Here is a link to the underlying documentation: Call for views on cyber security in supply chains and managed service providers

Questions below:

Call for views on cyber security in supply chains and managed service providers

1. **How much of a barrier do you think each of the following are to effective supplier cyber risk management?**

(a) **Low recognition of supplier risk**

- **Not a barrier**
- **[✓ Somewhat of a barrier]**
- **Severe barrier**
- **Don’t know**

(b) **Limited visibility into supply chains**

- **Not a barrier**
- **[✓ Somewhat of a barrier]**
- **Severe barrier**
- **Don’t know**

(c) **Insufficient expertise to evaluate supplier cyber risk**

- **Not a barrier**
- **Somewhat of a barrier**
- **[✓ Severe barrier]**
- **Don’t know**

(d) **Insufficient tools or assurance mechanisms to evaluate supplier cyber risk**

- **Not a barrier**
- **[✓ Somewhat of a barrier]**
- **Severe barrier**
- **Don’t know**

(e) **Limitations to taking action due to structural imbalance**

- **Not a barrier**
- **[✓ Somewhat of a barrier]**
- **Severe barrier**
- **Don’t know**

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

- **[✓ Yes]**
- **No**
- **Don’t know**

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

Many organisations lack the understanding, capability, and governance processes to assess and manage supply chain risk in connection with the use of Free and Open Source Software (FOSS) within supplier environments, as well as incorporation of FOSS as part of a solution delivered within the organisation's own environment. This is supported by evidence obtained during the preparation of OpenUK's report of March 2021, *"State of Open, The UK in 2021, Phase 1"*, where interviewees identified supply chain and compliance as key challenges in sourcing FOSS. An interview respondent further commented that *"providing companies with an open source compliance standard that they can trust will only help further drive open source adoption throughout the entire supply chain"*.

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

- **Yes**
- **[✓ No]**

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?**

(a) **Understanding the risks**

- **Not at all challenging**
- **Slightly challenging**
- **Very challenging**
- **[✓ Don't know]**

(b) **Establishing control**

- **Not at all challenging**
- **Slightly challenging**
- **Very challenging**
- **[✓ Don't know]**

(c) **Checking arrangements**

- **Not at all challenging**
- **Slightly challenging**
- **Very challenging**
- **[✓ Don't know]**

(d) **Continuing to improve, evolve and maintain security**

- **Not at all challenging**
- **Slightly challenging**
- **Very challenging**
- **[✓ Don't know]**

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

(a) Understanding the risks

(b) Establishing control

Guidance should include a focus on ensuring customers have considered whether their policies relating to open technologies should prevail, or those of the supplier. We have identified that only around half of businesses have policies and procedures in place, however we would recommend all businesses to put in place software policies (including open source), and would direct them to OpenChain (ISO 5230/2020) and SPDX as examples of helpful standards.

We are aware of some organisations with policies that do not allow updates and fixes on an 'as needed' basis, but instead impose an artificial timescale. This introduces vulnerabilities by not enabling zero-day issues to be resolved.

(c) Checking arrangements;

(d) Continuing to improve, evolve and maintain security

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

The open community has been working in this field for some time, and has substantial experience in using standards such as SPDX and the use of software bills of materials (SBOMs).

The NCSC's CAF (V3.0) acknowledges that there may be a need for some sector-specific aspects of the CAF. Open UK recommends that, in alignment with this principle, the NCSC incorporates sector-specific standards relevant to FOSS within the CAF and Cyber Essentials standards, as well as clarifying the application of the Supplier Assurance Questions as they apply to FOSS. Some examples of standards include:

- the Core Infrastructure Initiative (CII) Best Practices badge which focuses on criteria for FOSS projects; and
- OpenChain (ISO 5230/2020), which provides a framework for compliance programs within organizations that use FOSS from different projects in their solutions.

Open UK would welcome a collaboration with the NCSC to support appropriate consideration of FOSS within its standards.

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

- **Yes**
- **[✓ No]**

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?

- **[✓ Yes]**
- **No**
- **Don't know**

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

See question 7 above on the topic of aligning supply chain cyber risk management with FOSS risk management principles. In particular, a number of supplier assurance questions assume that a supplier’s supply chain will include only traditional organisations rather than the open source community.

11. How effective are the following commercial offerings for managing a supplier’s cyber risk?

(a) Private supplier assurance

- **Not effective**
- **Somewhat effective**
- **Very effective**
- **[✓ Don’t know]**

(b) Platforms for supporting supplier risk

- **Not effective**
- **Somewhat effective**
- **Very effective**
- **[✓ Don’t know]**

(c) Supply chain management system providers

- **Not effective**
- **Somewhat effective**
- **Very effective**
- **[✓ Don’t know]**

(d) Risk, supply chain and management consultancies

- **Not effective**
- **Somewhat effective**
- **Very effective**
- **[✓ Don’t know]**

(e) Suppliers of outsourced procurement services

- ● Not effective
- ● Somewhat effective
- ● Very effective
- ● [✓ Don’t know]

(f) Industry cyber security certification schemes

- ● Not effective
- ● Somewhat effective
- ● Very effective
- ● [✓ Don’t know]

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

13. How effective would the following government actions be in supporting and incentivising organisations to manage supply chain cyber risk?

(a) Awareness raising of the importance of supply chain cyber risk management through the use of campaigns and industry engagement

- ● Not effective
- ● Somewhat effective
- ● [✓ Very effective]
- ● Don’t know

(b) Additional support to help organisations to know what to do, such as:

(i) Improved or additional advice and guidance

- ● Not effective
- ● Somewhat effective
- ● [✓ Very effective]
- ● Don’t know

(ii) A tool that draws on existing advice and standards to help organisations manage supplier cyber risk

- ● Not effective
- ● Somewhat effective
- ● Very effective
- ● [✓ Don’t know]

(c) Providing a specific supplier risk management standard that:

(i) Outlines minimum and good practice and/ or

- ● Not effective
- ● Somewhat effective
- ● [✓ Very effective]

- **Don’t know**

(ii) Provides assurance that an organisation is managing their supply chain cyber risk

- **Not effective**
- **Somewhat effective**
- [✓ **Very effective**]
- **Don’t know**

(d) Targeted funding to help stimulate innovation and grow commercial offerings that support organisations with their supplier risk management (e.g. Government competitions, accelerator programmes)

- **Not effective**
- **Somewhat effective**
- [✓ **Very effective**]
- **Don’t know**

(e) Regulation to make procuring organisations more responsible for their supplier risk management.

- **Not effective**
- [✓ **Somewhat effective**]
- **Very effective**
- **Don’t know**

(f) Other (Please specify)

We believe that the Government could draw on the significant experience within the open community on managing supply chain cyber risk. We would be happy to work with the Government in establishing good practices in cyber risk management.

14. What additional benefits, vulnerabilities or cyber risks associated with Managed Service Providers would you outline?

Further clarity is required around the definition of ‘Managed Service Provider’, and in particular the distinctions to be drawn between single- and multi-product vendors and product types (such as enterprise grade products), where benefits, vulnerabilities, and risks may be different.

However, in the context of enterprise grade open source products/services, the benefits include expertise to ensure the supporting infrastructure is regularly updated for security patches, advanced threat monitoring is in place, alongside other common security controls and protections (network isolation, malware / CVE scanning etc).

The risks are that you as a tenant have no visibility into the security of the infrastructure on which the managed service runs (beyond trusting the experts above). For example, if a tenant runs their application within a virtual machine or a container upon a managed service, you cannot have full confidence that the underlying hypervisor, or container runtime is not compromised and cannot access or manipulate the tenants data. Further still , you cannot gain insight into the trust integrity of the firmware, bootloader , kernel etc of the host machine that runs the container runtime / hypervisor. The only way of a tenant being able to gain visibility into the integrity state of the host system within a managed service is access to a hardware root of trust measurement system via remote attestation. This is typically provided by a trusted platform module (TPM).

Open source leaders are able to provide a hardware attestation service for tenants in a managed service. This is via a project called Keylime now hosted under the CNCF (links below).

htps://keylime.dev
https://www.cncf.io/blog/2021/07/06/ibm-implements-remote-attestation-on-linux-with-a-hardware-root-of-trust-using-keylime/

15. Are there certain services or types of Managed Service Providers that are more critical or present greater risks to the UK's security and resilience?

We have observed that single-product vendors tend to introduce greater supply chain risk than multi-product vendors, which we believe may be due to the difference in longevity and stability of the business.

16. When considering the 14 Cyber Assessment Framework Principles, how applicable is each Principle to the cyber security and resilience considerations associated with Managed Service Providers? Please choose one of the following for each of the 14 Principles

- **Not applicable**
- **Somewhat applicable**
- **Completely applicable**
- **[✓ Don't know]**

Can you identify other objectives or principles that should be incorporated into a future Managed Service Provider security framework?

See question 7 above. In many cloud-based managed service environments, core infrastructure used in the Managed Service Provider's infrastructure will often include FOSS. Objectives/ principles should seek assurance in line with FOSS specific standards. In services where Dev-Ops support is provided where needed, organisations should establish their FOSS management principles (e.g. Openchain) and require that managed service providers align with these.

17. How effective would each of these options be in promoting uptake of a future framework for Managed Service Provider cyber security and resilience?

(a) Developing education and awareness campaigns

- **Not at all effective**
- **Somewhat effective**
- **[✓ Very effective]**
- **Don't know**

(b) Establishing a certification or assurance mark

- **Not at all effective**
- **[✓ Somewhat effective]**
- **Very effective**
- **Don’t know**

(c) Setting minimum requirements in public procurement

- **Not at all effective**
- **[✓ Somewhat effective]**
- **Very effective**
- **Don’t know**

(d) Developing new or updated legislation

- **Not at all effective**
- **[✓ Somewhat effective]**
- **Very effective**
- **Don’t know**

(e) Creating a set of targeted regulatory guidance to support critical national infrastructure sector regulators

- **Not at all effective**
- **Somewhat effective**
- **[✓ Very effective]**
- **Don’t know**

(f) Developing joined-up approaches internationally to managing Managed Service Provider security issues

- **Not at all effective**
- **Somewhat effective**
- **[✓ Very effective]**
- **Don’t know**

18. Please explain why you have provided the responses above and whether there are alternative ways the government could help address the cyber risks associated with Managed Service Providers?