

Part of [Objective A - Managing risk](#)

## Principle: A4 Supply chain

[← Previous Chapter](#)

[Principle: A3 Asset management](#)

**Current Chapter**

Current chapter – Principle: A4 Supply chain

[View all](#)

### A4.a Supply chain

“The organisation understands and manages security and IG risks to information, systems and networks supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.”

#### Overview

This contributing outcome is about ensuring your organisation has factored cyber security and information governance (IG) considerations into your approach to working with suppliers.

# Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the [mapping exercise](#) published by NHS England and Department of Health and Social Care (DHSC).

## Supply chain

It is your responsibility to understand the risks posed to the operation of your essential function by your supply chain, and to put appropriate controls in place to mitigate those risks.

As part of your [scoping exercise](#), you should have identified the information, systems and networks supporting your essential functions which are administered by, require the involvement of, or may be affected by suppliers. From here, you can work to understand what controls you need in place to ensure the security of those supplier systems and networks.

### Contracts

**(This is an increase in requirements for 2024-25 'Standards met')**

Reviewing contracts with third parties and identifying those with data security contract clauses in place was a non-mandatory requirement in the 23-24 DSPT.

Under the CAF-aligned DSPT framework, it's now necessary to conduct a review and ensure that appropriate security and data protection obligations are included in relevant contracts. As part of your review, you should consider all suppliers providing services or systems involved in the operation of your essential functions and all suppliers with access to confidential patient information.

There may be suppliers whose services would not impact the operation of your essential functions if compromised for a short period of time, such as HR systems. It may still be worth factoring these suppliers into your review from a time-bound perspective in case of prolonged disruptions.

## Cyber security obligations

You should determine which cyber security obligations you include in supplier contracts based on the service being provided, and the risk to your essential functions if the supplier were to become compromised by an incident.

Examples of cyber security obligations to consider are:

- **right to audit** – the right to conduct audits of the supplier's infrastructure, systems, services and premises with appropriate notification or in case of an incident

- **incident management** – the requirement for suppliers to inform your organisation of ongoing incidents and any impacts to your organisation
- **assurance** – the requirement for the supplier to provide appropriate assurance evidence at the commencement of the contract and regularly throughout the lifetime of the contract (the specific requirements around this will vary depending upon system and data sensitivity)
- **service level agreements (SLAs)** – these should also include security service levels covering out of hours support and reporting, handling and remediation of incidents
- **vulnerability management** – the requirement for the supplier to keep the system, service or software patched and on up-to-date operating systems
- **security governance** – the expectations of the organisation around security governance within the supplier including security risk management and signing off residual risks

Organisations are responsible for seeking their own legal advice and ensuring any contracts they sign are fit for purpose.

## Data protection obligations

Any contracts or agreements with suppliers must have the appropriate clauses in place to cover the requirements of data protection legislation. If you're using a contract that does not have a section on data protection, you must also have a data processing agreement. See the [ICO's guidance on contracts](#) for more information on data protection requirements.

The NHS [universal data sharing and processing agreement \(DSPA\) template](#) contains all of the necessary clauses needed to comply with UK GDPR and the Common Law Duty of Confidentiality. The [NHS standard contract](#) also covers relevant UK GDPR requirements.

Organisations are responsible for seeking their own legal advice and ensuring any contracts they sign are fit for purpose.

(These are an increase in requirements for 2024-25 'Standards met')

### Supplier assurance

Under the CAF-aligned DSPT framework, you should obtain assurance that all third-party connections to your network meet your security and IG requirements, and that any information you share with suppliers for the delivery of healthcare services is appropriately protected.

This will require engagement with your supply chain. In cases where you encounter obstacles to retrieving the information you need, these should be flagged in your DSPT response along with any mitigating actions you have taken.

### Incidents arising in your supply chain

Under the CAF-aligned DSPT framework, you should consider data security and protection incidents that might arise in your supply chain. This consideration of supply chain incidents may be reflected in a number of documents, including your due diligence processes, your incident response plans, and the contracts and agreements you have in place with suppliers.

Any supplier incidents or near misses that have a data security or data protection implication should be recorded.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- overview of contractual agreements in place
- supplier contracts
- current data sharing agreements
- current data processing agreements
- policy, process, procedure or strategy documents (such as third-party contracts, procurement)
- incident response plans
- supplier's due diligence and assurance procedures
- supplier's contracts database for services and products

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

**Indicator of good practice**

PA#1

You understand the general risks suppliers may pose to your essential function(s).

**Term**

'essential function(s)'

**Interpretation** Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions.

For more information, see [guidance on scoping essential functions](#).

**Indicator of good practice**

PA#3

You understand which contracts are relevant and you include appropriate security and data protection obligations in relevant contracts.

**Term**

'relevant contracts'

**Interpretation**

This applies to all contracts you have that may have a cyber security or data protection impact.

This will include, for example, catering services if they handle personal data that includes patient names and dietary requirements, and any supplier whose service includes an IT component.

**Indicator of good practice**

PA#7

All international data transfers to suppliers are covered by a legal protection.

**Term**

'legal protection'

**Interpretation**

You must be aware of all countries where data is being processed as part of any supplier-offered service. This should be documented in your information assets and flows register (see [A3.a Asset management](#) and [B3.a Understanding data](#)).

Where data is being processed by suppliers located in countries with no adequacy regulations, you must have an [International Data Transfer Agreement](#) in place. You can reference the International Data Transfer Agreement (IDTA) documents within other agreements (such as the [NHS Data Sharing and Processing Agreement \(DSPA\)](#) or [NHS standard terms and conditions for the procurement of non-clinical goods and services](#)) if needed.

## Additional guidance

For additional guidance, see:

[National Cyber Security Centre CAF guidance | A4 Supply chain](#)

[National Cyber Security Centre | Supply chain](#)

[Information Commissioner's Office | Contracts and data sharing](#)

## Mapping to other cyber frameworks

NHS England and DHSC have produced a [mapping document](#) showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

---

Last edited: 29 August 2024 9:43 am

[← Previous Chapter](#)

[Principle: A3 Asset management](#)

---

## Chapters

1. [Objective A - Managing risk](#)
2. [Principle: A1 Governance](#)
3. [Principle: A2 Risk management](#)
4. [Principle: A3 Asset management](#)
5. **[Principle: A4 Supply chain](#)**

## Legal

[Privacy and cookies](#)

[Terms and conditions](#)

[Looking after your data](#)

[Freedom of information](#)

[Modern Slavery Act Statement](#)

[Accessibility](#)

[Change cookie settings](#)

[Copyright \(c\) NHS Digital](#)

## Get in touch


[Contact us](#)

[Press office](#)

[Tell us what you think of our website](#)

[RSS feeds](#)

## Follow us on social media

 [Twitter](#)

 [Facebook](#)

 [LinkedIn](#)

