

## **Data Security and Protection Toolkit (DSPT)**

### **Frequently Asked Questions – Aligning the Cyber Assessment Framework (CAF) to the DSPT 2024 - 2025**

#### **Which organisations move to CAF based DSPT in summer 2024?**

- NHS trusts and foundation trusts
- Integrated care boards (ICBs)
- Arm's length bodies (ALBs) of the Department of Health and Social Care
- Commissioning support units (CSUs) within NHS England

#### **When will independent providers designated as Operators of Essential Services and key IT suppliers move to CAF based DSPT?**

They will remain with the existing DSPT until summer 2025.

#### **Which organisations are categorised as 'Independent providers designated as Operators of Essential Services' and 'Key IT Suppliers'?**

A small number of independent providers have been designated as 'operators of essential services' under the Network and Information Systems (NIS) regulations. These providers have been notified of their status by the Department of Health and Social Care (DHSC).

The larger IT suppliers with more than 50 staff and an annual turnover of £10million or more will be in scope for the changes to their DPST in summer 2025.

#### **Will 'other' organisations move to CAF aligned DSPT?**

A checklist approach mapped to CAF will be developed and implemented Summer 2026, however this is still subject to review.

#### **Why does DSPT CAF look different from NCSC's?**

NHS England (NHSE) and DHSC have enhanced NCSC's existing cyber framework with a health and care CAF overlay which covers data protection, confidentiality, and other information governance disciplines such as clinical coding.

#### **Has the National Data Guardian (NDG) had any input into DSPT being aligned with CAF?**

Yes, NDG have provided input and review of the standard and guidance.

#### **Will there be a focus on IG and cyber security with the CAF aligned DSPT?**

Yes, cyber security and Information Governance are being treated as two sides of the same discipline. The goal of the health and care CAF overlay is to ensure a joined-up approach to cyber security and IG in health and care, preventing gaps and minimising unnecessary duplication between disciplines.

#### **Why is there an objective E ?**

As part of the Health and Care overlay, objective E was added to ensure appropriate outcomes were included to cover 'Using and sharing information appropriately'.

### **What are 'indicators of good practice'?**

**Indicators of Good Practice** are examples of procedures and processes which help inform your organisation's decision about whether it has achieved a contributing outcome

### **What type of responses will be needed for each outcome?**

The DSPT interface will require a supporting statement, your supporting statement should justify your decision for categorising yourself as 'Not achieved', 'Partially achieved' or 'Achieved'. It should be written simply and concisely so that your senior board members, external auditors, NHS England or DHSC can understand your rationale. It will encourage NHS Trusts, ALBs, CSUs and ICBs to provide additional evidence (Upload a file, reference a previously uploaded document, specify an intranet/internet link, enter a text description or document location) before they can confirm (save as complete) they have met the achievement level of an outcome. In addition, for a small number of outcomes there will be the requirement to provide a numeric value or Y/N response.

### **How will I know I have met the standard expected?**

Standards met is defined for each outcome which indicates the expected achievement levels.

### **Will there be an increase in the level for standards to be met in 2024/25?**

The level of standard for cyber security and IG controls have remained at a comparable level to the levels set for DSPT 2023/24, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation. Where this is the case, this is clearly highlighted in the guidance.

### **What if we do not meet the standard set?**

Standards not met for NHS Trusts, ALBs, CSUs and ICBs is the confirmation of less than the expected achievement levels for one or more outcomes of the 2024-25 DSPT, an improvement plan will be needed for any outcomes with responses which do not meet the expected achievement level.

### **Will an improvement plan be required?**

Yes, it is expected that an improvement plan will be submitted at the end of 2024/25 DSPT year for those organisations who are 'standards not met'.

### **Does the CAF toolkit make allowances for organisations that are certified to Cyber Essentials+ , ISO 27001 or DCB1596?**

There won't be a direct exemption for certain controls that we know are included in CE+ or ISO27001 certifications as there has been up until now. We are working on some mappings from the CAF based DSPT through to ISO27001, to allow organisations to show they are completing the indicators of good practice. In the DSPT we will be asking for a response at the outcome level rather than the indicator of good practice level, so there will still be a need for organisations to assess and determine if they are meeting the outcome overall.

We will share some supporting statements and examples as part of the new guidance.

**When you say the DSPT will align to CAF but not change mid year, how will it deal with changes to the CAF?**

The CAF is published and maintained by the NCSC (National Cyber Security Centre) and we are not anticipating any mid-year changes for 2024-2025. Once the DSPT framework is published, it becomes an information standard. The standard does allow for an emergency change process, if something specific is updated in the CAF, so we do have the ability to do that. We are however mindful of the need to have a stable set of requirements and any mid-year changes or additions would only be done in exceptional circumstances.

**Will standards exceeded be recorded as part of the CAF DSPT?**

No this is not available to NHS Trusts, ALBs, CSUs and ICBs in 24-25 DSPT. We will consider this again for 2025-26 DSPT.

**Who is expected to sign off DSPT?**

It is expected that the Senior Information Risk Owner (SIRO) will take responsibility for the annual sign off prior to submission.

**Baseline / Interim Assessment for large NHS organisations**

**When will NHS Trusts, ALBs and ICBs need to complete their baseline interim assessment?**

The interim assessment for the 2024-25 DSPT will need to be submitted by 31<sup>st</sup> December 2024. These are the only organisations who need to complete a baseline assessment this year.

**Is the new date for the interim baseline assessment a permanent move?**

As it is a year of change for the DSPT, we want to get results back earlier this year so we can spot any trends or areas where organisations need more help and support. Leaving the interim assessment until closer to the deadline gives less time to deliver this help and support. The timing will be reviewed for 2025-26 and we would be happy to take views on this.

**Have the impacted organisations been consulted on the date being moved to December for the interim assessment?**

No not formally. The date has been brought forward, to make sure teams have started their thinking earlier. Organisations should have a view of where they think they are by the end of December. By completing this gap analysis in December 2024, it allows a full 6 months to work on those areas.

**Is the baseline submission still only for reassurance that we are working on it - i.e. no one is assessing what has been submitted**

A baseline is not a full assessment of your toolkit submission. It is an interim assessment to indicate that your self-assessment is under way. It may also highlight to your organisation, areas which need particular focus ahead of the full assessment deadline.

The baseline assessment is not formally assessed by NHS England, but it allows NHS England Cyber Operations Team to review interim responses to evidence items and determine whether further guidance is required. In previous years we have

undertaken additional webinars on Penetration testing and unsupported software based on reviews of interim assessments.

### **DSPT incident reporting function**

#### **Is anything changing with the incident reporting function for those organisations moving to the CAF aligned DSPT?**

The incident reporting still works in the same way, nothing has changed with this function.

#### **Has a role been created in DSPT for staff who need to report incidents but should not touch the DSPT submission?**

This is something we will look at in future development work.