# Mapping your supply chain

**How organisations can map their supply chain dependencies, so that risks in the supply chain can be better understood and managed.**

## Introduction

This guidance is aimed at medium to large organisations who need to gain confidence or assurance that mitigations are in place for vulnerabilities associated with working with suppliers.

Please read in conjunction with the NCSC's guidance on How to assess and gain confidence in your supply chain cyber security.

---

## What is supply chain mapping?

Supply chain mapping (SCM) is the process of recording, storing and using information gathered from suppliers who are involved in a company's supply chain. The goal is to have an up-to-date understanding of your network of suppliers, so that cyber risks can be managed more effectively, and due diligence carried out.

Many organisations rely upon suppliers to deliver products, systems, and services. Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it. This makes it difficult to know if you have enough protection across the entire supply chain.

> **Note**: SCM follows the principles of all good risk management; organisations need to understand the risks inherent in their supply chain, and then introduce security measures that are in proportion to the likelihood (and impact) of those risks materialising.

### Benefits of SCM

Understanding **who** your suppliers are, **what** they provide and **how** they provide will help you manage the cyber security risks that can arise. Mapping your supply chain allows you to make more informed business decisions based upon risk, specifically:

- better insight into the cyber security considerations that could be more easily enforced via contracts
- more prepared to respond to supply chain related cyber incidents
- the ability to establish repeatable methods so you have confidence in suppliers' security practices, and can build long term partnerships
- easier compliance with legal, regulatory and or contractual responsibilities
- regularly assessing the supply chain will reduce the likelihood of a cyber attack or breach

It is not possible to **completely** eradicate supply chain attacks. Should a risk materialise, being able to rapidly respond will limit the scope of damage to your organisation.

---

## What information should SCM contain?

Gathering information about your suppliers in a consistent manner and storing it in a centralised repository that's access controlled will ensure it's easier to analyse and maintain. This ultimately will allow you to better manage the risks, as you'll have a comprehensive view of the supply chain that is always up to date.

Typical information that may be of use includes:

- a full inventory of suppliers and their subcontractors, showing how they are connected to each other
- what product or service is being provided, by whom, and the importance of that asset to your organisation

- the information flows between your organisation and a supplier (including an understanding of the value of that information)
- assurance contacts within the supplying organisation
- information relating to the completeness of the last assessment, details of when the next assurance assessment is due, and any outstanding activities
- proof of any certifications required, such as Cyber Essentials, ISO certification, product certification

Acquiring this information, especially for large organisations with complex supply chains, can be a massive undertaking. The NCSC guidance on How to assess your supply chain cyber security will assist with this task, and can also ensure that supply chain dependencies from new suppliers is captured.

> Note: This information is an attractive target to attackers, so all SCM assets should be held in a secure repository with strong Security Architecture underpinning its design.

### Tools to map suppliers

Information about existing suppliers may already exist in your procurements systems. If there are multiple entry points for suppliers, relevant information will need to be aggregated. Depending on the size of your organisation, it might be beneficial to consider commercial tools which can:

- reconcile existing supply chain information
- help to keep information about supplier assurance up-to-date
- monitor supply chains beyond the initial tier, and identify concentration risk with contractors and sub-contractors
- make it easier to connect with, interact and visualise your supply chain

---

## Subcontractors in the supply chain

A vulnerability that exists anywhere within the supply chain, whether in your direct suppliers, or the suppliers that they sub-contract out to, could impact your organisation. For large organisations decisions around the practicality and

usefulness of understanding beyond the primary tier should be evaluated, and only the information on *direct* contractors should initially be captured.

How far down the supply chain do you need to go? What exactly has been subcontracted, and what is its criticality (taking into consideration the organisation's risk criteria) ? These questions require some upfront consideration of the need to obtain information vs the cost of acquiring it. You should:

- determine the criticality of the technology, systems and services you use
- consider how much effort you are prepared to put into establishing the whole supply chain
- build into the contract terms with your primary suppliers to provide visibility cascading down their supply chains
- reassure suppliers how this information is to be used and who will have access to it, as suppliers may be cautious about sharing commercially sensitive information
- use this shared information to understand key shared suppliers that your immediate tier one suppliers are using, highlighting a concentration risk
- ensure you consider data supply chains as well (that is, your products may use data from third parties, or even rely upon data from others)

## Contract terms for suppliers and subcontractors

The following terms should be considered for contracts with suppliers and subcontractors:

- incident management response and notification time frames for responding to a breach (along with provision of support to the organisation to find the root cause)
- ability to audit suppliers/subcontractors (and expected frequency of audits)
- data management (only necessary data may be transferred out of the organisational network)
- data integrity (is data protected via authentication and encryption, will data be segregated if held on a supplier platform?)

- management controls for suppliers' access to physical sites, information systems and intellectual property (including the process for ensuring this is kept up to date)
- any requirements that your direct suppliers should be demanding from *their* supply chain (as described above)

---

## Getting started

Your approach will depend upon your organisation's procurement and risk management processes, and the tooling that you have available to you. The following is a top-level set of priorities for organisations approaching SCM for the first time.

1. Use existing stores, such as procurement systems, to build a list of known suppliers. Prioritise suppliers, systems, products and services that are critical to your organisation.
2. Decide what information would be useful to capture about your supply chain.
3. Understand how you will store the information securely and manage access to it.
4. Establish whether you want to collect information about your suppliers' subcontractors, how far down the chain is useful to go.

- Consider using additional services which evaluate your suppliers and provide supplementary information about their cyber risk profile.
- For new suppliers, state upfront within your procurement process what you expect your suppliers to provide.
- For existing suppliers, inform them what information you want to capture about them and why, and retrofit information collected from existing suppliers into a centralised repository.

5. Update standard contract clauses to ensure the information required is provided as standard when initiating working with a supplier.

6. Define who is best placed in your organisation to use this information; this might include procurement, business owners, cyber security and operational security teams. Make them aware of the information store and provide access.
7. Consider creating a playbook to deal with situations where an incident occurs and you may need to co-ordinate effort across both the extended supply chain, and third parties such as law enforcement, regulators and even customers. A useful Supply Chain scenario can be found in the NCSC Exercise in a box service.
8. Finally, document the steps that will need to change within your procurement process as a result of supply chain mapping. For example, you may need to consider excluding suppliers who cannot satisfactorily demonstrate that they meet your minimum cyber security needs.

**PUBLISHED**

16 February 2023

**REVIEWED**

12 October 2023

**VERSION**

1.1

**WRITTEN FOR**

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

Self employed & sole traders