Policy questions on the Cyber Security and Resilience (CSR) Bill

Introduction

DSIT is updating the NIS Regulations through the Cyber Security and Resilience Bill to strengthen the UK's defences and ensure that more essential digital services than ever before are protected. DSIT ran a consultation on the policy proposals in 2022, however there are some evidence gaps that need to be addressed or updated. We invite you to fill out this Call for Evidence on some of our proposals to help DSIT assess the impact of the changes on those who are already regulated by the NIS Regulations or who will be regulated by the forthcoming CSR Bill.

We ask that you do not share any personal data in this survey as this may result in that part of your response being deleted.

This survey is being shared with a wide range of stakeholders, both those that are regulated under the NIS Regulations currently and those that **may** be captured under the 2022 proposals. The survey will introduce the sections of the NIS Regulations that may change with a very brief introduction.

If you are not currently regulated by the NIS Regulations, we encourage you to review the gov.uk page that covers a brief overview.

Screeners

Is your organisation currently regulated by the UK NIS Regulations?

- Yes
- No

If yes, who is your competent authority?

[list all 12 CAs]

If no, who would likely be your competent authority?

[list all 12 CAs] + Don't know

How large is your organisation?

- Micro (2 - 10 employees)
- Small (11 – 49 employees)
- Medium (50 – 249 employees)
- Large (250+ employees)

Which sector(s) do you operate in? Tick all that apply

Energy
Health
Drinking Water
Transport
Digital infrastructure
Digital services (including a relevant digital service provider of cloud services, but excluding managed services)
Managed services*
Other (please specify)

*DSITs proposed characteristics of a Managed Service Provider have 4 criteria:

1. *The service is provided by one business to another business, and*
2. *The service is related to the provision of IT services, such as systems, infrastructure, networks, and/or security, and*
3. *The service relies on the use of network and information systems, whether this is the network and information systems of the provider, their customers or third parties, and*
4. *The service provides regular and ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, IT network, and/or the security thereof.*

Questions targeted at firms currently regulated by NIS

RDSPS will select ICO on who their competent authorities are.

OESs is everyone else.

Incident reporting

The NIS regulations require regulated entities to report high impact cyber incidents to their regulator. We are considering introducing changes to these reporting requirements via the Cyber Security and Resilience Bill to ensure more incidents are reported and that incident information is communicated to relevant parties more quickly and clearly. These changes include:

1) A change to the definition of an incident under the existing NIS Regulations. To meet the current reporting threshold, an incident must have led to a significant or substantial disruption to service continuity. We are proposing to change the definition of a reportable incident to ensure that a wider range of incidents are captured, including incidents capable of resulting in a significant impact to service continuity and incidents that compromise the integrity of a network and information system.
2) A change to the amount of time an organisation has to report an incident from when it is detected. Currently, incidents must be reported without undue delay and no later than 72 hours after being made aware of the incident. We are assessing whether this time can be reduced to no later than 24 hours after being made aware of the incident.
3) New transparency requirements. We are considering introducing a transparency requirement which will ensure customers are notified of incidents which significantly compromise the integrity of a digital service upon which they rely.

The following questions look to capture what impacts these measures might have on firms currently regulated by NIS.

Changing the reporting timescale - 24-hour reporting

1. Which members of staff are needed to develop and submit an NIS incident report? [**To firms – small and micro businesses and medium/large**]
2. Do you have the people required to submit an incident report already working weekend shifts? [**To firms – small and micro businesses and medium/large**]
3. Could you have staff on call as opposed to working weekend shifts in case there is the need to report an NIS incident? Could you save money by calling in members of

staff when an incident is detected? [**To firms – small and micro businesses and medium/large**]

4. Is there a higher rate of pay for staff working weekends than those working during the week? If so, what overtime rate do staff get paid? [**To firms – small and micro businesses and medium/large**]

Transparency requirement

5. If an incident occurred which affected a service you provide, would you be able to identify which customers have been affected? ('Customers' in this question should be interpreted as businesses which rely on a digital service provider for a service, not individual clients.) If so, how long would it take to identify which customers have been affected? **[For RDSPs]**
6. Do you have a plan in place for what to do if an incident occurs? **[For RDSPs]**

Managed Service Providers (MSPs)

In the 2022 consultation, DSIT proposed expanding the definition of a Relevant Digital Service Provider, to include Managed Service Providers. The following questions are to better understand the impacts of the measure and how to reflect the definition to include the right firms in the scope of the NIS Regulations.

7. **[for OES]** Do you use services provided by an MSP[1] (or multiple MSPs) to deliver your essential service(s)? This would also include, for example, companies which provide IT outsourcing, BPO (business process outsourcing) where it is provided through IT networks, or cyber security services.
    a. If yes, please provide examples of where these services provided by an MSP (or multiple MSPs) are critical to the provision of your essential service? *(note: names of companies are not required)*
8. **[for RDSPs]** Do you provide managed services[2]? This would include, for example, providing IT outsourcing, Business Process Outsourcing (BPO) where it is provided through IT networks, or managed security services.

[1] By MSP we mean an entity which provides a service that is:
1.provided **by one business to another** business **and**,
2.related to the **provision of IT services**, such as systems, infrastructure, networks and/or security, **and**
3.relies on the **use of network and information systems**, whether this is the network and information systems of the provider, their customers or third parties **and**,
4.provides **regular and ongoing management support**, active administration and/or monitoring of IT systems, IT infrastructure, IT network and/**or the security thereof.**

[2] By managed service we mean a service which is:
1.provided **by one business to another** business **and**,
2.related to the **provision of IT services**, such as systems, infrastructure, networks and/or security, **and**

If yes to {8} the following questions.

9. Do you provide Business Process Outsourcing (BPO) services that involve ongoing management of an IT system/ infrastructure/ network and have a connection or access to the customer?
    a. If yes, please provide examples of the BPO services provided by your organisation.

10. Do you provide managed IT services that secure or manage operational technology (OT)?
    a. If yes, please provide examples. Detailed examples are welcome, particularly where these relate to critical national infrastructure (CNI).

11. Do you provide system integration?
    a. If yes, is the system integration provided as part of a managed service? Please provide examples of the system integration you provide as part of a managed service.
12. Do you provide telecommunications services (e.g. WAN, LAN)?
    - If yes, please provide examples of the telecommunications services you provide.
    - If yes, do you consider that any of these telecommunication services constitute a 'managed service'?
    - If yes, are these telecommunications services regulated under the Communications Act 2003?

13. Is the cyber security of the services you provide (in the UK or overseas) currently regulated? Are you currently regulated for the cyber security for any of your services offered (in the UK or overseas)?
    - If yes, please provide details of these regulations.

Small and micro digital service providers

14. **[for OES]** Are you aware of any small and micro cloud or managed services in your supply chain? For example, companies which provide IT outsourcing, cloud services, Business Process Outsourcing (BPO) and cyber security services.

3.relies on the **use of network and information systems**, whether this is the network and information systems of the provider, their customers or third parties **and**,

4.provides **regular and ongoing management support**, active administration and/or monitoring of IT systems, IT infrastructure, IT network and/**or the security thereof.**

a. If yes, please provide examples of the functions these supply (note: names of companies are not required)

Critical Dependencies

In 2022 DSIT proposed to regulate the firms in the supply chain that are a critical dependency for the wider sector. The following questions look to capture the potential impacts of different parts of the measure.

Operational Technology (OT)

15. Does your organisation use operational technology to manage any critical or essential services?

16. [if yes to 15] If you purchase operational technology (OT) from a vendor, do you maintain and operate it 'in house'?

17. [if yes to 15] Do you outsource the management of operational technology (OT) to third party providers?
    a. If yes, are these third party providers Managed Service Providers (MSPs)*? (i.e., the same company that manages your IT) systems/networks/Infrastructure)
    b. If yes, please provide examples of operational technology (OT) that you outsource to third parties (note: a description of the company would suffice, names are not required)

* DSIT's proposed characteristics of a Managed Service Provider have 4 criteria:
1. The service is provided by one business to another business, and
2. The service is related to the provision of IT services, such as systems, infrastructure, networks, and/or security, and
3. The service relies on the use of network and information systems, whether this is the network and information systems of the provider, their customers or third parties, and
4. The service provides regular and ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, IT network, and/or the security thereof.

Managing risks

DSIT is keen to understand the range of costs that regulated entities might incur when responding to incidents that have compromised or disrupted their network and

information systems. The following questions seek to understand the cost impacts that might be incurred in relation to the most serious incidents, where wholesale changes are needed to manage the risks.

18. How much would it cost your organisation to conduct a full rollout of multi-factor authentication for all users?
19. How much would it cost your organisation to conduct a full organisation-wide reset of passwords?
20. What other actions do you anticipate you might need to take to protect your organisation in the event of a major cyber security attack or resilience incident?

Questions targeted at firms not regulated by NIS

RDSPs will select ICO on who their competent authorities are.

OESs is everyone else.

Incident reporting

The NIS regulations require regulated entities to report high impact cyber incidents to their regulator. We are considering introducing changes to these reporting requirements via the Cyber Security and Resilience Bill to ensure more incidents are reported and that incident information is communicated to relevant parties more quickly and clearly. These changes include:

4) A change to the definition of an incident under the NIS Regulations. To meet the current reporting threshold, an incident must have led to a significant or substantial disruption to service continuity. We are proposing to change the definition of a reportable incident to ensure that a wider range of incidents are captured, including incidents capable of resulting in a significant impact to service continuity and incidents that compromise the integrity of a network and information system.
5) A change to the amount of time an organisation has to report an incident from when it is detected. Currently, incidents must be reported without undue delay and no later than 72 hours after being made aware of the incident. We are assessing whether this time can be reduced to no later than 24 hours after being made aware of the incident.
6) New transparency requirements. We are considering introducing a transparency requirement which will ensure customers are notified of incidents which significantly compromise the integrity of a digital service upon which they reply.

The following questions look to capture what impacts these measures might have on firms currently regulated by NIS.

Changing the timescales - 24-hour reporting

21. Which members of staff are needed to submit an external incident report? [**To firms – small and micro businesses and medium/large**]
22. Do you have the people required to submit an incident report already working weekend shifts? [**To firms – small and micro businesses and medium/large**]

23. Could you have staff on call as opposed to working weekend shifts in case there is the need to externally report a cyber incident? Could you save money by calling in members of staff when an incident is detected? [**To firms – small and micro businesses and medium/large**]
24. Is there a higher rate of pay for staff working weekends than those working during the week? If so, what overtime rate do staff get paid? [**To firms – small and micro businesses and medium/large**]

Critical dependencies

Operational Technology (OT)

25. If you purchase operational technology (OT) from a vendor, do you maintain and operate it 'in house'?

26. Do you outsource the management of operational technology (OT) to third party providers?
    a. If yes, are these third party providers Managed Service Providers (MSPs)*? (i.e., the same company that manages your IT systems/networks/Infrastructure)
    b. If yes, please provide examples of operational technology (OT) you outsource to third parties (note: a description of the company would suffice, company names are not required)

DSIT's proposed characteristics of a Managed Service Provider have 4 criteria:

5. *The service is provided by one business to another business*
6. *The service is related to the provision of IT services, such as systems, infrastructure, networks, and/or security*.
7. *The service relies on the use of network and information systems, whether this is the network and information systems of the provider, their customers or third parties*.
8. *The service provides regular and ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, IT network, and/or the security thereof*.

Managing risks

DSIT is keen to understand the range of costs that regulated entities might incur when responding to incidents that have compromised or disrupted their network and information systems. The following questions seek to understand the cost impacts that might be incurred in relation to the most serious incidents, where wholesale changes are needed to manage the risks.

27. How much would it cost your organisation to conduct a full rollout of multi-factor authentication for all users?
28. How much would it cost your organisation to conduct a full organisation-wide reset of passwords?

Small and micro MSPs/CSPs

29. [**For MSPs/Cloud service providers]** are you a small or micro entity (add definition} If yes, do you supply CNI or essential services? Please indicate "yes" to the following:

    - Chemicals
    - Civil Nuclear
    - Communications
    - Defence
    - Emergency Services
    - Energy
    - Finance
    - Food
    - Government
    - Health
    - Space
    - Transport
    - Water
    - Digital Infrastructure (*i.e. Digital infrastructure is the physical hardware and software-based technologies that enable digital services, e.g. DNS Domain Name System).*
    - Other (specify)

Managed Service Providers

In the 2022 consultation DSIT proposed expanding the scope of digital services regulated under the NIS Regulations to include "managed services". "Digital services" currently include online marketplaces, online search engines and cloud computing services.

The following questions will help us better understand the impacts of the measure and how to reflect the definitions to include the right firms in the Cyber Security and Resilience Regulations.

30. [For MSPs] Do you provide Business Process Outsourcing (BPO) services that involve ongoing management of an IT system/ infrastructure/ network and have a connection or access to the customer?

a. If yes, please provide examples of the BPO services provided by your organisation.

31. [For MSPs] Do you provide managed IT services that secure or manage operational technology?
    a. If yes, please provide examples of the managed IT services you provide that secure or manage operational technology. Detailed examples are welcome, particularly where these relate to critical national infrastructure (CNI).
32. [For MSPs] Do you provide system integration?
    a. If yes, is the system integration provided as part of a managed service?Please provide examples

30. [For MSPs] Do you provide telecommunications services (e.g. private WAN, LAN)?
    - If yes, please could you provide examples?
    - If yes, do you consider any of these services to constitute a 'managed service'?
    - If yes, are these services regulated under the Communications Act 2003?

33. Is the cyber security of the services you provide (in the UK or overseas) currently regulated? Are you currently regulated for the cyber security for any of your services offered (in the UK or overseas)?
    - If yes, please provide details of these regulations.

Questions targeted at Competent Authorities (CAs)

Incident reporting

24-hour reporting

34. Do you have people working weekend shifts that would be able to receive incident reports? If not, who would be required to work the weekend shifts?
35. If you have staff on available to manage an incident report received at weekends or in the evenings, are these staff on site or on call? How many people do you have working in the evenings / at weekends?
36. Do you pay overtime at weekends / evening shifts?

Cost Recovery

37. Please provide an overview of the types of organisations you regulate. Specifically, please provide a breakdown of the number of private and public organisations and their size (e.g. micro, small, medium, large).

Split between public and private

Type of business	Private	Public
All firms	%	%

Size of public and private

Type of business	Private	Public
Micro	%	%
Small		
Medium		
Large		
Total	100%	100%

[for CAs and the ICO]

Critical dependencies

Supplier contracts

38. Do any Competent Authorities currently review the supplier contracts of regulated entities to ensure that appropriate measures are being taken to manage supply chain risk? E.g. that regulated entities have visibility of their suppliers' supply chain, have some level of assurance of the cyber security and resilience measures

followed by their supplier, and/or have the right to audit their supplier? If so, please share details

Data centres

39. How many standalone data centres are owned and operated by OES/RDSP/MSP businesses under your remit in the UK?
40. Do you include standalone data centres owned and operated (enterprise data centres) by OES/RDSP businesses under your remit in your supervisory activity?
    a. If no under your current scope, have you previously considered or are you currently considering expanding your supervision to focus on your sector's enterprise data centres?
    b. If yes, what compliance obligations are applicable to and what assurance is required in relation to OES/RDSP owned-and-operated data centres? *For example, appropriate and proportionate measures + CAF*.
    c. If yes, are there any measures or assurance designed for the data centre infrastructure that you apply and/or assess for your sector's data centres (or that guide your supervision) under the NIS? *For example, standards designed for operational resilience of data centre infrastructure, the cyber security of operational technologies/industrial control systems, or levels of physical security of data centres*.
41. To what extent do you agree with the following statements:
    a. It would be beneficial to have standardised guidance on "appropriate and proportionate" measures in relation to the security and resilience of data centres / data centre infrastructure
        i. Strongly agree
        ii. Agree
        iii. Neither agree nor disagree
        iv. Disagree
        v. Strongly disagree
    b. UK third-party operated data centres should be brought into the scope of the NIS under dedicated supervision with a view to protecting them as CNI and OES/RDSP supply chains?
        i. Strongly agree
        ii. Agree
        iii. Neither agree nor disagree
        iv. Disagree

v. Strongly disagree