NHS
England

Frequently Asked Questions – CAF aligned DSPT 2024 – 2025

General toolkit questions

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 the output of our exercise scoping our information, systems and networks supporting our “essential functions” need to be submitted as part of our DSPT assessment?

The document which you produce scoping your information, systems and networks supporting your “essential functions” will not need to be submitted as part of your DSPT assessment. This will be an important document to maintain and continuously update internally. However, your DSPT auditors, NHS England and the Department of Health and Social Care may ask to review, provide input and where necessary, challenge scoping assessments.

Will there be an essential functions assessment document template issued?

This is not currently planned, however the guidance relating to scoping essential functions can be accessed here: Scoping essential functions - NHS England Digital

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.

What organisations are categorised as ‘other’?

- Dentist
- General Practice (GP)
- Local Authority
- Optician

- Other (including charities and NHS business partners)
- Pharmacy
- Social care
- University (including researcher / department / secondary use)

Will Clinical Trials Unit's be part of Category 3?

Clinical Trials Unit would fall under University (including researcher / department / secondary use) which is Category 3.

Will private providers with charitable status also be Category 3?

Private providers with charitable status would fall under Other (including charities and NHS business partners)

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. We have also published a joint NHSE/NDG statement which can be accessed here: CAF-aligned DSPT: Evolution of our assurance model - Information governance - NHS Transformation Directorate (england.nhs.uk)

Will there be a focus on information governance (IG) and cyber security with the CAF aligned DSPT?

Yes, cyber security and IG 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

How will I know I have met the standard expected?

"Standards met" is defined for each outcome which indicates the expected achievement levels. The profile indicates the standard to be met for each outcome and it is indicated on screen on the outcome page.

Do we have to achieve all indicators of practice for not achieved before we can move to partially achieved and then to achieved?
To decide your achievement level, you should read the indicators of good practice under each contributing outcome and decide whether your organisation’s practices reflect them.

To be ‘Partially achieved’ or ‘Achieved’ on the contributing outcome, your organisation’s practices and behaviours should be aligned with all indicators of good practice underneath the ‘Partially achieved’ or ‘Achieved’ columns. If your practices are not aligned with one of the indicators of good practice, you must select ‘Not achieved’ for that contributing outcome, unless you can justify that you have achieved the outcome by different means.

How can 'partially achieved' be 'standards met'? Some standards may never be 'fully met'.
The standards to be met are a combination of ‘not achieved’, ‘partially achieved’ and ‘standards met’ which are set annually against each outcome. For 24/25 the profile of standards to be met has been baselined against the achievement levels for 23/24 with a small number of increased achievements. There are some contributing outcomes where the expected level of achievement for ‘standards met’ is ‘not achieved’. For these contributing outcomes, you are still required to assess your organisation’s achievement level and provide a response, showing you have considered the implications for your organisation’s cyber security and IG activities. The DSPT ‘standards met’ expectation should be regarded as a minimum compliance level, not the end goal of your organisation’s cyber security and IG activities.

If you have confirmed that none of the items in 'not achieved' apply to you, but you aren't able to 'tick' all the 'partially achieved' elements, what position do you end up in?
You would be ‘Not Achieved’ for that particular outcome, with actions to work on to get to ‘Partially Achieved’.

Why is there no ‘partially achieved’ for some of the outcomes?
There are some outcomes which do not work well with having a mid-point of partially achieved. For example, detecting malicious activity.

Will it be clear what evidence is acceptable to meet the outcome level?
For each contributing outcome, a suggested list of evidence items is provided which you can use to help you demonstrate your achievement of the associated requirements. The move to the CAF-aligned DSPT places a bigger emphasis on good decision-making guided by expert judgment at the local level. You will need to make an informed judgment, using the guidance provided by NHS England, to determine whether you have met the outcome and justify your decision to auditors.

Do you have to include all the items listed under the "Supporting evidence" section when submitting evidence?
No - the list is to give you an indication of the kinds of documents you hold locally which would help you evidence your achievement of the outcome. It is up to you

which ones accomplish the task, and to provide a supporting statement to back up your response.

For areas that are expected to be 'not achieved' this year, would we still be expected to submit evidence to show that we are working towards 'partially achieved'?
Yes - you should be aiming for the higher level of achievement and show that you are working towards it.

What are the expectations on the breadth of accepted evidence across the different organisations in the first tranche, noting the differences in scale and scope.
We aim to be helpful wherever we can, and if you have a specific question around providing evidence against a particular outcome, you can discuss that directly with us via your Regional Security Leads, the IG policy engagement team or the DSPT support inbox. The goal of the pure CAF produced by NCSC is a move towards organisations' decisions being guided by expert judgment, and the CAF-aligned DSPT fundamentally mirrors this.

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 'standards met'?
'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.

Some of our data flows depend on "Standards Met" and also our supply of some services - how will the new "partially achieved" status affect these dynamics?
Those organisations meeting the CAF profile will have the equivalent of standards met status and show as Standards met on the DSPT organisation search once published.

Will there be mandatory and non-mandatory items?
No, each contributing outcome requires you to write a supporting statement and upload, reference or provide a link to relevant documents which justifies your decision to categorise your organisation as 'Not achieved', 'Partially achieved' or 'Achieved', in a way which should be understandable to other members of your team, external auditors, NHS England and DHSC.

Will an improvement plan be required for organisations who are 'standards not met'?
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'.

How will actions plans be completed for 24-25?
Details on Improvement plans for 23-24 DSPT Toolkits including when updates are required, what happens if organisations do not complete them can be found at: https://www.dsptoolkit.nhs.uk/News/improvement-plans-2023-2024.

It is planned that there will be an improvement plan process for 24-25. Details will be published closer to the DSPT deadline.

How are we going to be rated if work is in progress over a 5 year period?
You will update the supporting statement each year with your progress of the improvement. This will produce a DSPT Status for each year, as currently.

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.

The guidance on supporting statements can be accessed here: How to approach it - NHS England Digital

Information Standard DAPB0086: Data Security and Protection Toolkit - will this change or stay the same standard number?
The standards number will not change.

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 the 2024-25 DSPT. We will consider this again for 2025-26 DSPT.

Who is expected to sign off the DSPT?
The Senior Information Risk Owner (SIRO) is responsible for signing off the DSPT prior to submission.

Will NHS Trust organisations who have GP practices under their umbrella, have to complete two versions of DSPT?

This depends on the scope and how the GP practices have been incorporated into the NHS Trust. If the Trust is 'hosting' the GP practices, and they are run as a stand-alone practices and separate organisations, they will need to complete separate toolkit submissions.

Will there be support, to ratify what is 'in scope' for what constitutes those essential systems to ensure the lists respondents created are appropriate?

A guidance document covering scoping is available at:
Scoping essential functions - NHS England Digital

This was covered in the DSPT Webinar on ‘using and sharing information appropriately’, the recordings are available at: News (dsptoolkit.nhs.uk)

Where can I access the CAF-aligned DSPT guidance?

Guidance to support the specific group of organisations moving to CAF-aligned DSPT is available here: Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT) guidance - NHS England Digital

Will the mappings from V6 to CAF DSPT (V7) be made available?

Yes, this information is available on the DSPT news page under ‘supporting information’: News (dsptoolkit.nhs.uk)

How many outcomes are there in total, and what is the proportional split between data protection outcomes and cyber security outcomes?

There are 47 outcomes in total. 19 can be regarded as primarily cyber-oriented and 8 can be regarded as primarily IG-oriented. However, the majority of the outcomes have no clear delineation by discipline. Your organisation’s cyber security and IG teams are responsible for reading through the CAF-aligned DSPT and deciding how to most suitably allocate ownership of each contributing outcome. Where outcomes are shared, you will need responsible teams to collaborate to complete the submission.

Can we use the previous IT Health Check (ITHC), if budget is restricted?

The IT Health check would support some of the outcomes but it would not meet the requirement for DSPT Audit.

Should a training analysis be in a report form or is there a form this should be documented as?

We do not specify a particular format for the Training Needs Analysis. We have produced a specimen TNA which is available through the guidance or at https://www.dsptoolkit.nhs.uk/News/Attachment/726

How will you deal with inconsistencies in how organisations are completing the CAF-style DSPT (flexibly with a move away from prescription) and how auditors are approaching the audit as it seems the audit guidance will still have prescriptive elements to it?

NHSE are working with a supplier to develop a CAF aligned audit framework to ensure there is alignment with completion of the assessment and the audit process.

Is there a definition of 'up to date'? Within last year, six months, month?

It will be the responsibility of organisations to determine what is ‘up to date’. There may be specific events such as changes in regulations, organisational change or emerging issues which may require updates to be made more frequently for some organisations.

Our policies have a 3 year review. Are you suggesting that we need to review them this year even though they are not scheduled for review?

It is up to your organisation to make a risk-based decision on the frequency of your policy reviews. The important thing is that you can justify your intervals to auditors and to NHSE / DHSC.

Where can I access the recordings and slides from the webinars?

All the recordings and slides from the CAF-aligned DSPT webinars can be accessed here: News (dsptoolkit.nhs.uk)

Baseline / Interim Assessment for 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 31st 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 areas in the toolkit are being worked on and not a full assessment?

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

If the Baseline expectation is partially achieved does this mean organisations must have partial achievement by a baseline date or by the final submission date, or must have achieved by submission date?
By baseline expectation we mean the minimum that is required at the final publication in June 2025.

Will it be possible to see the profile of standards met for years 2 to 5?
This is something the Joint Cyber Unit is working on and will be shared when complete.

Does the CAF-aligned DSPT include response plans of the clinical services or only the IT services?
The CAF-aligned DSPT response plan requirement is based around the recovery of the operation of essential functions which rely on information, systems and networks, which equates to whatever an organisation needs in order to provide its essential service. If the essential service is providing healthcare to patients (as will be the case with trusts and foundation trusts), under the CAF-aligned DSPT the organisation's response plan would need to cover how they would continue providing healthcare to patients in the event of an incident impacting information, systems and networks relied upon to provide healthcare. Clinical services would definitely need to be considered as part of the plan, as well as processes underpinning them such as communications between staff members and access to clinical health data.

In the CAF to DSPT mapping document, the way that DSPT assertions link to the CAF-aligned outcomes is quite broad. Could this be made more specific to particular indicators of good practice?
There is no one-to-one correlation between the requirements of the legacy DSPT and the requirements of the CAF. The CAF brings a completely new approach to assurance. For this reason, it is not possible to map specific indicators of good practice within the CAF-aligned DSPT to specific legacy DSPT assertions.

Top three risks will be a snapshot in time, do we only update just before submission?
You might find it helpful to record your top three risks when you start to complete your assessment, amending and updating with a final review before submission.

Has pass / fail submission been removed and are we moving back to a % achieved type of scoring?
No, organisations will be either ‘standard met’ or ‘standard not met’

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.

Will the incident reporting function notify NCSC?
This is done manually on behalf of the organisation, the NHSE Cyber Security Operations Centre pass the information to NCSC.

Audits

Will NHS Trusts, ALBs, CSU and ICBs have a requirement to undertake a prescribed DSPT Audit?
There remains a requirement to undertake an independent audit and a new CAF aligned audit framework is being developed to incorporate the indicators of good practice and an independent assessors guide will be made available. The audit guidance will be updated and the process will be tested with a small number of organisations in the first instance.

We are also working with other sectors who have implemented audit frameworks for CAF based regimes.

Will organisations still need to Audit the interim submission?
There is no requirement to audit the interim submission, and there has never previously been a requirement to audit the interim submission.

Will the auditor's timelines change with the interim assessment being brought forward to December?
There will be no changes to the auditor timelines.

Will the independent assessment undertaken by auditors cover all principles or just a sample as per previous years?
This will be confirmed in due course.

When can we get hold of the Independent Assessment and Audit Guide for the CAF DSPT?
There have been some delays which have been incurred which have been out of the control of NHS England. Timelines and more information will be shared shortly.

Will the DSPT audit process be required for independent providers designated as Operators of Essential Services and key IT Suppliers for 24/25?
Yes it will. DSPT Audit will be a mandatory requirement for independent providers designated as Operators of Essential Services and key IT Suppliers for 24/25.

Details are available on the DSPT website https://www.dsptoolkit.nhs.uk/News/auditnews.

Will the audit guidance properly align with the new CAF DSPT?
A new CAF audit framework is being developed to incorporate the indicators of good practice and an independent assessors guide will be made available.

Resourcing and Funding

Will there be funding for the GAP analysis?
No, there will be no funding for the gap analysis.

Has an analysis taken place to assess the time needed to complete the assessment? Does CAF require more, the same or less effort than the previously?
In the immediate / short term, there will be more effort required, however in the longer term there will be greater clarity on the profiles and a better understanding of future requirements. Once teams have understood the new CAF based requirements, plans can be developed to take you forward for the next 1-2 years. As we raise the bar for protections, that may require additional capability within organisations. Through the Cyber Improvement Programme, we are looking at what central support needs to be in place to help organisations reach the endpoint.

Will there be extra funding for resources to support the completion of the assessment?
No there will not be any extra funding to support the completion of the assessment.
In most cases, this should not mean making significant changes to your local cyber security and IG procedures. However, the new toolkit requires you to think differently about what your approach to people, processes and technology achieves in terms of increasing your organisation's cyber and IG resilience.

After the interim submission will there be scope for organisations to have "supported" conversations with their senior leaders to ensure the best outcomes are achieved. A lot of this may require funding to achieve and some of this may need to be brought forward within current strategies and bringing funding forward could be a challenge without support.

Yes, we would encourage you to have a discussion with your Regional Security Lead in the first instance.

Will there be funding for to support areas of improvement which are contributing to standards not being met?
This will depend on what areas of improvement are required. There are already a range of centrally funded cyber security services which NHS organisations can access and your Regional Security Lead will be able to advise on what additional support can be put in place.

Platform / toolkit security and functionality
Will the answers from Version 6 of the toolkit be populated to their respective outcomes in Version 7 of the toolkit? Unfortunately not, due to the approach of the new framework. However, you will still be able to access the information you have submitted for V6.
What security protections are incorporated into the toolkit to ensure that the data we are entering is safe and secure? NHSE Risk assessment is carried out based on the information that is held within the DSPT, that determines the security controls which needs to be in place for the system. There is a legal direction for the toolkit, which outlines the legal basis for holding the data as directed by the Secretary of State for Health and Care.
As part of the final submission will it allow any number of submissions as the DSPT 23/24? Yes, this feature is still supported in CAF DSPT.
Does DSPT support MFA? Yes it does, see support article at https://www.dsptoolkit.nhs.uk/News/27 to find out how to move your DSPT account to MFA.
When assigning owners, is a change control available for each item? Will I be able to look at a draft response and see if, when and who updated it last so I can keep a general oversight? At the moment, the last change is viewable so there isn't a full audit trail displayed in the frontend. This has been explored as part of user research which found that this can get complicated very quickly where there are hundreds of changes being made. This is an area we will keep under review, to help support toolkit users.
Will system generated alerts be possible, to inform you when an objective has been updated by a contributor? This is not currently a feature of the DSPT, but may be considered for future development work.
Can DSPT be used as our primary recording mechanism and download the information to a spreadsheet/document to work from and use as an action plan? Yes, there will be an ability to download your assessment via the reporting function. There will be a limited amount of functionality on day one, then will build on it over time and develop this through our user research.
When saved as complete can you reopen and add? Yes, you are able to reopen a completed outcome to amend/update the response.
Can password memory be applied to DSPT? This is browser dependent, DSPT does not support saved password.
Do you have to assign an owner to each outcome? No this is optional and can be used to help manage who is taking the lead on the response.

Can I assign more than one owner to each outcome?
No, the development only allows one owner per outcome.

Will clinical coding be marked as not applicable for ICB's?
Clinical coding outcomes will only be seen by those organisations who will need to respond to the outcome.

Will the file size upload be increased as DSPT struggles with some documents?
There are ways of reducing the file size such as converting to PDF. We will keep this area under review.

There is a lot of repeated evidence collection required, does this impact the resources and storage?
The lists of evidence items are indicative, not definitive. You would not need to upload every item from the list. You would use your own expert judgment to choose the ones you feel are sufficient to justify your achievement of the outcome, and explain your rationale.

You are also able 'Reference a previously uploaded document' function on the outcome page. Scroll past the 'Upload a document' section.

Will CAF DSPT have the functionality to hyperlink documents?
CAF DSPT collects responses at Outcome level. Each outcome has a section asking for a supporting statement and that allows you to upload documents, provide a text or to include a link (URL) to a document. This would allow you to hyperlink to an external document.
In the supporting statement you can include the text of a link, but the text box will not resolve this into a hyperlink. The link could be copied and pasted into a browser but would not clickable. The input into the supporting statement box only accepts text input.

Will Category 1 organisations be able to share evidence items with other organisations for shared services? Or will the evidence have to be provided multiple times?
An organisation controls who has access to their DSPT assessment and to what level. If an organisation added other people in a shared service as a user of its DSPT, the IT shared service person could provide detail into an outcome in the DSPT assessment.

If the shared service person had access to multiple other organisations DSPTs the shared service person could provide evidence for multiple other organisations. The access for this would have to be provided by each individual organisation each individual person at the shared service so they could fully control who had access to their DSPT

Where the same evidence such as asset registers are needed across multiple outcomes, will you still be able to upload once and link to all?
Yes there will be the feature to support uploading evidence one and linking to more than one outcome.

Will there be a report which can be used in excel to use as an action plan?
Reporting is the next phase of development; more information will be shared shortly.

Local Authorities and Adult Social Care

When will Local Authorities move to CAF assessments?
Is there any communication between NHS and Department of Levelling Up to ensure that the profile for local government meets the requirements of both?

For Local Authorities, there will be only be incremental changes made to the toolkit which they currently complete until at least summer 2026. For LAs, we work closely with the Department of Levelling Up, who are also implementing CAF for local government. We have shared the health and care overlay with the Department of Levelling Up, and are in conversation with them about the options for Local Authorities that gives us the required level of assurance whilst reducing the need for duplication of effort.

Will CAF DSPT changes 24/25 apply to those LA who deliver services such as health visiting and school nursing?
No not in 24-25. We will be reviewing the questions asked of Local Authorities in the future to align them to the CAF and the current plan is to complete this for the 2026-2027 DSPT.

Supply chain

Will suppliers be evaluated based on the same baseline for NHS organisations? For example, are they going to be measured only at standards met for the next year?
For 23-24 large IT suppliers used the same question set as NHS Trusts, CSUs, ALBs and ICBs.
For 24-25 there are no ‘IT suppliers’ that will see the CAF-aligned DSPT. The threshold they are required to meet is about the nature of their organisation, which defines whether they see a more comprehensive list of questions (equivalent to 23-24 ‘Category 1’) or less (equivalent to 23-24 ‘Category 3’), whatever those categories end up being called for 24-25 or beyond.

As Accenture and IBM are under national contracts, and have more access to PII than other NHS providers, will they be required to submit a CAT1 Toolkit and will we have visibility of that to assure ourselves of those elements of the supply chain? Or do we need to seek assurance from NHSE as the primary contractor?
For NHS Trusts, CSUs, ALBs and ICBs in the 24-25 DSPT the supply chain is anything that impacts the delivery of the essential service. A PPE or catering supplier would be included if it impacted the delivery of the essential service. Specific guidance on scoping of essential functions is available below, this will help to identify which services, networks and information need to be included in the scope of the DSPT return:
Scoping essential functions - NHS England Digital

Is uploading evidence mandatory for IT Suppliers?
For 24-25 a response is required against all the evidence items. Some ask for text responses, some for dates and some ask for a document to be uploaded.

Is it likely that Category 3 organisations who currently don't fit the large IT supplier criteria organisational profile/requirements will be revised if they are processing large volumes of patient data?
We always review our assurance requirements but local organisations ought to assure every supplier they believe is critical to provision of care.

How far are we expected to go when reviewing suppliers/contractors? For example, we assess the supplier's credentials, but do we need to get assurances from the supplier we have contracted about their processors or suppliers. How deep do we need to go to be assured vs how much do we rely on the contract that the supplier has done their due diligence?
Credentials are a sign of the organisation’s compliance with industry certifications but do not assure the products and services provided. Knowing who else supplies your supplier helps in supply chain and risk management.

Standards

Why should organisations consider completing other standards (eg. CE+/IS027001) if they do not result in exemptions for sections of CAF DSPT?
The DSPT implements the CAF as the principal cyber security standard for health and care as set out in the cyber security strategy. Organisations may wish to pursue additional standards if they consider them relevant for their own reasons, or if entering into contractual arrangements that require other standards, but there is no requirement from NHS England to do so.

Outcome specific questions and answers

A3.a	***Asset management***	***Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).***

Will NHS England be releasing a new Information Assets & Flows Register template to comply with the asset management requirements of the CAF-aligned DSPT?

Under the legacy DSPT, you were required to maintain an Information Assets & Flows Register for cataloguing information assets and complying with the UK GDPR requirement to maintain a Record of Processing Activities (ROPA). NHS England provided a universal Information Assets & Flows Register template for this purpose. You were also required to maintain an inventory of your hardware and software assets, which could be included in the same document. Although the CAF-aligned DSPT uses a different assurance approach, these asset management requirements have not changed, and the NHS England Information Assets & Flows Register template remains fit for purpose.

B2.b	*Device management*	*You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).*

Is device management including all medical devices, connected to the network? And are modalities included in "mobile devices?"
Yes, all devices that support your provision of service should be included in your scope.

Is device management including all medical devices, connected to the network?
Yes, all devices that support your provision of service should be included in your scope.

Would the MDE device discovery function assist with B2.b assertion?

It would certainly support with the indicator of good practice
PA#3
You have sought to understand the security properties of third-party devices and networks before they can be connected to your systems. You have taken appropriate steps to mitigate any risks identified.

And also PA#5:
You are able to detect unknown devices being connected to your network and investigate such incidents.

For Trusts who have fully deployed MDE - is there a model answer to these questions?
Example answers are being developed and will be shared soon

B3.d	*Mobile data*	*You have protected data important to the operation of your essential function(s) on mobile devices.*

With mobile devices, why are laptops included and desktop PCs excluded?
The definition is "Mobile devices are any devices that are portable in nature which your organisation uses to perform specific functions." All devices are covered in *B2.b Device - You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).*

Does 'mobile device' include Bring Your Own Device (BYOD)?
If those BYOD devices hold personal data or support your essential functions, then yes, they should be included as part of your assurance of mobile devices.

In the future we won't be permitted to have BYOD? We can currently use own devices and connect via a VPN. This is potentially going to be very costly if this is correct.
It will be the responsibility of organisations to manage access to IT infrastructure and ensure systems and information remain secure.

Would the MDE device discovery function assist with B2.b assertion?
The decision should be managed by organisations on the use of BYOD, it is the responsibility of organisations to ensure their technical infrastructure is not comprised by allowing such access.

B5.a	*Resilience preparation*	*You are prepared to restore the operation of your essential function(s) following adverse impact.*

Would a Business Impact Assessment (BIA) cover B5.a?

A Business Impact Assessment BIA would support but not necessarily cover all of the outcome for B5.a.

This specific guidance document explains all the requirements for B5.a: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/2024-25-caf-aligned-dspt-guidance/objective-b/principle-b5-resilient-networks-and-systems#b5-a-resilience-preparation

Some examples of the sort of evidence you might use from the guidance are:

- information assets and flows register or information asset register
- DSPT scoping documentation
- business continuity and disaster recovery plans
- sources of threat intelligence
- risk registers

B4.a	*Secure by design .*	*You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential*

<table>
<tr><td></td><td></td><td><i>function(s) should not be impacted by the exploitation of any single vulnerability</i></td></tr>
<tr><td colspan="3"><b>Seems to focus more on IT arrangements but a lot of our data flows are smaller between organisations to facilitate workstreams. Is IT the new direction?</b>

Requirements that typically come under the umbrella of IG such as your IAR and ROPA are required under B3.a Understanding data. The CAF-aligned DSPT does not diminish responsibilities to document data flows which are not the traditional domain of IT and how they are protected.</td></tr>
<tr><td><i>B4.d</i></td><td><i>Vulnerability management</i></td><td><i>You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).</i></td></tr>
<tr><td colspan="3"><b>Will one evidence item be enough for B4.d or will more than one be needed?</b>

The decision rests with your organisation. If one document contains all the features necessary to show you have met all requirements of an outcome, then you can justify a decision to only upload one document. You would need to be able to rationalise your thinking in your supporting statement. This response relates to all outcomes.</td></tr>
<tr><td>B5.c</td><td>Backups</td><td>You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).</td></tr>
<tr><td colspan="3"><b>Does B5.c require you to look at and interrogate your third party IT suppliers to ensure service and systems are restored quickly?</b>
This should naturally form part of contractual agreements with suppliers and key performance indicators monitoring.</td></tr>
<tr><td>D1</td><td>Response and recovery planning</td><td>There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) in the event of system or service failure and to uphold the rights of impacted individuals. Mitigation activities designed to contain or limit the impact of compromise are also in place.</td></tr>
<tr><td colspan="3"><b>Can D1 be evidenced with an Incident Response Plan?</b>
Yes, that will certainly form part of your provided evidence. The goal here is ensuring that your response plan aligns with the indicators of good practice, taking account of likely incident scenarios, providing you with a pathway back to delivering your services, being understood by relevant stakeholders (which may require training needs analysis to show how you have ensured this is the case), etc.

<b>Does D1 require one incident response plan, we have several looking at various different types of critical event (Environmental, Cyber, Major incident)</b></td></tr>
</table>

No - the expectation is that you would have several and you should look to cover wide-ranging scenarios as you have mentioned. These response plans may all be part of the same document, but that is for you to decide locally.