the measures set through this framework, as necessary.

Questions

11. Please express your preference on the options set out for the treatment of data centres that are owned and operated by cloud service providers:

    a. Option A

    b. Option B(1)

c. Option B(2)

Please explain the reasons for your answer.

12. Please express your preference on the options set out for the treatment of data centres that are owned and operated by managed service providers:

    a. Option A

    b. Option B(1)

    c. Option B(2)

Please explain the reasons for your answer.

Mechanisms to adjust the scope

The government intends to introduce or adopt delegated powers to adjust the scope of the framework to enable the government to act in the face of the rapidly evolving technological, commercial, threat and regulatory landscape.

These mechanisms would be accompanied by appropriate constraints and safeguards:

- Where held by the government, the government would have a duty to consult prior to the exercise of these powers.
- Any statutory instrument introduced through the exercise of this power would be accompanied by an impact assessment (IA) in accordance with Better Regulation guidance.

Where held by the government, the use of these powers would be subject to appropriate parliamentary scrutiny, the affirmative procedure, where it materially changed the scope of organisations who are subject to the duties in the framework. This is because the use of these powers could mean placing new legal duties on organisations, or exempting organisations from duties (potentially reducing security and resilience protections). This would mean that any statutory instrument must be actively approved by both Houses of Parliament.

Power to expand the scope

This may include expanding the scope to other relevant data infrastructure, data centre services, or interdependent organisations where under- or unmanaged risks are identified and evidenced.

The scope of the mechanism would be constrained to a definition of data storage and processing infrastructure. Subject to the safeguards above, it could be used to bring other infrastructure into scope. This might include:

- Other data centres and data centre services, including enterprise implementations.

- Emerging data storage and processing technologies and infrastructure, such as data transmission technologies and DNA storage.
- Elements of the data centre supply chain.

Power for a regulator to designate

We also intend to introduce a power for a regulator to designate an organisation or service as a data centre provider or relevant data centre service. This would ensure that the regulator has the power to designate an organisation or service as within scope. The intention is to account for circumstances where organisations or services may be in grey areas of any eventual definitions. Prior to use of this power, the regulator would engage with the relevant organisation. There would also be mechanisms in place to allow decisions made by the regulator to be challenged (see Enforcement).

Power to exempt from scope and set exemption thresholds

This proposed power could be used to exempt organisations, services, or data centres/sites from scope, and set thresholds to do so. This would allow for the government to ensure that only the appropriate organisations are within the scope. It would also allow for the government to refine or reduce the scope following monitoring and evaluation of the impact of the framework or significant reduction in risk profile for relevant data centre providers or services.

The government has built in proportionality at the design stage of these proposals. Security and resilience measures would be applied uniformly to anyone in scope and designed to be appropriate, proportionate and, wherever possible, outcome-based. We intend to empower a regulator to undertake risk-based supervision of the sector, which would mean that the level of supervision could be tailored to the level of risk, potentially leading to lighter touch supervision of smaller and lower-risk providers. This would allow a regulator to tailor the level of assurance it requires from organisations.

The government considers that this approach will lead to proportionate burdens across the sector, as organisational size (and other factors) would play a role in any risk assessment. However, we would welcome views on whether there may be small or micro businesses for whom it is disproportionate to place duties on because they do not present a significant security and resilience risk due to the scale of their operations and service(s).

It is challenging to determine where this might be the case and therefore what criteria (for example, size of provider or energy consumption of an individual data centre) could be used to set an exemption or threshold that would not have unintended consequences, such as missed security and resilience risks or dependencies. The following are some considerations that complicate such a determination:

- Our current market analysis indicates that the industry comprises a relatively small number of businesses and that many of these businesses operate a small number (in many cases a single) site (170 providers to 250 sites). A large proportion of data centre capacity is concentrated into a relatively small number of large sites, operated by a small number of operators. However, anecdotally, there are indications that this could

change as edge becomes a more important part of the infrastructure, with both an increase in the number of smaller businesses operating individual sites, and an increase in the number of businesses operating many small edge data centres.

- The government is concerned not just with local, but with systemic security and resilience risks that may be manifest only in the aggregate. Where data centres are part of a wider network, baseline protections should be in place across that network.
- The potential for data centres to provide redundancy and contain backups for one another could mean that if one data centre was outside the scope it could have resilience implications for another that was within the scope. Similarly, edge deployments and trends towards decentralised data storage and processing may also run the risk of being excluded if care was not taken with any threshold. A small edge data centre may not present a significant risk when seen in isolation but seen as part of a wider service and network, that picture could be quite different.
- The government is also mindful not just of the risks of a national scale, but of risks to small, micro and medium enterprises, who may depend upon smaller data centre providers for their data storage and processing needs. We do not have evidence to suggest that an appropriate baseline of security and resilience measures is in place in smaller sites. An exemption for small data centre providers may reduce protections (registration, security and resilience requirements, incident reporting, assurance), and the ability for the government to set measures around information asymmetry to improve transparency for customers on what data centre security and resilience mitigations mean.

The government currently considers that a blanket exemption based on the scale of an individual site, which would likely be achieved through setting a threshold based on energy consumption, (for example, 1MW), may not adequately navigate the challenges above, although we welcome views on this. Instead, if an exemption was to be made (on top of the proposed risk-based supervisory approach) we consider that an exemption for micro entities based on the size of an organisation is more likely to achieve the desired effect (without compromising systemic protections and other policy outcomes). An example of such a definition of a micro entity can be found in section 384A of the Companies Act 2006.[10]

The government welcomes views on this topic. If it has the evidence to do so, the government could consider introducing a scope threshold from the outset, exercise a power to exempt from scope prior to commencement or any active supervision, or introduce one following advice from a regulator once supervision had commenced.

13. Please share any views you may have on the proposed power to expand the scope.

[10] Micro-entity qualifying conditions (in a year): Turnover, not more than £632,000; Balance sheet total, not more than £316,000; Number of employees, not more than 10.

We are particularly interested in information on existing or emergent forms of data storage and processing infrastructure, data centre services and connected infrastructure which may warrant future attention from the perspective of security and resilience.

14. Please share any views you may have on the proposed power to exempt from scope and set exemption thresholds. We would welcome any information or evidence that could be helpful for the government to decide on any approaches to small and micro-businesses, and to small data centres, whether initially, or using the proposed power.

Organisations within scope

Relevant data centre providers

Some of the proposed legal duties are intended to be applied directly to operators of data centres within the scope. Organisations would be considered to be within scope as a relevant data centre provider, when they provide a relevant data centre service.

The data centre providers in scope have direct responsibility over the day-to-day operations of data centres or the parts of data centres they are responsible for to deliver their service. Appropriate levels of security and resilience are considered part of the service they provide and so are appropriate to hold responsibility for the measures in the proposed framework, within the boundaries of the service they provide.

In instances where organisations provide multiple relevant data centre services, for example, if an organisation offers colocation and co-hosting, perhaps within one facility, then they are still regarded as a data centre service provider. If a relevant data centre service provider was to provide other services as well as colocation or co-hosting, through a data centre they operated, this would not preclude their being within the scope.

The obligations placed on data centre service providers are initially intended to be uniform regardless of the route to scope, although having the flexibility to differentiate data centre services provided by organisations would allow for individual treatment of risks through mechanisms in the framework, should differences be identified and evidenced.

Data centre owners

Data centre providers may operate a data centre, or parts of a data centre, or they may own and operate a data centre. Given an owner may not always provide a relevant data centre service, and instead lease a data centre to another organisation wholesale, the government is considering whether owners of data centres that provide, or are intended to provide (if not yet leased and in operation), a relevant data centre service should be considered an organisation within scope of the framework.

The government is considering whether in instances where the owner of a data centre is different to the operator of a data centre, that the owners should be subject to a duty to meet

the same security and resilience measures as data centre providers, in respect of the elements of a data centre that they retain responsibility for.

The intention behind this would be to ensure that there are no security and resilience gaps where owner-operator responsibilities are split, and to establish a stable backstop for data centre provider legal duties. A duty on owners to ensure that service providers they own or contract meet their duties provides an additional layer of accountability for strategic or financial decisions affecting security and resilience. The government views this approach as compatible with instances where an owner is also the relevant data centre provider, as the effect would be voided.

Additionally, responsibilities for data centre sites and the infrastructure itself may shift throughout its life cycle from design, planning, procurement, construction, integration, installation, to operation and maintenance. If the government or a regulator were to set measures relating to different aspects of the life cycle, for example the site selection, design and construction phases, then the ability to place obligations on an ownership organisation may be necessary.

Certain service models may also lead to shifts in operators, for example, wholesale arrangements may have different customer-operators over time, depending on who the facility was leased to. In these cases, having a static organisation to be a responsible party may be necessary.

Respondents to this consultation have the first-hand, in-depth knowledge of owner-operator responsibilities, structures and contracts. The government welcomes any information that may inform a firm approach to this topic.

Questions

14. How much do you agree or disagree that owners of third-party data centres should be included within the scope of the proposed framework? [scale from strongly disagree to strongly agree]

    Please explain the reasons for your answers to the previous question.

15. Please provide any information that you consider would be helpful to inform the government approach. For example, information on ownership and market structures, owner and wholesale leaseholder contractual arrangements and divisions of responsibility.

Registration

Relevant data centre providers would be required to register with the designated regulator once this framework comes into force. This would provide the regulator clarity in regard to who considers themselves to be in scope, as well as up-to-date contact information to enable effective communication and collaboration.

The registration process would consist of relevant data centre providers notifying a regulator and providing certain details. We would welcome views on the information that could be required at the point of registration.

Box 6 – possible registration information

- the name of the organisation and/or service;
- address of the UK-based head office (or a foreign head office address along with a UK correspondence address) and name of a nominated representative, along with contact details;
- information on the number of sites/facilities provided within the scope of the framework, their geographical location, energy consumption and availability level/rating/tier;
- information on current customer types, e.g. financial organisations, healthcare;
- information on risks, impacts and existing mitigations or controls, e.g. a risk register, a business impact analysis;
- information on ownership (including ultimate beneficial ownership).

Note: *DSIT is also considering requiring that updates are provided on any changes in ownership that meet the criteria of a trigger event, as set out in the National Security and Investment Act. The government is currently reviewing its position on this point and will confirm through a published response to this consultation.*

Relevant data centre providers would be encouraged to notify the regulator of any changes to their details as soon as possible, within a specified timeframe. Failure to register or update details would be backed by enforcement action, such as penalties.

Within certain constraints, the regulator would be able to provide this information to DSIT and other relevant government functions and agencies. We cover this and related topics in Information gateways and safeguards.

Question

16. Please share your views on the information that could be required at the point of registration. Do you have any recommendations for other information or data that you feel should be required?

Security and resilience measures

Relevant data centre providers would have a duty to take appropriate and proportionate technical and organisational measures to protect and enhance the security and resilience of their services.

The intention is to provide for a baseline of security and resilience risk mitigation for relevant data centre providers. Supervision by a regulator would be guided by a risk-based approach (see section on Risk-based supervision).

Requirements would be designed to be effective, proportionate and, wherever appropriate, outcome-based and standards-aligned. They would be designed to support the protection of:

- the performance, reliability and availability of operations;
- the confidentiality, integrity and availability of data;
- the reputation and revenue of relevant data centre providers and their customers.

Any power to specify security and resilience requirements would be designed to enable the measures to cover the following areas (whether initially or in the future):

- organisational processes;
- the physical infrastructure / facilities / equipment, for example:
    - IT
    - network telecommunications and cabling
    - Operational technology (OT) / Industrial Internet of Things (IIoT)
    - Power Distribution Unit (PDU), Uninterruptable Power Supply (UPS), generators
- virtual and logical infrastructure, for example:
    - industrial control systems (ICS), such as SCADA
    - environmental control and monitoring systems, BMS (Building Management Software), DCIM (Data Centre Infrastructure Management software)
    - security systems and software
    - virtualisation and containerisation software and control planes
    - timestamping systems
    - remote monitoring and control platforms
    - any other software used to facilitate or control operations or networks

Requirements would be able to relate to the above and may cover:

- risk management

- the physical and cyber security of facilities, networks and systems, including measures targeted at specific areas or functions (for example, meet-me rooms)
- incident management
- resilience and service continuity
- monitoring, detection, auditing and testing
- governance and personnel
- supply chain management
- site and facility design and construction

These areas are non-exhaustive but have been identified as areas and aspects of data centres and data centre operation that are key to security and resilience, and where vulnerabilities and risks have existed and can exist. We would welcome further input; the design and introduction of security and resilience measures would follow a process of engagement with relevant stakeholders.

Indicatively, the government is considering introducing baseline measures similar to those outlined in Table 6. This baseline is similar to the measures Relevant Digital Service Providers (including CSPs) are subject to under the NIS Regulations, and are compatible with the existing standards and frameworks, which may be used to assure, and also provide assurance beyond, baseline measures.

Table 1 – indicative baseline security and resilience measures	
The security of facilities and systems	
Systematic management of facilities and systems: - Risk analysis - Human resources - Security of operations - Security architecture - Secure data - System lifecycle management - Encryption, where applicable	**Supply chain:** establish and maintain appropriate policies to maintain knowledge of the accessibility and traceability of critical supplies. - Accessibility of critical supplies - Traceability of critical supplies
Physical and environmental security measures: establish and maintain a set of measures that protect facilities and systems from impacts. - Encryption (where applicable/appropriate) - System failure	**Access controls to systems:** establish and maintain measures that ensure both physical and logical access is authorised and restricted based on business and security requirements. - Implementing the principle of least privilege and zero trust

- Human error - Malicious action - Natural hazards	- Implementing multi-factor authentication (MFA), wherever it would protect and enhance security and mitigate vulnerabilities such as with RFID technology - Where appropriate, establishing secure areas
Resilience and service continuity	
The capability to **maintain or restore the delivery of services to acceptable predefined levels** following a disruptive incident or to facilitate maintenance. This relates to contingency planning and disaster recovery. - Define and test appropriate availability and redundancy levels - Conduct business impact analyses and use the results to establish and test contingency plans - Establish and test recovery capabilities	
Incident management	
Establish and maintain procedures for supporting the **detection, analysis and containment of any incident, and the follow-up response.** - Timely and adequate awareness of anomalous events - Testing and maintenance - Incident reporting - Identify weaknesses in systems and security measures - Ensure an appropriate incident response - Testing of response and reporting on the results - Incident analysis - Collection of relevant information - Continuous improvement process	
Monitoring, auditing and testing	
Establish and maintain policies concerning **systems assessment, inspection and verification**, including: - Observations to assess whether systems are operating as intended - Penetration testing - Verification that guidelines are being followed - Ensuring records are accurate - Ensuring that efficiency and effectiveness targets are met	

These specific measures are indicative and mark the government's intent. They are deliberately outcome-based, with further driving of behaviours and assurance being sought through other areas of the framework. For some of these topics, more prescriptive approaches may be necessary to effectively introduce specific mitigations. We would welcome views on instances where this could be effective, appropriate and proportionate.

The government intends to introduce mechanisms that allow measures to be adjusted, added to, or strengthened. To do this, the government would strike a balance between legislation, secondary legislation and regulator guidance. If a power to set additional measures required the government to introduce secondary legislation to do this, the use of these powers would be subject to formal consultation, impact assessment and appropriate parliamentary scrutiny.

Throughout and following this consultation, the government would undertake a programme of work with relevant stakeholders, including the NCSC, the NPSA, industry and experts, to finalise its approach and, as needed, alter and develop additional security and resilience measures tailored to the sector. An update would be provided through the government's response to this consultation.

Questions

17. How much do you agree or disagree that the proposed mechanisms to set security and resilience measures will provide the necessary capability to address security and resilience risks, now and in the future? [scale from strongly disagree to strongly agree]

    Please explain the reasons for your answers to the previous question.

18. How much do you agree or disagree that an outcome-based approach to the baseline measures is the most effective approach? [scale from strongly disagree to strongly agree]

    Please explain the reasons for your answers to the previous question.

19. Please share any comments or reflections on the indicative measures, including where there may be gaps.

We would welcome views on whether there are any areas or measures where a more prescriptive approach may be required to effectively protect or enhance security and resilience.

Standards, assurance, and testing

A variety of standards can be, and are already, applicable to data centres. Some standards are sector-agnostic and pertain to information security and business continuity, while others are designed for data centres and data centre providers, covering aspects like physical security, availability, and energy efficiency. Certain standards address the technologies employed in data centres, which have known risks and vulnerabilities, including operational technology and industrial control systems. Data centre providers can also adopt standards driven by the legal frameworks their customers operate within.

The majority of respondents to our 2022 Call for Views highlighted the importance of standards. They emphasised that standards not only influence on-the-ground practices but also provide a consistent and testable means to assess security and resilience risks and mitigation strategies. Respondents advocated for standards to play a central role in any government interventions and that any requirements should be aligned with and where possible adopt recognised and, ideally, international standards. Feedback has also indicated that industry would be receptive to a mechanism to provide evidence of conformity against appropriate standards in order to increase regulator and government assurance.

Several concerns surrounding standards were also raised. These concerns primarily revolved around the inconsistent application and certification of standards rather than the standards themselves. Respondents highlighted potential risks linked to organisations adopting a superficial "tick-box" approach and using a limited scope when applying standards to their facilities, systems, and procedures. There was also apprehension regarding claims of equivalence to certain standards without the backing of certification or assurance.

These market concerns can be addressed and there are clear benefits to leveraging the existing standards used by the industry. A standards-based or standards-aligned approach can be effective in driving comprehensive, considered risk management, ensuring good practice, and enhancing information transparency and assurance, as well as minimising undue burdens and maximising interoperability with other frameworks in the UK and abroad.

This is in line with the 2022 Resilience Framework, which lays out a stronger, standards-based approach to assurance for CNI and essential services. The government proposes to use standards in the following ways:

- **Ensure that security and resilience measures are aligned and compatible with international and recognised standards, wherever appropriate.**
    - The government intends to work with the NCSC, the NPSA, the British Standards Institute (BSI), industry, experts, and regulators, to investigate how standards can inform sector-appropriate security and resilience measures. Through this, standards would be used to both inform the security and resilience measures themselves, and back them up with additional detail.

  - We would work with relevant stakeholders to map the standards landscape in greater detail to further inform our approach, this could include taking the best elements from multiple standards to:
    - inform the development of an enhanced assessment framework, a third-party data centre PAS (publicly available specification), or other tool(s) that could be used for assurance processes;
    - be incorporated into a code of practice, or security and resilience measures compliance guidance.

- **Establish an "earned recognition" mechanism in the framework.**
  - Through this proposed mechanism, relevant data centre providers who demonstrate conformance with relevant standards, assessment frameworks, or undergo testing, would be able to earn recognition from a designated regulator.
  - Earned recognition is an established method of integrating standards in support of good regulation. It is a process of establishing trust that in this case means a regulator can build assurance around the risk assessments and mitigations deployed by relevant data centre providers. Concurrently, relevant data centre providers would have assurance that their security and resilience activities are recognised and taken into account.
  - Indicatively, it could involve a regulator maintaining a categorised map of relevant standards, assessment frameworks, assurance processes, audits and testing frameworks (including penetration tests). These tools could be categorised by the area they cover and ranked the extent of assurance they provide. Consideration could also be given to the credentials of an independent third-party provider who has made any assessment (where applicable). Through this, the extent to which these activities give a regulator assurance that certain risks are being identified, managed, and mitigated by any given provider, for a given site or sites, would be able to form a profile, earning them "recognition".
  - Not all of these tools would have to be adopted to earn recognition and evidence of the use of these tools would be provided on a voluntary basis to a designated regulator.
  - Use of this mechanism may not be tied directly to compliance with the legal obligations in the proposed framework, and instead have a more nuanced effect. This mechanism could form part of the supervisory approach outlined in the section on Risk-based supervision, allowing regulators to allocate their resources based on an assessment of the risks and mitigations for any given provider, site, or sites.
  - We welcome views on possible approaches to the shape and implementation of this mechanism.

- **Establish powers for a regulator to mandate assurance, conformity assessment processes, and testing.**
  - The proposed powers would include:

- the ability to specify standards, standards add-ons, and assessment frameworks as mandatory;
    - This would include the ability to set rules around how standards are used or applied, for example, specifying security controls, or a particular scope of application when using a specified standard.
- the ability to require that conformity assessment, assurance, and testing are performed by an independent and accredited third-party;
- the ability to require that statements of conformity, certifications, or assessment reports are provided to a designated body, and at a set cadence (for example, every x years).

This power would include within scope any third-party audits, assessments, or penetration testing.

Next steps

There are a number of programmes of work we are considering that could play a role in the use of these mechanisms and support the delivery of the outcomes of these proposals. This work may be started by government and then provided to and carried on by a regulator in the event they assume responsibility for the sector:

- working with standards bodies and within committees to monitor, inform, and be influenced by the development of standards;
- working with industry organisations to adopt or develop conformity assessment procedures, auditing, and testing frameworks;
- working with stakeholders to understand how we can improve transparency for customers and the sector around what the use of these tools mean and what level of assurance they provide, especially where outputs are currently limited or vague.

As well as ensuring elements of this framework are aligned or compatible with international and recognised standards the government has an ambition to lead the international market on the standards we require, and for the UK to be the global gold standard for data centre security and resilience. We have already received a range of evidence on these topics and have been reviewing the relevant standards and tools in some detail, but would welcome further detailed evidence on the use of and efficacy of standards, certifications, assurance, and testing in the sector. We have framed questions for this section to reflect the level of detail that will be useful to inform our approach and accompanying analysis.

Questions

20. Please provide information on your use of standards, assessment frameworks, and testing (and any other security and resilience assurance tools) for your UK operations, sites, and services using the table provided in the Catalogue of questions section.

This will be used to inform the design and potential implementations of the proposed standards, assurance, and testing mechanisms, and may inform the design of baseline security and resilience measures.

21. How much do you agree or disagree with the proposed inclusion of an earned recognition mechanism to account for existing tools used in the sector? [scale from strongly disagree to strongly agree]

22. Please share any views on the proposed approach, and any design and implementation recommendations or suggestions you may have.

23. Please share any views you have on this section and these topics. This may include your views on the most effective and appropriate security and resilience-related standards, certifications, assurance assessments and testing for the sector.

Personnel

Personnel with access to data centres and their associated networks and systems may misuse this to cause harm. This misuse of privileged access by employees is known as insider threat. In the case of third-party data centre services, certain personnel have varying degrees of access to services. For example, the access that comes with remote and smart hand offerings - remote hands often offers a lighter touch IT support while smart hands services are more extensive such as performing hardware deployment.

Insider threats can be exacerbated by outsourcing security and maintenance staff which interrupts continuous management and background checks of personnel, but can also result from inadequate management and controls related to direct employees, or corporate or operational processes.

As referenced in the Security and resilience measures section, the government intends for baseline measures for access controls to systems to be set. This includes establishing and maintaining physical security measures and adopting the principles of least privilege and zero trust, to mitigate against insider threats. Conducting background checks on certain data centre providers' personnel can also play a role in minimising the risk of insider threats by providing transparency for employers when making recruitment decisions.

Risks have also been identified in relation to data centre customer access to sites and facilities, and access by contractors or those providing supply chain services or products. These risks may be mitigated by relevant operational security processes and protocols, but may justify the introduction of specific requirements.

The government would welcome further views on the approach taken to these risks in the sector, in order to inform its assessment on how best to support the sector and facilitate appropriate and consistent risk mitigation.

Questions

24. Please indicate whether you conduct any background checks on staff and/or require this of visiting contractors? If so, please share what they entail (i.e. overseas checks, financial checks and/or qualification and employment checks).

25. How confident are you that your current background checks provide sufficient risk mitigation? [scale from very confident to not at all confident]

26. Please share your views on the forms of government support that could help you conduct background checks.

Incident reporting

Incident reporting to a regulator

Incidents are unplanned events that can have serious consequences for relevant data centre providers, customers, and other connected infrastructure and organisations.

The government would introduce mandatory incident reporting to a regulator, calibrated to an appropriate and proportionate level, to mitigate these impacts. With increased transparency of incidents, regulators, agencies, and the UK government would be better equipped to:

- support industry and any affected parties when an incident does occur;
- make informed decisions on interventions, such as measures to address shared risks;
- assess the direct and indirect impacts of incidents (to identify systemic risks)

Data centres experience a wide range of events on a regular basis (see Table 7 for examples). Not every event should constitute a reportable incident. For example, an instance of packet loss, or a minor disruption to energy supply that does not disrupt continuity of service should not be reported.

Table 2 - events that can impact data centres or data centre services

Power	Network	Cyber	Human	Environmental
Surges Spikes Brownouts Blackouts Battery / generator / equipment failure	Congestion Latency Packet loss IT equipment failure	Malware attack Denial of service attack Pre-positioning attack Phishing attack Injection attack Identity-based attack	Errors Negligence Accidents Infiltration Sabotage Vandalism	Flood Fire Heat Cold Earthquake Lightening HVAC failure

The primary risk with the setting of thresholds is the potential for underreporting, or the missing of relevant incidents. However, in order for incident reports to be useful and actionable and to avoid disproportionate burden on the sector and a regulator through overreporting, the government intends to set minimum thresholds describing reportable incidents.

The minimum thresholds are intended to achieve the following effect:

- **Any significant impact on the continuity of service should be reportable.** The inclusion of the word significant is intended to limit the risk of a need to report inconsequential or relatively minor events.
- **Security incidents should be reportable**. A range of unwanted security impacts on facilities, systems, or services are described to provide coverage and for clarity.
- **Any security incidents, irrespective of initial impact, that could lead to actual impact or compromise should be reportable.** Threat actors may gain persistent unauthorised access to a given physical space, network, or service, without causing disruption or outage, with the objective of using this access to cause disruption or harm later. This is known as “pre-positioning”.

Box 8 - duty to report incidents - minimum thresholds

- incidents that significantly impact the continuity of service
- any unwanted access, changes, exploitation, or interference with facilities, systems, or services;
- any impact on security which may allow any person to bring about further security compromises or impact on the continuity of service.

Note: *This approach largely aligns with existing approaches to mandatory incident reporting for similar sectors, with an added emphasis on the facility.*

The government would empower a designated regulator to be able to narrow down the thresholds for reportable incidents in guidance, this guidance may include material thresholds to define what constitutes a significant impact. The designated regulator would also be able to stipulate the form incident reports should take and the information they should contain, if not specified in statute.

The government is keen to foster an environment of transparency and trust between industry and a designated regulator. An incident occurring would not in and of itself mean there had been a breach of duties. However, the act of not reporting an incident when one should have been reported would constitute a breach of duties. If investigation into a particular incident showed that there was a failure to meet other duties, such as adequately following measures or standards, then enforcement action could be considered by a regulator.

Ransomware breaches are captured within the minimum reporting thresholds, and the government also proposes to set out a duty for operators or owners to report any ransomware payments.

Notifying customers and other affected parties of incidents

The government is concerned with risks that relate to potential failures to appropriately prioritise customers and other affected parties (such as data centre providers’ immediate

suppliers) in response to an incident. There is the potential that perverse market incentives, such as fear of financial and reputational loss, could impact otherwise well-intentioned behaviours around the sharing of incident information to relevant parties.

Appropriately managed transparency over security and resilience incidents is seen as best practice. Timely disclosure of incidents to data centre customers and other affected parties can mean that:

- they are better able to plan for and manage incidents, including notifying downstream customers/consumers;
- coordinated incident management becomes possible, which is critical in an industry with many interdependencies;
- there is improved understanding of shared threats and vulnerabilities to inform measures and risk mitigations;
- there is improved accountability and trust within the sector, potentially informing customer (and supply chain) choice in the market.

The government intends to introduce a duty for relevant data centre providers to notify their customers of an incident, under certain conditions. Proposed conditions are set out in Box 9.

Box 9 - conditions under which a data centre provider should notify a customer or another affected party

Relevant data centre providers should report incidents to customers or other affected parties:

- Where a significant risk of security compromise occurs in respect of a relevant data centre service;
- the operator must clearly inform anyone who may be adversely affected;
- they must indicate the existence and nature of the risk, any specific vulnerabilities, and what was impacted;
- communicate any measures that could prevent or mitigate against the risk;
- and offer contact details for a person who can provide further information.

Parties within a supply chain have service level agreements (SLAs), and these can include requirements for each party to inform the other of incidents that may impact the other. It is unclear whether such provisions are universal and how consistent the language used to define reportable incidents is.

Question

27. Please share your views on the proposals for incident reporting to a regulator, and to other affected parties. For example, views on the proposed indicative minimum threshold and conditions.

Customer incidents

The interdependent nature of networks and systems means that incidents that impact customers can also impact data centres and data centre providers. Such incidents may not have anything to do with the security of a data centre and its systems but instead, in the first instance, with a business customer.

Following a breach to a customer's space, equipment, or network, it can be possible for sophisticated threat actors to circumvent measures and protections to impact wider data centre networks and systems as well as move laterally and impact other colocated or co-hosted customers.

Incidents that might affect customers in the first instance but have a risk of wider impact are therefore also important to consider. Transparency around incidents, no matter their origin or initial target, can allow relevant parties to undertake incident management, including informing other affected parties if necessary.

The government has considered mirroring the duty for relevant data centre providers to notify customers of incidents so that customers are also obliged to reciprocate. However, it is currently minded to take a different approach for a number of reasons:

- this would mark a significant expansion of the scope of organisations in scope of the framework;
- there is a risk that such an approach could influence customer choice around their use of DPSI, impacting competition;
- the government judges that in this case behaviours are best suited to be driven through other means, such as guidance.

The government intends to encourage and support relevant data centre providers to include customer incident notification provisions in their service level agreements. We welcome feedback on providers' existing arrangements and the language used to determine notifiable incidents, and whether our support could help, whether it be in the form of guidance, the collecting and sharing of standardised clauses, or any other recommendation respondents to this consultation may have, including the expansion of legal duties to customers of data centre services.

Supply chain incidents and vulnerabilities

Incidents that directly impact other parties within the supply chain can impact data centre providers and their infrastructure and services.

Data centre providers rely on other organisations, including electricity suppliers, fuel suppliers, equipment suppliers, software providers, and telecommunications network providers. An incident or vulnerability affecting these different organisations or their product or services can impact data centres in different ways depending on the nature of their business. Examples might include fuel, electricity or equipment shortages which could inhibit data centres from operating at full capacity, or a DCIM software vulnerability, which could be exploited.

As with incidents that affect customers, transparency around any type of incident would allow for impacted parties to undertake incident management, such as communication of the existence and nature of the incident as well as contingency planning.

The government intends to encourage and support relevant data centre providers to include incident notification and vulnerability disclosure provisions within service level agreements.

We welcome any information that would help the government support the sector around this. We are mindful that supply chain agreements may have differences to those held with data centre customers and may not persist as an ongoing agreement. In these circumstances, the government urges data centre providers to be proactively vigilant to the vulnerabilities and risks that could arise within the supply chain and the equipment, software, and services they procure.

Questions

28. Please share your views on the proposed approach to customer incidents, and to supply chain incidents and vulnerabilities.

29. Please share any information you feel would be relevant on your Service Level Agreements with customers and supply chain actors. What forms of government support could assist with these agreements and arrangements for the sector?

Public disclosure

In certain scenarios the public may need to be made aware of a significant incident. The government intends to introduce or adopt a power for a regulator to inform the public of incidents. This power could only be used in constrained and select circumstances, for example, in instances where incidents:

- have a significant impact on the economy, on essential services, or on critical national infrastructure;
- involve bulk or sensitive data (non-personal data outside of the scope of GDPR);
- involve public safety or security;
- have an impact on national security.

A process of managed disclosure would be specified, to be followed by a regulator if this power was exercised. Managed disclosure would be important in order to minimise the risk of further impact and take into consideration the financial and reputational risk of parties involved. This process would involve close cooperation between all parties, and, where appropriate, the government and relevant agencies, before a decision to disclose to the public was reached.

Question

30. Please share your views on public disclosure. This may include views on the process described, the parties involved, and the examples given for circumstances that could lead to a regulator considering whether the public should be informed.

Cross-sector incident management

A single incident can impact multiple organisations and sectors. Due to the complexity of the infrastructure and services in question there is a risk of cascading failures causing widespread impact. For example, an incident on telecoms infrastructure may also impact data centres, other types of infrastructure, essential services, and customers. Communication, collaboration, and coordination in incident management is therefore key.

The government would encourage regulatory bodies or competent authorities of interdependent sectors, many of which are subject to incident reporting duties in legislation or regulation, to work together. It is important to pre-emptively establish common links between sectors as part of risk assessment and also to enable processes and procedures to be established or maintained to share information internally, with other affected parties, with regulatory bodies, and with relevant government agencies. This can feed into work to uncover systemic interdependencies, risks, impacts and ultimately allow for impacted sectors to be supported.

Such processes and procedures are already in place in many cases. The Digital Regulation Cooperation Forum (DRCF) is an example of good practice in inter-regulator coordination on online regulatory matters, and legal information gateways exist in some regimes. The government would adopt or introduce legal information gateways as needed to ensure data processing and storage infrastructure and relevant data centre providers are considered within this equation.

Regulatory model and function

A regulator would hold responsibility for the implementation of elements of the proposed framework and enforcement against non-compliance. Existing regulatory bodies are being considered to fulfil this function, but we do not propose to identify, designate, or establish an appropriate regulatory body until further views on the regulatory proposals have been received and assessed, and the resulting framework is developed in more detail. This would include consultation with existing regulators with responsibility for relevant areas.

The designated regulator would need to be equipped with the powers, resources, relationships, and expertise needed to effectively carry out its role. The government would consider whether multiple regulators may be required or enabled to collaborate to ensure effective and appropriate supervision and enforcement of specialist areas of security and resilience. For example, physical security and resilience, and cyber security and resilience.

In order to determine the appropriate regulator, the government would consider:

- Expertise, capabilities, and experience. The regulator should be efficiently resourced to understand and work with others to understand the sector, services and technologies within scope and be able to effectively use the regulatory tools provided.
- Relationships and influence. The regulator should have experience of collaborating with relevant stakeholders and the ability to use its influence and information channels.
- Aligned functions and objectives. The regulator's existing core functions and objectives should be aligned with the outcomes the framework aims to achieve and, if new functions are to be created, it should be feasible to align them.
- Funding model. Any existing funding models should be suitable and sustainable to effectively achieve the policy outcomes of the regulation.

Feedback provided in response to this consultation would shape any supervision and enforcement approach and therefore impact the body considered to be best placed to deliver it.

Proposed functions

The regulator would have functions that allow it to fulfil its remit to ensure relevant parties are suitably mitigating against security and resilience risks, including:

- Issuing and maintaining advisory and duty-bound guidance related to (non-exhaustively) security and resilience measures, incident reporting thresholds, testing and compliance.
- Maintaining a register of relevant entities in scope of the framework.
- Receiving, logging, and analysing information received through mechanisms in the framework, and working with relevant stakeholders, including government, government agencies and relevant regulators to make risk assessments.

- Monitoring the market to develop a holistic understanding of the sector and its dependencies.
- Taking prompt, effective, and proportionate enforcement action in the event of non-compliance.
- Supporting the UK government by providing information to assist in the risk assessments, the formulation of policy, incident management, and relevant national security functions. This would include, for example, details of registered providers and incident reports.

Principles

The government would seek to develop a supervisory model and enforcement approach with relevant stakeholders to serve its policy intent and outcomes, working with industry and relevant stakeholders to reflect commercial and operational pressures and considerations.

The regulator's approach to fulfilling its duties would have implications for the relevant data centre providers and the extent to which the outcomes of these proposals are met. We intend for the supervision and enforcement approach to be guided by a number of shared principles:

- **Risk-based:** the regulator should assess the risks to relevant data centre services and allocate its resources to the risks with the greatest impact on the sector and wider economy.
- **Effective and proportionate:** the regulator should focus on delivering policy outcomes and strategic objectives while considering industry burdens and risk in its approach.
- **Evidence-based and testable:** the regulator would build expertise and ensure interventions are measurable and then measured and evaluated for impact.
- **Pro-innovation and growth**: the regulator should pay regard to innovation and growth in its decision making.
- **Collaborative and transparent:** working with the sector, relevant agencies, and, where appropriate, the government, to share information and manage risks.

The regulator would have independence in how it acts on these principles and performs its functions. However, in select instances, it can be appropriate for regulators to be duty-bound to follow government direction on approaches, or adhere to certain principles, such as having regard to innovation and growth. The government is also considering whether there is a need to provide a mechanism to allow the periodic setting out of a statement of strategic priorities for the regulator, to provide further direction.

Risk-based supervision

The regulator would have a duty to take a risk-based proactive supervisory approach. Duties on organisations within scope would be applied uniformly but a regulator's oversight and

activities would be risk-directed, focused on mitigating risks with the highest impact to society. This is in line with our design principle of proportionality, and could mean that some relevant data centre providers, data centre services, or particular data centres are subject to lighter-touch supervision after an assessment of their risk profile.

Box 10: risk-based supervision in practice

A regulator would be empowered to independently "follow the risk" to ensure proportionality and allocate its resources effectively.

The government has designed this framework to ensure that a designated regulator would have the necessary information to make effective risk assessments.

A regulator would be able to seek and take into account the following:

- risk, threat, and intelligence information, assessments and reports from government agencies (such as the NCSC and NPSA), the government itself, and from external sources (where validated);
- information gathered through a regulator's power to seek information from relevant data centre providers to inform risk assessments;
- information on connected infrastructure such as digital infrastructure, CNI, and, and information on customer base/dependant organisations, such as Operators of Essential services OES;
- research and data the regulator or collaborating regulators have or develop on interdependent sectors, such as cloud and telecoms, and other digital infrastructure;
- information from tests, assessments, and certification against standards;
- incident reports;
- information gathered using enforcement powers, in instances where that was necessary.

The government would ensure that the designated regulator has the appropriate information sharing gateways to receive information and be legally able to share information with key stakeholders. It would be important to work closely with the National Cyber Security Centre, and the National Protective Security Authority across its supervisory responsibilities. The government would likely also require gateways beyond regular reporting mechanisms in order to receive timely information from the regulator to inform its policies and risk assessments.

Enforcement

The regulator would have a duty to enforce and a typical range of powers to enable it to do so. The regulator would use these powers in a proportionate manner, taking into account its effect on relevant data centre providers and the wider economy.

Box 11 - enforcement powers

Power to issue information notices involves requiring additional information from operators regarding alleged breaches. Once the regulator has acquired the additional information, it could be used to help the regulator determine whether further enforcement action is required.

Power to issue compliance or enforcement notices to relevant data centre providers if they do not meet the obligations set out in the framework, including the baseline security and resilience measures, and setting a timeframe to respond with an action plan, or interim steps, to rectify the issue.

Power to issue inspection notices, to verify the validity of information provided by operators. An inspection notice gives the regulator the ability to audit in-person, or designate a credible third-party to conduct inspections or tests. For example, an inspection notice could be issued to ensure that duties have been met.

Power to issue stop notices would ensure that a regulator has recourse to act in the event of continued noncompliance, and after no improvements were seen following prior enforcement action such as interim steps. A stop notice would mean that a relevant data centre provider must stop providing a data centre service in the UK within a specified period of time if they are in breach of legal duties and are likely to carry on being in breach of duties. Naturally, this power would be considered an option of last resort in situations where a serious security and resilience risk was posed by non-compliance.

The regulator would also need to have the power to issue civil fines for proven failures in clearly defined circumstances. Civil fines can be tied into metrics such as annual turnover. This power can be used where the use of other measures has not incentivised a change in behaviour.

We recognise that, if these proposals were to be implemented, relevant data centre providers must have confidence that any regulator is acting fairly and within its powers. Therefore, we would ensure that there is an appropriate mechanism to appeal the regulator’s decisions. In addition, the regulator would be accountable to Parliament to act within the bounds of its remit.

Funding

In line with the principles described in this consultation, we will explore a range of models to fund the necessary regulatory function. This would include working with existing regulators to

model prospective and retrospective cost recovery mechanisms, following best practice and precedents, as well as further engagement with industry.

As a baseline, it is likely that initial funding would come from the government and the costs of enforcement against individual organisations, such as inspection costs, would fall on regulated organisations. In addition, the regulator could also engage in cost recovery by charging fees to the regulated organisations. We would provide further detail through a published response to this consultation and costs would be fully modelled in an impact assessment.

Information gateways and safeguards

The regulator would be able to provide information to DSIT and other relevant government functions and agencies to inform assessments and policy development, such as analysing systemic dependencies and risks, as well as monitoring and evaluating the impacts of introduction and implementation of the framework, and for other purposes related to critical incident management and national security.

Information would only be shared within certain constraints and under safeguards. Non-exhaustively, this information could include:

- Incident reports.
- Registration information.
- Information on enforcement action taken by the regulator on an annual basis.
- Information that could result in significant threat to the economy, national security and public.

Where possible, the government and regulator would use existing legal information gateways to facilitate information sharing, and if and where needed, new gateways may be created.

The regulator would have access to and handle a range of data related to the organisations within scope. Therefore, it is crucial for the regulator to have safeguarding measures for the data. The safeguarding and handling of personal data would be subject to existing legislation (e.g. the Data Protection Act 2018 and UK GDPR).

Confidential and information on security or commercial interests of regulated organisations would be protected and handled responsibly. In most cases, information would only be shared with other designated parties (Security Agencies, Government) in an anonymised, aggregated, state, unless otherwise covered by appropriate legal information sharing gateways.

Questions

31. Please share any views on the Regulatory model and function section, including the proposed supervisory and enforcement approaches.

32. How much do you agree or disagree that the proposed powers are sufficient to effectively supervise the sector and enforce the proposed security and resilience duties? [scale from strongly disagree to strongly agree]

33. Which existing bodies should be considered as candidate regulators?

34. Please share your views on the proposed methods of funding. Are there further funding methods or avenues that you feel we should consider?

Monitoring and evaluation

The government recognises the importance of monitoring and evaluating the impacts of any statutory intervention to assess whether it is achieving policy objectives over time. We would ensure that testability, transparency, and accountability are built into the framework at the design stage. Our evidence base is currently being developed further and would provide a baseline for future monitoring and evaluation.

We would ensure that appropriate reporting mechanisms are in place for the framework and for the designated regulator. The introduction of any framework would be accompanied by a publicly available impact assessment, which would include more detail on the end-to-end monitoring and evaluation approach. This would also require effective engagement with the industry.

Questions

35. We welcome your views on the cost to businesses of the proposed framework should it be implemented. Please provide evidence.

36. We welcome views on costs to small and micro businesses in the UK of the proposed framework should it be implemented. In particular, consider how best to quantify the impact on profits of small and micro data centre providers. Please provide evidence.

Statutory vehicle

The government is taking a policy-first and statutory vehicle-agnostic approach to developing and delivering this proposed framework. They have been designed so that they could be:

- introduced through a bespoke or other relevant legislative vehicle, whilst being interoperable and where necessary aligned with other regulations for related and interdependent sectors;
- introduced through existing legislative frameworks, should that be deemed appropriate and effective.

Last year, the Government set out its intention to expand the NIS Regulations to include additional sub-sectors. Data infrastructure was explicitly not included for direct regulation under this proposed measure, as they were under review. The government may use the NIS regulations as a vehicle to regulate data infrastructure and deliver these, or components of these, proposals.

Environmental considerations

When designing effective and efficient regulation, we have considered the potential environmental harms that may occur as a result of proposals providing powers to set requirements, while ensuring that the aim of mitigating against disruption to or compromise of data held in third-party data centres is met. During our assessment, we have identified the following potential indirect environmental effects that may result of the proposed statutory framework proposals;

- The use and/or management of land and/or landscape through potential site, facility design and construction requirements.
- Greater greenhouse gas emissions through potential increased reliance on non-renewable electricity and back-up generators, if statutory requirements were to oblige or indirectly result in operators providing continuity of service or in the event of power blackouts without a mitigation against this.
- Pollution by waste as a result of operators choosing to dispose of redundant equipment if they decided to replace and / or upgrade IT equipment to meet requirements.

During the continuing policy formulation and implementation of proposals we will continue to consider the environmental effect of proposals and potential mitigation against harms.

Question

37. Please share your views on how to ensure unnecessary environmental harm would be mitigated to meet statutory requirements.

Catalogue of questions

Questions about the respondent

1. Are you responding as an individual or on behalf of an organisation?
    a. Individual
    b. Organisation
2. If you are responding on behalf of an organisation:
    a. Which of the following describes your organisation? [please refer to multiple if your organisation provides multiple services or infrastructure]
        i. Colocation data centre provider
        ii. Co-hosting or other non-Cloud data centre service provider (i.e. Hardware-as-a-Service [HaaS])
        iii. Cloud or hyperscale data centre provider
        iv. Managed service data centre provider
        v. Enterprise and on-premises data centre provider
        vi. Network data centre provider
        vii. Regional data centre provider
        viii. Edge data centre provider
        ix. Modular data centre provider
        x. Cloud platform provider (i.e. infrastructure-as-a-service [IaaS] or platform-as-a-service provider [PaaS])
        xi. Other cloud computing providers (e.g. Software-as-a-Service [SaaS])
        xii. Managed service provider (MSP) which provides data storage and processing services
        xiii. Managed service provider (MSP) which does not provide data storage and processing services
        xiv. Internet exchange point operator
        xv. Content delivery network provider
        xvi. Telecommunications operator

xvii. Financial services organisation

xviii. Trade body

xix. Research institution (e.g. academic organisation, think tank, etc.)

xx. Data centre supplier or service provider

xxi. Consultancy (e.g. security consultancy)

xxii. Data centre land and facility owner

xxiii. Real estate

xxiv. Other [please specify] - it may help to refer to SIC codes

b. How many data centres do you operate or are you responsible for part of? If necessary, please provide detail on the types of data centre you operate, or data centre services you provide.

c. Does your organisation operate in the UK, the EU and/or outside the EU?

3. Please describe your role or the capacity in which you are responding

Voluntary Measures and Industry Support Structures

4. What forms of digital or data-related infrastructure should the government the government consider for potential CNI designation?

5. How would you compare the expertise required to appropriately risk manage the colocation data centre sector to other critical sectors, such as Communications?

6. Are there particular benefits, opportunities, or risks to CNI designation for the colocation data centre sector that you would wish to draw our attention to?

7. What forms of intra-sector and sector-to-government voluntary cooperation would be most useful for the sector?

8. What voluntary cooperation mechanisms, if any, have you experienced in this or other sectors that demonstrate improvement to risk management?

9. Which issues lend themselves to intra-sector cooperation, and on which issues would industry welcome further government involvement?

Scope

10. Please share any views you may have on the definitional approach, and on the proposed indicative definitions for:

a. a data centre

b. relevant data centre services

i. colocation

ii. co-hosting

11. Please share, and explain, any views you may have on the proposed scope of third-party data centres, the operation of which are part of colocation and co-hosting services.

12. Of the services and infrastructure that are indicated as outside the scope of the proposed framework, are there any that you feel should be included, or that you feel require a different treatment? Please explain the reasons for your answer.

13. Please share any information that you consider might help to inform the government's scope approach. This might include, for example, information on the taxonomy of and terminology used to describe the data centre and data centre services landscape and market.

14. Please express your preference on the options set out for the treatment of data centres that are owned and operated by cloud service providers:

    a. Option A

    b. Option B(1)

    c. Option B(2)

    Please explain the reasons for your answer.

15. Please express your preference on the options set out for the treatment of data centres that are owned and operated by managed service providers:

    a. Option A

    b. Option B(1)

    c. Option B(2)

    Please explain the reasons for your answer.

16. Please share any views you may have on the proposed power to expand the scope.

    We are particularly interested in information on existing or emergent forms of data storage and processing infrastructure, data centre services, and connected infrastructure which may warrant future attention from the perspective of security and resilience.

17. Please share any views you may have on the proposed power to exempt from scope and set exemption thresholds.

We would welcome any information or evidence that could be helpful for the government to make a decision on any approach to small and micro-businesses, and to small data centres, whether initially, or using the proposed power.

18. How much do you agree or disagree that owners of third-party data centres should be included within the scope of the proposed framework? [scale from strongly disagree to strongly agree] Please explain the reasons for your answers to the previous question.

19. Please provide any information that you consider would be helpful to inform the government approach. For example, information on ownership and market structures, owner and wholesale leaseholder contractual arrangements and divisions of responsibility.

Registration

20. Please share your views on the information that could be required at the point of registration. Do you have any recommendations for other information or data that you feel should be required?

Security and resilience measures

21. How much do you agree or disagree that the proposed mechanisms to set security and resilience measures will provide the necessary capability to address security and resilience risks, now and in the future? [scale from strongly disagree to strongly agree]

    Please explain the reasons for your answers to the previous question.

22. How much do you agree or disagree that an outcome-based approach to the baseline measures is the most effective approach? [scale from strongly disagree to strongly agree]

    Please explain the reasons for your answers to the previous question.

23. Please share any comments or reflections on the indicative measures, including where there may be gaps.

    We would welcome views on whether there are any areas or measures where a more prescriptive approach may be required to effectively protect or enhance security and resilience.

Standards, assurance, and testing

24. Please provide information on your use of standards, assessment frameworks, and testing (and any other security and resilience assurance tools) for your UK operations, sites, and services using the table provided in the Catalogue of questions section.

This will be used to inform the design and potential implementations of the proposed standards, assurance, and testing mechanisms, and may inform the design of baseline security and resilience measures.

Question 24 – survey table						
Standard / assessment / assurance tool (if there are multiple versions or types, please indicate)	**Use (in the UK)** [Y/N]	**Primary reason for use** e.g. customer requirement, competitor-alignment, customer reassurance, because of controls/assurance provided	**Estimation of resourcing costs associated with use** (annually, in GBP, where possible)	**Self-assessed / third-party verified/certified** [S-A / TPV]	**Estimation of cost per third party assessment and frequency of assessment** (in GBP, where possible)	**Are costs proportionate to security and resilience benefits?** [scale from strongly disagree to strongly agree]
ISO/IEC 27001 and 2						
ISO/IEC 22301						
ISA/IEC 62443						
ISO/ IEC 22237						
EN 50600						
ANSI/TIA-942						
Uptime Institute Tier standard						
PCI DSS						
SOC1						

SOC2						
ANSI/TIA-942						
NIST CSF or SP						
Cyber Essentials						
Cyber Essentials +						
Cyber Assessment Framework (CAF)						
Other tools [please specify]						

25. How much do you agree or disagree with the proposed inclusion of an earned recognition mechanism to account for existing tools used in the sector? [scale from strongly disagree to strongly agree]
26. Please share any views on the proposed approach, and any design and implementation recommendations or suggestions you may have.
27. Please share any views you have on this section and these topics. This may include your views on the most effective and appropriate security and resilience-related standards, certifications, assurance assessments and testing for the sector.

Personnel

28. Please indicate whether you conduct any background checks on staff and/or require this of visiting contractors? If so, please share what they entail (i.e. overseas checks, financial checks and/or qualification and employment checks).
29. How confident are you that your current background checks provide sufficient risk mitigation? [scale from very confident to not at all confident]
30. Please share your views on the forms of government support that could help you conduct background checks.

Incident reporting

31. Please share your views on the proposals for incident reporting to a regulator, and to other affected parties. For example, views on the proposed indicative minimum threshold and conditions.
32. Please share your views on the proposed approach to customer incidents, and to supply chain incidents and vulnerabilities.
33. Please share any information you feel would be relevant on your Service Level Agreements with customers and supply chain actors. What forms of government support could assist with these agreements and arrangements for the sector?

Public disclosure

34. Please share your views on public disclosure. This may include views on the process described, the parties involved, and the examples given for circumstances that could lead to a regulator considering whether the public should be informed.

Regulatory model and function

35. Please share any views on the Regulatory model and function section, including the proposed supervisory and enforcement approaches.
36. How much do you agree or disagree that the proposed powers are sufficient to effectively supervise the sector and enforce the proposed security and resilience duties? [scale from strongly disagree to strongly agree]
37. Which existing bodies should be considered as candidate regulators?
38. Please share your views on the proposed methods of funding. Are there further funding methods or avenues that you feel we should consider?

Monitoring and evaluation

39. We welcome your views on the cost to businesses of the proposed framework should it be implemented. Please provide evidence.
40. We welcome views on costs to small and micro businesses in the UK of the proposed framework should it be implemented. In particular, consider how best to quantify the impact on profits of small and micro data centre providers. Please provide evidence.

Environmental considerations

41. Please share your views on how to ensure unnecessary environmental harm could be mitigated where organisations are required to meet statutory requirements.

General

42. Should provision be made for potential insolvency of significant data centres or other operators to prevent loss of cumulative UK capacity?

Analysis and evidence

Annex A contains a number of statistics produced via research and analysis, and also contains observations based on more anecdotal evidence. Please consider it from your individual business's point of view as well as looking across the wider industry and share any views.

43. To what extent do the estimates of the total revenue generated and number of people employed by data centres fit with your understanding?
44. Does the estimated number of data centres align with your knowledge and evidence?
    a. How many of the data centres are colocation data centres, co-hosting data centres, managed service providers and colocation managed service providers?
45. What are your views on the estimate that downtime costs the industry in the low single-digit billions per year (noting that there is a wide error range around this)?
46. Please share your views on the drivers behind decisions to supply data centre capacity:
    a. What was the decision-making process for the location of your facilities?
    b. What would be the potential benefits and disbenefits of locating them elsewhere, including in other UK locations or abroad?
    c. How do environmental considerations play a part in such decisions?
    d. If you had the power to change them, how would you change factors outside your direct control? For example, the ability of the grid to supply energy (has this restricted or will it restrict your ability to provide DC capacity?).
47. Do you have plans to expand capacity? If so, what type of facility would this expansion take the form of, and where would it be?
48. Annex A mentions that the industry is highly-concentrated.
    a. Do you have a view as to the market forces behind this?

b. Do you have views on whether the market forces are likely to change in future, particularly if edge becomes more prevalent?

49. Similarly, how do you think the market structure may be affected by use cases? For example, might AI lead to increased market concentration as a result of the need for large-scale compute capacity in one place, or might AI lead to a greater proliferation of smaller providers?

50. Do you operate edge data centres?

    a. If not, why not, and do you plan to expand into the edge market in future? Again, if not why not?

    b. If yes, how is this being delivered, i.e. what form of data centre are you/will you construct?

    c. How do you see the market for edge taking shape in future?

Annex A: Evidence Base and Impact of Proposals

Market size and structure

The size and structure of the 'data centre sector' is difficult to determine. Definitions of what a 'data centre' is (and specifically what a 'colocation data centre' is) vary, even within the industry. We also lack the definitive data on data centres and their operating models necessary to determine with high confidence how many data centres there are, especially since there is no statutory registration requirement or direct regulatory oversight.

Our current estimates range from around 250 to around 400 colocation data centres currently operating in the UK, representing around 1.5 GW of capacity across approximately half a million square metres of usable floor space.[11]

We estimate that around 90% of total colocation capacity is centred around London.[12] This is believed to be caused by a combination of the need to minimise latency for customers in the banking sector carrying out large numbers of rapid transactions and demands from a more general concentration of the IT industry in the south (increasing the convenience of physical access to data centre facilities). It is possible that there is also a feedback loop caused by induced demand.

Further, it may be the case that the construction and take up of edge in the future may be driven by, or itself drive, demand for low-latency applications outside London.

Total wholesale colocation capacity in London doubled[13] in the two years from 2018 to 2020 and continues to increase with additional capacity being constructed.

Economies of scale have historically been an important determinant of the structure of the market, which may be the main driver behind what is considerable market concentration. Two thirds of live capacity is operated by the ten largest operators. These are all multinationals headquartered overseas. Around two thirds of overseas-owned capacity is owned by US companies, with the remaining third split between Japan, Singapore, and China. It is possible that there is a feedback loop between concentration of market capacity, concentration of skills and economies of scale, given that the technical expertise required to design, construct and operate data centres are relatively specialised.

[11] European Data Flow Monitoring
[12] From an internal DCMS report compiled by Knight Frank.
[13] Ibid.

We estimate that UK colocation data centres are operated by approximately 170 data centre operator (DCO) companies. These generated an estimated total of £4.6bn in revenue in 2021 in the UK, and it is estimated that they employed approximately 17,000 people.[14]

DSIT research has, more broadly, identified around 800 data centre operators, including those which provide other managed data centre services (many of which may be considered managed IT services). It is estimated that around 80 operators provide such services as well as being a colocation operator.

This research shows that market concentration is also apparent in the revenue estimates:

- Of the £4.6bn total revenue, we estimate £4.3bn (94%) is generated by those which generate at least £40m in revenue per year.
- By count, these DCOs represent 10% (around 20) of all DCO companies.
- They employ around 15,500 people, which is 90% of all DCO employees. This suggests that these DCOs achieve slightly more productivity per employee than other DCOs, which makes sense given the economies of scale achievable in data centres.[15]
- The 10 largest operators which, as mentioned, are responsible for around two thirds of capacity, generate at least 80% of the total revenue.

This revenue estimate comes from The Data City, which employs a machine learning algorithm to identify data centre operators from their websites, discover them in publicly available Companies House data, and match this with their revenue in publicly available business listings. However, the identification of data centre operators also involved manual intervention and use of other sources. There are some caveats to this estimate:

- The set of businesses used in the estimates may not be definitive. There may be missing businesses or false positives.
- The revenue for each business is an estimate based on a combination of corporate accounting and reporting, and estimates made by business data providers.
- Corporate structures are sometimes complex, and the estimate may include or exclude revenue relevant or not relevant to data centre operations.
- In many cases, the £40m threshold is applied to the total of a number of related companies. This is to ensure revenue reported through group accounting or holding companies is not excluded, but also because DCOs are often split up in various ways (possibly for management or accounting purposes).

[14] Based on internal research and modelling at DSIT.
[15] In other words, if the largest companies generate 94% of all the revenue using 87% of all the employees, then each employee must, on average, contribute slightly more to the revenue of their employer than the other businesses, which use 13% of all the employees to generate only 6% of the revenue.

Dependency on Data Centres

Business behaviour is changing, with higher data utilisation and an increasing use of the cloud, and consequently data centres. Some indicative information on where businesses store their data, from the UK Business Data Survey 2022 (UKBDS)[16]:

- 83% of businesses that handle digitised data use standalone devices to store and process their data
- 19% said they use public cloud providers
- 15% said they use private cloud providers
- 14% said they use servers owned by their own business (whether in their offices or another location owned by the business)
- 4% said they use servers owned by them in a rented space in a data centre
- 7% said they use servers of an outsourced IT services provider
- 14% of UK businesses report that they house some or all of their data in data centres

Businesses were able to choose more than one of these options. Looking at businesses that chose one or more of the three answers 'use public cloud providers', 'use private cloud providers' or 'use servers owned by them in a rented space in a data centre', we see that 28% of all UK businesses use services housed in data centres (either directly or indirectly via the cloud). For large businesses (with at least 250 employees) this is 62%.

The options a given business chooses are likely to change as the business grows. This can include migrating to the cloud to leverage economies of scale or because the reliability and security are attractive or, for very large businesses, migrating from the cloud to their own infrastructure to avoid paying for the cloud provider's profit margins, once they are able to afford the capital cost. Certain businesses may also be attracted by speed, compute power, privacy and control, but not wish to fund high-end equipment, and so opt for other solutions, such as forms of hosting, bare metal servers, hardware-as-a-service or dedicated hosting, that may not be considered a form of cloud.

Perhaps the most pertinent individual figure is the 4% of businesses that use servers owned by them in a rented space in a data centre. This is substantially higher for medium (50 to 249 employees) and large (250+ employees) businesses, at 15% each. 4% of sole traders selected this answer which, subjectively, would seem quite high given the cost involved (this may indicate a misunderstanding of the question).

Businesses categorising themselves into the 'Information and Communication' and 'Finance and Insurance' sectors are the most likely to choose this answer. Businesses in London are more likely to choose this answer than businesses located elsewhere, although that may be

[16] Respondents could select more than one option.

because the two sectors mentioned are more likely to be based on London. More detail on these statistics can be found in the tables published alongside the UKBDS report, here.

In 2021, around 85% of UK live data centre capacity was in use.[17] Of London's capacity, around three quarters was taken up by cloud service providers.

According to the European Commission in its data flow monitoring research, in 2023, total cloud storage in the UK was estimated to be 157 EB (exabytes), and the volume of data flowing through cloud services in the UK is estimated to be approximately 330 PB (petabytes) per month. These are far in excess of other European countries. The table below shows this for the UK and the six European countries with the largest amounts.

The figures in brackets indicate the estimated growth since 2020. This shows that both storage capacity and the flow of data into and out of cloud facilities in data centres has more than doubled in the three years.

Country	Total cloud data flows, PB per month	Total cloud storage capacity, EB
UK	438 (130%)	158 (130%)
Germany	265 (160%)	96 (160%)
Italy	197 (130%)	71 (130%)
France	127 (140%)	46 (130%)
Spain	110 (130%)	40 (120%)
Netherlands	98 (150%)	36 (140%)
Sweden	78 (120%)	28 (120%)

European Commission forecasts indicate that the vast majority of the growth from 2022 to 2030 in storage capacity in EU27 countries will be at edge facilities rather than at 'main' data centres, and has itself set a goal for 10,000 edge data centres by 2030.[18] The UK may see a similar, independent growth in edge data centre capacity, driven by the market and in competition with EU and other international markets.

In the UK, it is estimated that around two thirds of data flows are from businesses with 250 or more employees.

[17] From an internal DCMS report compiled by Knight Frank.
[18] The EC's Economic Value of Data Flows Final Study Report forecasts a transition of data processing from main to edge, with a ratio of 80:20 in 2020 to 4:96 in 2030.

Outage Cost

Estimating the total cost per year of data centre outages is challenging. This is largely due to a lack of data on incidents, their causes and the costs. It is possible such data exists, but is decentralised and considered commercially sensitive, so that neither the UK government nor any other single organisation has access to it. It will require further research to understand the incident landscape and build a picture of the frequency and type of incidents, in anonymised form. It may also necessitate a reporting regime (which could take many forms, including one that is mostly automated) that will allow the UK government to monitor the ongoing health and performance of the industry.

Some research and modelling have been undertaken in recent months to begin to understand this at a high level, and an estimate of the cost of outages has been made. However, and again due to a lack of data, this excludes incidents involving unwanted access to data or data exfiltration, ransomware attacks and the like. It focusses on the direct cost of downtime, which may be caused by power or equipment failures, or human error.

Internal modelling carried out by DSIT estimates the average annual cost to the data centre industry of data centre outages to be in the low single-digit billions. This does not include costs unrelated to downtime, such as the impacts of unwanted access to data or ransomware attacks.

This modelling work is based on research carried out in late 2021 to early 2022 into the cost per MW of an outage at a data centre, and data on instances of cloud outages. This requires two main assumptions:

- That there is a linear relationship between the duration of an incident and its cost. This is known not to be true but insufficient data is available to remove this assumption.
- That cloud outages, with some adjustment, are a reasonable proxy for data centre outages.
- That 50% of cloud outages have data centre outages to blame.

The result is based on a relatively large number of short-duration incidents (less than an hour) and a small number of long-duration incidents (lasting several hours), although the total number of incidents is low, around 20 per year. This is likely not to include a much larger number of very small incidents, and further research is needed to understand this.

The other research mentioned above concluded that the knock-on cost to customers as a result of a loss of productivity amounts to, for 2019, something below £1.4bn (where all cloud outages upon which this figure is based had data centre outages to blame). Applying the 50% assumption above to this estimate, the knock-on impacts on productivity are approximately £0.7bn.

Market Dynamics

Until recently, delivery and take-up of edge capacity has been slower than initially expected, and capacity has been mainly concentrated into large data centre facilities, centred on a small number of geographical regions, predominantly London and Manchester. Historically, this has been driven by a combination of:

- economy of scale – one large 20 MW data centre is more efficient (in terms of energy, land use and staffing) than twenty 1 MW data centres;
- use cases – the concentration in London, for example, is driven by the need for low latency transactions at scale in the banking and finance sector; and
- geographical considerations – availability of suitable land and access to sufficient power from the grid.

However, it appears that the market structure looks both to expand outside the traditional South East concentration, and to diversify into a larger number of smaller colocation facilities, with a broader geographical spread, with many providers looking to provide facilities dedicated to delivering edge compute and storage (based on an examination of many data centre operators' websites, and anecdotal evidence from industry representative bodies). This is driven by:

- a demand in the market for localising physical access by customers (for installing/maintaining their own equipment);
- access to local power supplies;
- cheaper land outside London and the South East;
- environmental considerations including a cooler climate further north, and facilitating use of waste heat;
- market demand pushing the need for a variety of data centre designs that prioritise their different aspects differently for different types of customers and use types: latency, connectivity, price, resilience and security;
- development of architecture and control systems, enabling new types of data centre such as shipping container-sized or even locker-sized DCs for highly-distributed edge facilities;
- recognition that many use cases do not actually benefit sufficiently from low latency and that data centres can therefore be built further away from population centres where land is expensive; and
- in the longer term, and somewhat converse to the previous point, certain future use cases. For example, low-latency, 6G-enabled[19] applications such as autonomous vehicle control systems and remote surgery.

[19] 6G's goal is to deliver microsecond latency, as compared to 5G's millisecond latency.

Annex B: Responses to Call for Views

The Data Storage and Processing Infrastructure Security and Resilience Call for Views ran from May to August 2022, and focussed primarily on the security and resilience of data centre infrastructure and cloud platform infrastructure, and did not cover telecommunications infrastructure.

In it, we asked respondents to provide evidence and views that would help us understand the current landscape and potential options to best support and steward data storage and processing infrastructure providers. It sought to develop the government's evidence base, and collect views prior to developing policy.

Summary of Findings

Below is a summary of our (non-exhaustive) key points from the responses we received. This is a collection of significant or common claims and views, and does not reflect any analysis or commentary by the relevant team or Government on the relevance, validity or reliability of claims. We are grateful to all of those who responded to this call for views, as well as those who provided further views and commentary through subsequent discussions and correspondence around that time.

- There was broad agreement that the risks identified in our call for views were the right ones for the government to consider. In addition, respondents raised:
    - Risk of/associated with supply chain failure. Solutions proposed included forums bringing the data centre supply chain together, instilling security practices by placing them in government contracts, raising awareness of cybersecurity threats, and promoting best practice.
    - Risk associated with operators failing to fully engage with risks that seemed out of a single organisation's control, such as 'force majeure'-type risks, risks impacting the entire sector relatively equally, and geopolitical risks.
    - Risks associated with a lack of consistent information and awareness across government and the sector, including holding a picture of which data centres exist in the UK.
    - Risks related to climate change, and the importance of data centres to achieving net-zero. This included climate adaptation to natural hazards, such as heatwaves and flooding. Some data centre operators reported that most data centres are not equipped to deal with >38°C temperatures, and longer and hotter future heatwaves are a concern. One respondent also raised that redundancy and 'edge' poses a sustainability risk, as it increases energy demand and carbon footprint.

  - The impact of increased energy prices on data centre operators, and the constraints power availability places on the expansion of the sector – to the extent that it cannot meet demand. Changes to the Electricity Intensive Industries Scheme, clean energy levies and planning system were suggested as solutions.
  - Additional risks related to infrastructure serving the UK being located abroad.
  - Increasing risk associated with insufficient talent, due to a limited pool of relevantly skilled labour to draw on, and high levels of competition for those skills.
  - Increasing risk associated with digitisation and Internet of Things innovation, due to an increased attack surface, outages or compromises having wider cascade impacts along increasingly complex networks, and storage and processing activity occurring on devices that are not within the boundaries of control for cybersecurity teams.
- There was a notable difference between the views of operators of data infrastructure and other respondents (e.g. research institutions, consultancies) on the level to which risks are currently being mitigated.
  - Data Centre Operators and Cloud Service Providers self-reported that risks are largely mitigated in their facilities, although there were comments about credentials and consistency in assurance. The primary drivers of data centre operator security and resilience were the contracts with and expectations of enterprise customers (including cloud service providers), with subsequent high standards becoming a norm across the market. Cloud service providers were both regulated and subject to high expectations from customers. Generally, these organisations supported non-legislative interventions, or none at all.
  - Other respondents expressed alternative views, and supported stronger interventions including regulatory oversight (e.g. a regulatory body for all data infrastructure) to raise standards and consistency, penalties for non-compliance, increased transparency, similar licensing or regulatory regimes to peer countries, and targeted action based on tiering of organisations or systems.
- Evidence was provided by both major data centre operators and cloud service providers that significant resources are invested in physical security and resilience of data centres. However smaller and non-colo (e.g. enterprise or managed service) data centres may be less physically secure given they are more likely to be ‘done on a budget’.
- Some respondents stated cybersecurity risk largely relates to the servers owned by data centre operators’ customers (e.g. cloud service providers, businesses), and the software services layer hosted on those servers. While there is some evidence of a relatively small attack surface for data centre operators themselves, it could lead to potential blind spots for areas used by multiple organisations (e.g. meet-me rooms), or for risks that could be overlooked unless a systems approach to digital security risk management is taken. Additionally, evolving service offerings, increasing network complexity, automation, and remote monitoring and control have and may continue to expand the attack surface.

- The facilities infrastructure underlying the functioning of data centres is controlled using industrial control systems and relies on operational technology and Industrial IoT. Respondents strongly highlighted the growing cyber risks around IT and operational technology convergence. Operational technology security has not kept pace with that of IT, and this is a risk that will worsen with future technological change if not addressed. Industrial control systems supplier security practices need strengthening.
- Many respondents recognised a broad trend of increasing security and resilience risks across all industries (with particular attention to cyber). Views were mixed as to whether the sector was keeping pace. There was demand for more proactive horizon-scanning analysis of the 'attack surface' and how this is changing as technology progresses and demand increases, along with mitigation, planning and sharing.
- Many respondents referenced the 'shared responsibility' between data centre operators and their customers (e.g. cloud service providers), and cloud service providers and their customers (e.g. a business). This is the premise a provider can only do so much for security and resilience, and some responsibility must lie with the customer. There is a risk that displaced responsibility and confidence in the security of cloud service providers and data centres can lead to a false sense of security for customers. The risk lies where this is ill-defined or misunderstood.
- Some respondents felt that concentration of physical infrastructure and the cloud market causes security and resilience risks by creating single points of failure. Alternative views were also shared that concentration can result in security benefits, as larger cloud service providers and data centre operators have consistently higher security standards. Hybrid cloud (public and private cloud) and multi-cloud architecture (IT setups enabling the use of multiple cloud service providers simultaneously) were suggested as one solution. Another suggestion called for Government advice to CNI operators on the location of their infrastructure, mandatory declaration of which data storage and processing sites CNI providers were using, and a secure Government register of the sites operators use.
- Some respondents were conflicted about the relative security and resilience of different market structures and technologies. Moving data and resources away from fixed premises and to 'the edge' could improve resilience, while others felt this increases vulnerability through duplication and data being less in direct control of operators.
- A number of respondents were supportive of the Government working closely with stakeholders to deliver a forum that facilitates information-sharing and collaboration among data centres, but also customers and trade associations. Voluntary information-sharing was promoted, as well as threat assessment sharing by the Government. Some respondents suggested that there should be legal incident response information-sharing and cooperation requirements placed on industry.
- Respondents raised challenges with post-incident recovery, such as varying levels of preparedness across sectors, vulnerable supply chains and industrial control systems, difficulty in knowing whether a breach has occurred and how to restore trust following this, and inherent resilience risks in the traditional fixed-premises data centre/Cloud

model. Greater attention to these challenges, and a shift toward '5G/edge computing' were suggested.

- Respondents also raised the high demand for, but lack of availability of, technical skills. This included cloud security skills, as well as management of infrastructure physically and remotely. This 'technical debt' is likely to increase in future (across the UK tech sector). Respondents who operated data centres generally felt sufficient staff were allocated to security and resilience, but there were mixed views among other respondents.
- Respondents provided lengthy submissions on standards, and highlighted a wide range of standards that data centres use, although few are designed for data centres specifically. Some argued that these are useful when implemented properly, not just as part of a tick-box approach or marketing, or saying they are equivalent to a standard without actually being certified.
    - Many respondents felt standards were important, as they inform and evidence security and resilience measures and practices, and felt government should lean on these recognised standards for any potential interventions. Interventions could include working to keep standards up-to-date, creating conformity assessment procedures, and ensuring standards are part of any guidance or legislation as this would, amongst other things, ensure global applicability and interoperability, as well as independent assurance of compliance.
    - If regulation was chosen as a suitable intervention, this should be targeted, proportionate, flexible, future proof and have an element of international alignment.
- Respondents who operated data centres claimed that the existing costs of legal and regulatory compliance were significant but proportionate to the benefits. Risks associated with compliance include increasing prices and/or squeezing profits (which can reduce investment), also presenting significant barriers for new market entrants.
- Opponents to regulation mainly claimed that standards of security and resilience were sufficiently high, and voiced concerns of unnecessarily adding to an already complex regulatory landscape. Multiple respondents suggested a need for more clarity and consistency, particularly where organisations operate internationally and are subject to varying regulatory frameworks (e.g. EU Network and Information Systems). One data centre operator stated that they are not particularly worried about new regulations, due to dealing with global regulations and standards.

Support and encouragement for government regulation came primarily from non-data centre operators, but private corporations and cloud service providers also had recommendations for particular types of regulation. There was a strong consensus that any regulations should be standards-aligned, targeted and flexible. This would mean they are proportionate to the risks, would minimise international regulatory compliance burden (e.g. EU Network and Information Systems) and be future proof. Some data centre operators shared similar views on design, if regulation was to be introduced.

This consultation is available from: www.gov.uk/government/organisations/department-for-science-innovation-and-technology

If you need a version of this document in a more accessible format, please email alt.formats@dsit.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.