



CALL FOR VIEWS ON CYBER SECURITY IN SUPPLY CHAINS AND MANAGED SERVICE PROVIDERS

Issued 23 June 2021

ICAEW welcomes the opportunity to comment on the Call for views on cyber security in supply chains and managed service providers published by Department of Culture, Media and Sport on 17 May 2021, a copy of which is available from this [link](#).

ICAEW

Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
T +44 (0)20 7920 8100 F +44 (0)20 7920 0547 icaew.com

The Institute of Chartered Accountants in England and Wales (ICAEW) incorporated by Royal Charter (RC000246)
Registered office: Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

This response of 23 June 2021 has been prepared by the ICAEW Tech Faculty. Recognised internationally for its thought leadership, the faculty is responsible for ICAEW policy on issues relating to technology and the digital economy. The faculty draws on expertise from the accountancy profession, the technology industry and other interested parties to respond to consultations from governments and international bodies.

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 156,000 chartered accountant members in over 149 countries. ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and apply the highest professional, technical and ethical standards.

© ICAEW 2021

All rights reserved.

This document may be reproduced without specific permission, in whole or part, free of charge and in any format or medium, subject to the conditions that:

- it is appropriately attributed, replicated accurately and is not used in a misleading context;
- the source of the extract or document is acknowledged and the title and ICAEW reference number are quoted.

Where third-party copyright material has been identified application for permission must be made to the copyright holder.

For more information, please contact: representations@icaew.com

KEY POINTS

1. Cyber risk management should not be seen in isolation. As with cyber security more generally, it needs to be integrated into business processes rather than operating as a separate IT-focused silo. In the context of supplier management, cyber risk management therefore needs to be part of a full life-cycle supplier management process which connects a number of functions, including IT/cyber security, legal, procurement and relevant business or commercial functions. Crucially, though, consideration of cyber risks must go beyond the initial procurement process. Regular checks of how key processes are being implemented should be considered and built into supplier management processes.
2. SMEs are likely to have the biggest issues in supply cyber risk management, with low levels of awareness of the risks, limited time and capabilities, and few cheap tools available to help. Government attention should therefore be focused on how to best help this sector, through actions such as guidance, templates and standard cyber-related information about major tech suppliers.
3. However, the lack of baseline and reusable standards is also a substantial problem for all organisations. Too much time and effort is currently wasted filling in bespoke questionnaires on security practices which add little to risk management. Cyber Essentials Plus is a useful tool but it is not necessarily suited to larger organisations or more complex or risky situations. The government should therefore also prioritise having a broader baseline standard which can provide a starting point for supplier risk management, avoid duplication of work and be added to as needed in individual cases.

ANSWERS TO SPECIFIC QUESTIONS

Question 1. How much of a barrier do you think each of the following are to effective supplier cyber risk management? [Severe barrier, somewhat of a barrier, not a barrier, don't know]

- Low recognition of supplier risk - **severe barrier**
- Limited visibility into supply chains - **somewhat of a barrier**
- Insufficient expertise to evaluate supplier cyber risk - **somewhat of a barrier**
- Insufficient tools or assurance mechanisms to evaluate supplier cyber risk - **somewhat of a barrier**
- Limitations to taking action due to structural imbalance - **severe barrier**

Question 2. Are there any additional barriers preventing organisations from effectively managing supplier cyber risk that have not been captured above?

- Yes

Question 3. [If Yes] What additional barriers preventing organisations from effectively managing their supplier risk are you aware of?

4. Different types and sizes of organisation are impacted by the barriers in different ways. In smaller organisations, the biggest barrier is likely to be low recognition of supplier risks, along with lack of time and expertise. In larger organisations, the barriers are more likely to be focused on access to large suppliers to audit them or get the required information.
5. We would also highlight the specific problems caused by the lack of a baseline standard beyond Cyber Essentials Plus. The resulting proliferation of bespoke questionnaires or reliance on a variety of international standards creates a lot of duplication and diverts attention from more valuable risk management activities. Cyber Essentials Plus has been a useful tool to help in supplier management, either through mandating compliance or enabling companies to demonstrate a baseline of practices. However, this is inadequate for many larger organisations or higher-risk settings, and further work to broaden the baseline would be very welcome to many organisations.

Question 4. Have you used the NCSC's Supply Chain Security Guidance?

6. No

Question 5. How challenging do (or would) organisations find it to effectively act on these principles of supply chain cyber risk management, as outlined in the NCSC's Supply Chain Security Guidance? [Not at all challenging, slightly challenging, very challenging, don't know]

- Understanding the risks - **slightly challenging**
- Establishing control - **very challenging**
- Checking arrangements - **very challenging**
- Continuing to improve, evolve and maintain security - **very challenging**

Question 6. What are examples of good practice for organisations implementing these aspects of supply chain cyber risk management?

7. Understanding the risks - doing detailed risk assessments of suppliers is a key part of the process, as well as being prepared to make difficult decisions where suppliers do not fare well in the assessment. Where risks are identified, it is preferable for larger organisations to help suppliers improve their security, especially with small companies. Working with business representatives can help to identify where suppliers are particularly valued and therefore where investment in security would be beneficial. However, where needed, companies need to be prepared to drop suppliers if the identified risks are too great, or if the supplier refuses to provide adequate information for an assessment to be made.
8. Establishing control - we would highlight the value of penetration testing in identifying issues and building confidence in the suppliers' security. This can be hard to agree in contracts, however, with suppliers simply sharing the fact that they have been penetration tested. Where it is possible to gain more information about the scope (e.g. environment in which the test was carried out, and what tests were covered) and results (such as written affirmation that any critical vulnerabilities identified have been remediated) of any testing, this can be particularly useful information.
9. Checking arrangements - as highlighted earlier, the lack of clear and consistent standards in this area is problematic and we would recommend further work on this as a matter of priority.
10. Continuing to improve, evolve and maintain security – as highlighted earlier, working with suppliers to suggest and discuss potential security improvements or solutions is an important priority for many larger organisations.

Question 7. What additional principles or advice should be included when considering supply chain cyber risk management?

11. It is important to put cyber risk management in a much broader context of effective supplier management. Cyber needs to be integrated into good practices around the end-to-end management of suppliers and should not be seen in isolation. This is not the same as good procurement. It requires follow up on, for example, incident management, and regular reviews of security practices.
12. Furthermore, good practices have many touchpoints across the organisation. It is not simply a matter for IT or the cyber security team. Rather, it needs close co-operation with procurement specialists, legal departments and the commercial or business teams that will be using the suppliers. It also needs an international perspective to understand the location of data and associated risks of that.

Question 8. Have you used or do you plan to use the NCSC's Supplier Assurance Questions?

13. No

Question 9. Since publishing the NCSC's Supplier Assurance Questions, it has been noted that the guidance could also cover the use of supplier-provided apps (e.g. where a supplier requires use of apps on an organisation's network to deliver its service to that organisation). Are there any additional areas of supplier assurance that should be outlined?

14. Don't know

Question 10. 9[If Yes] What additional areas of supplier assurance should be outlined?

15. No comment

Question 11. How effective are the following commercial offerings for managing a supplier's cyber risk? [Not effective, somewhat effective, very effective, don't know]

- Private supplier assurance – **don't know**
- Platforms for supporting supplier risk – **don't know**
- Supply chain management system providers – **don't know**
- Risk, supply chain and management consultancies – **don't know**
- Suppliers of outsourced procurement services – **don't know**
- Industry cyber security certification schemes – **don't know**

Question 12. What additional commercial offerings, not listed above, are effective in supporting organisations with supplier risk management?

16. GRC portals are very useful tools that can help larger organisations stay on top of supplier management processes. However, these tools are expensive and therefore unlikely to be relevant to smaller organisations. More affordable tools, especially those with high levels of automation, could help smaller organisations develop a structured and continuous processes of managing the cyber risks of suppliers.
17. We would also highlight the value of open-source intelligence and risks assessments of suppliers and further products or services in this area could be useful.

Question 13. How effective would the following government actions be in supporting and incentivising organisations to manage supply chain cyber risk? [Not effective, somewhat effective, very effective, don't know]

- Awareness raising of the importance of supply chain cyber risk management through the use of campaigns and industry engagement - **somewhat effective**
- Additional support to help organisations to know what to do, such as: improved or additional advice and guidance; a tool that draws on existing advice and standards to help organisations manage supplier cyber risk - **somewhat effective**
- Providing a specific supplier risk management standard that: outlines minimum and good practice and/ or provides assurance that an organisation is managing their supply chain cyber risk - **very effective**
- Targeted funding to help stimulate innovation and grow commercial offerings that support organisations with their supplier risk management (e.g. Government competitions, accelerator programmes) - **somewhat effective**
- Regulation to make procuring organisations more responsible for their supplier risk management - **not effective**
- Other (Please specify) - **templates for using with suppliers; standard information or risk assessment of the big tech suppliers**

Question 14 – 19 – Managed service providers

18. No comment

20. Are you responding as an individual or on behalf of an organisation?

- Individual
- **Organisation**

Question 21.[if individual] Which one of the following statements best describes you?

- Not relevant

Question 22. [if organisation] Which of the following statements best describes your organisation? (Select all that apply)

- A Managed Service Provider
- An organisation that uses Managed Service Providers
- An organisation that acts as a supplier
- An organisation that manages suppliers
- Organisation that employs, contracts or uses cyber security professionals
- Cyber security training provider and or certification/qualification provider
- A cyber security professional body
- Other form of cyber security professional organisation
- An academic or educational institution
- Organisation with an interest in cyber security
- **Non-cyber security specific professional body or trade organisation with an interest in cyber security**
- Other Free text

Question 23.[if organisation] Which one of the following best describes the sector of your organisation?

- Agriculture, forestry & fishing
- Production
- Construction
- Wholesale and retail; repair of motor vehicles
- Transport & Storage (inc. postal)
- Accommodation & food services
- Information & communication
- Finance & insurance
- Property
- **Professional, scientific & technical**
- Business administration & support services
- Public administration & defence
- Education
- Health
- Arts, entertainment, recreation
- Other services

Question 24.[if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.

- Under 10

ICAEW REPRESENTATION 62/21 CALL FOR VIEWS ON CYBER SECURITY IN SUPPLY CHAINS AND MANAGED SERVICE PROVIDERS

- 10–49
- 50–249
- **250–999**
- 1,000 or more

Question 25. [if organisation] What is the name of the organisation you are responding on behalf of?

- ICAEW

Question 26. Are you happy to be contacted to discuss your response and supporting evidence?

- Yes

Question 27. [If yes] Please provide a contact name and email address below.

- Kirstin Gillon, kirstin.gillon@icaew.com