NHS England

Cyber Assessment Framework–aligned Data Security and Protection Toolkit

Strengthening Assurance –
Short audit guide for outcomes mandated 2025

Creating a culture of Improvement

Information and Technology for better health and care

16th Dec 2024

Purpose of the document

This document is being provided in advance of the full Independent Assessment Guide to support planning and provide detailed guidance for the specific outcomes which are mandated to be audited for the 2024-2025 Data Security and Protection Toolkit (DSPT). Outcomes mandated to be audited for 2025 are:

Health and care CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective A - Managing risk				
Risk management	A2.a Risk management process		PA	
Supply chain	A4.a Supply chain		PA	
Objective B - Protecting against cyber attack and data breaches				
Identity and access control	B2.a Identity verification, authentication and authorisation		PA	
System security	B4.d Vulnerability management		PA	
Objective C - Detecting cyber security events				
Security monitoring	C1.a Monitoring coverage		PA	
Objective D - Minimising the impact of incidents				
Response and recovery planning	D1.a Response plan		PA	
Objective E - Using and sharing information appropriately				
Upholding the rights of individuals	E2.b Consent			A
Using and sharing information	E3.a Using and sharing information for direct care			A

Note organisations are required to select a further 4 outcomes to be audited. These outcomes should be approved by the Board of each organisation and will reflect areas of concern that warrant additional assurance over the controls in place during that audit period.

The contents of this document apply to the independent assessment arrangements of NHS Trusts (Acute, Foundation, Ambulance and Mental Health), Integrated Care Boards, Commissioning Support Units and Department of Health and Social Care (DHSC) Arm's Length Bodies.

The approach and documentation list described in this guide provides guidance to auditors on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved. Independent assessors are expected to use their professional judgement when assessing organisations against CAF aligned DSPT.

More information will be made available in the NHS England (NHSE) CAF DSPT Independent Assessment Guide. Further updates will be provided on the DSPT News website: https://www.dsptoolkit.nhs.uk/News.

Principle A2: Risk management

Description

The organisation takes appropriate steps to identify, assess and understand risks to the security and governance of information, systems and networks supporting the operation of essential functions. This includes an overall organisational approach to risk management.

Overview of the underlying contributing outcomes

Contributing outcome A2.a – Risk management process

Outcome A2.a – Risk management process

Description

Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).

The expectation for this contributing outcome is **Partially Achieved**.

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Risk assessments are not based on a clearly defined set of threat assumptions. NA#2. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. NA#3. Risk assessments (including DPIAs) for network and information systems supporting your essential function(s) or high-risk processing activities are a “one-off” activity (or not done at all). NA#4. The security and IG elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. NA#5. There is no systematic process in place to identify risks, and then ensure that identified risks are managed effectively, which	PA#1. Your organisational process ensures that security and wider Information Governance (IG) risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process. PA#2. Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your essential function(s), as well as your other data processing activities. PA#3. The output from your risk management process is a clear set of security and IG requirements and mitigations that will address the risks in line with your organisational approach to security and IG more widely. PA#4. Significant conclusions reached in the course of	A#1. Your organisational process ensures that security and wider Information Governance (IG) risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process. A#2. Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your information, systems and networks. A#3. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your

	includes incorporating data protection by design and default.		your risk management process are communicated to key decision -makers and accountable individuals.		essential function(s) and your sector.
NA#6.	Systems and risks are assessed in isolation, without consideration of dependencies and interactions with other systems or risks in other areas of the business. For example interactions between IT and operational technology environments, or finance risks and the impact on information governance.	PA#5.	You conduct risk assessments (including DPIAs) when significant events potentially affect the essential function(s), such as replacing a system, commencing new or changing high-risk data processing, or a change in the cyber security threat.	A#4.	Your risk assessments are informed by an understanding of the information and vulnerabilities in the systems and networks supporting your essential function(s), as well as a good understanding of your data processing activities in all areas of your organisation. This includes evaluation of repeated or significant near misses.
NA#7.	Security and IG requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function(s).	PA#6.	You perform threat analysis and understand how generic threats apply to your organisation.	A#5.	The output from your risk management process is a clear set of requirements that will address the risks in line with your organisational approach to security and IG more widely.
NA#8.	Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve. These risks may be out of date or incomplete.	PA#7.	Your risk process clearly demonstrates how your organisation's processing complies with data protection principles and relevant legislation, including the right to a private life.	A#6.	Significant conclusions reached in the course of your risk management process are communicated to key decision-makers and accountable individuals.
				A#7.	Your risk assessments (including DPIAs) are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use or processing, and new threat information.
				A#8.	The effectiveness of your information and security risk management process is reviewed periodically, and improvements made as required.
				A#9.	You perform detailed threat analysis and understand how this applies to your

			organisation in the context of the threat to your sector and the wider Critical National Infrastructure.
		A#10.	Your risk process clearly demonstrates how your organisation's processing complies with data protection principles and relevant legislation, including the right to a private life.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Risk management process** - Verify that:
   a) The organisation has comprehensive processes for identifying, analysing, prioritising and managing information governance and cyber security risk (PA#1, A#1)
   b) There is a specific process which the organisation adheres to for conducting risk assessments when significant events occur that could affect the organisation's essential functions (PA#5, A#7)
   c) There is a specific process which the organisation adheres to for conducting DPIAs before beginning any type of processing which is likely to result in a high risk to the rights and freedoms of individuals (PA#5, A#7)
   d) The organisation's adherence to agreed processes are reflected in the organisation's risk management documentation such as risk registers and risk assessments (PA#1, A#1)
2. **Risk management documentation** - Verify whether the documents show:
   a) Data protection by design and by default, incorporated in the process; (PA#1, A#1)
   b) Consideration of data protection principles and relevant legislation, including the right to private life where applicable. (PA#7, A#10)
3. **Understanding information and vulnerabilities** – Obtain and inspect the organisation's risk registers and a sample of the organisation's risk assessments. Verify that:
   a) For projects involving personal information, the nature of personal and sensitive information is appropriately considered as part of risk management processes (PA#2)
   b) For projects involving changes to systems and networks, vulnerabilities are appropriately considered as part of risk management processes (PA#2)
4. **Risk management actions** - Obtain the outputs of the risk management process discussed in step 1 and step 3, and assess whether the outputs include clear requirements and mitigation to address risks in line with the organisation's approach to cyber security and IG more widely. (PA#3, A#5)
5. **Communicating to accountable individuals** - Verify that the organisation has established thresholds for situations where outputs of risk management processes should be communicated to key decision-makers and accountable

individuals. Obtain evidence that this communication occurs where it is needed. (PA#4, A#6)

6. **Threat analysis** - Assess how the organisation has incorporated threat intelligence into its cyber risk management processes. (PA#6, A#9)

Additional approach to testing - Achieved

1. **Risk impact** – Discuss the process for evaluating the business impact of various scenarios, and assess whether the adverse impacts on the organisation's essential functions has been understood and documented. Obtain a sample of scenario business impact evaluations and verify that the results are fed into the risk management process. (A#2)
2. **Threat assumptions** - Obtain evidence that the organisation maintains a set of threat assumptions based on threat intelligence it receives and its own threat analysis, and that it has an effective review process to ensure these assumptions remain up-to-date. Verify that the threat assumptions are tailored to the organisation's individual circumstances and cover a wide range of possible attacks. Assess whether these threat assumptions are appropriately integrated into the organisation's risk management processes. (A#3)
3. **Near misses** - Obtain a sample of the organisation's repeated or significant near misses and assess whether the organisation effectively integrates lessons learned from these into its risk management processes. (A#4)
4. **Dynamic risk assessments** - Determine whether there are processes and controls in place to ensure that the risk assessments are updated based on changes in threats, data use or processing and technical changes. Obtain evidence of risk assessments updated following this process. (A#7)
5. **Risk management process review** - Verify what specific criteria the organisation uses to evaluate the effectiveness of its risk management processes. Obtain evidence that evaluations occur on a scheduled or efficiently reactive basis and improvements are made to strengthen risk management processes where appropriate. (A#8)
6. **Threat analysis** - Obtain evidence that the organisation performs ongoing detailed threat analysis to understand the wide range of attacks and threat actors it is subject to at any given time. Verify that threat assumptions are reviewed in response to changes in the threat landscape such as significant geo-political events, knowledge of new cyber-attack campaigns and threat intelligence received from authoritative sources. Obtain evidence that this detailed threat analysis is incorporated into risk management processes. (A#9)

Suggested documentation – Partially Achieved

- Procedures for identifying, analysing, prioritising and managing information governance and cyber security risk
- Risk assessments
- Data protection impact assessments (DPIAs)
- Risk registers
- Evidence of data protection by design and by default being incorporated into risk management processes
- Evidence of data protection principles and relevant legislation being incorporated into risk management processes
- Evidence of nature of information being considered as part of risk management processes
- Evidence of vulnerabilities in systems and networks being considered as part of risk management processes
- Procedures for communicating significant conclusions from risk management processes to accountable individuals
- Evidence of threat intelligence being used for cyber risk management processes

Additional documentation – Achieved

- Evidence of business impact evaluations for multiple scenarios
- Threat assumptions and review process
- Evidence of lessons learned from near misses being integrated into risk management processes
- Evidence of dynamic risk assessments
- Procedures for evaluation and improvement of risk management processes
- Evidence of ongoing detailed threat analysis

Principle A4: Supply chain

Description

The organisation understands and manages security and information governance (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 of the underlying contributing outcomes

Contributing outcome A4.a – Supply chain

Outcome A4.a – Supply chain

Description

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.

The expectation for this contributing outcome is **Partially Achieved**.

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:		**Partially Achieved** All the following statements are true:		**Achieved** All the following statements are true:	
NA#1.	You do not know what data belonging to you is held by suppliers, or how it is managed.	PA#1.	You understand the general risks suppliers may pose to your essential function(s).	A#1.	You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as IG considerations, due diligence, supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes.
NA#2.	Elements of the supply chain for essential function(s) are subcontracted and you have little or no visibility of the sub-contractors.	PA#2.	You know the extent of your supply chain that supports your essential function(s), including sub-contractors.	A#2.	Your approach to supply chain risk management considers the risks to your essential function(s) arising from supply chain subversion by capable and well-resourced attackers.
NA#3.	You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security or information governance (IG) obligations.	PA#3.	You understand which contracts are relevant and you include appropriate security and data protection obligations in relevant contracts.	A#3.	You have confidence that information shared with suppliers that is essential to the operation of your function(s) is appropriately protected from sophisticated attacks.
NA#4.	Suppliers have access to systems that provide your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.	PA#4.	You are aware of all third-party connections and have assurance that they meet your organisation's security and IG requirements.	A#4.	You understand which contracts are relevant and you include
NA#5.	IG is not factored into the procurement process.	PA#5.	Your approach to security and data protection incident management considers incidents that might arise in your supply chain.		
NA#6.	You are not sure if any data shared with suppliers leaves the UK, or if all international data transfers are covered by a legal protection.	PA#6.	You have confidence that information shared with suppliers that is necessary for the operation of your essential function(s) is appropriately protected		

	from well-known attacks and known vulnerabilities. PA#7. All international data transfers to suppliers are covered by a legal protection.	appropriate security and data protection obligations in relevant contracts. You have a proactive approach to contract management which may include a contract management plan for relevant contracts. A#5. Customer / supplier ownership of responsibilities are laid out in contracts. A#6. All network connections and data sharing with third parties is managed effectively and proportionately. A#7. When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents. A#8. You routinely liaise with other teams to keep track of changes to services that impact your organisation's agreements. A#9. All international data transfers to suppliers are covered by a legal protection. A#10. Your processor has appropriate certification and agree to be audited either by your organisation or an independent auditor.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Supplier risks** - Ascertain how the organisation identifies, and documents risks posed by suppliers to its essential functions. (PA#1)
2. **Knowledge of supply chain -** Verify that the organisation has understood and documented all suppliers who support its essential functions. Where possible, this should include sub-contractors involved in the services supporting the essential functions. Where identifying sub-contractors is not possible, the organisation should document the efforts they have made to acquire this information. (PA#2)
3. **Supplier contracts** - Obtain a sample of the organisation's supplier contracts. Verify that:
   a) Appropriate cyber security and data protection obligations have been included; (PA#3)
   b) The data being shared by the organisation is clearly documented and understood by both parties; (PA#3, PA#6, A#3)
4. **Third-party connections** - Obtain evidence that the organisation has documented all third-party connections to its networks. Verify what assurance the organisation has in place that each third-party connection and the vendor it belongs to meets the organisation's cyber security and information governance requirements. Where gaining assurances is not possible, the organisation should document the efforts they have made to acquire this information. (PA#4)
5. **International data transfers -** Verify that the organisation understands and documents all countries where data is being processed as part of its supplier-offered services. Obtain evidence that there are either adequacy decisions in place for these countries, or where there is no adequacy decision the organisation has appropriate legal mechanisms in place to facilitate the data transfer. (PA#7, A#9)
6. **Supplier assurance** - Verify what assurances the organisation obtains from suppliers to ensure that they meet the organisation's security and IG requirements. The assurances should be sufficient to confirm that information shared with the supplier is appropriately protect from well-known attacks and known vulnerabilities. (PA#6)
7. **Incident management** – Discuss the incident management process and assess whether third-party incidents are considered. Verify that the organisation has agreed specific measures in their process to aid their response to incidents involving third parties. (PA#5)

Additional approach to testing – Achieved

1. **Detailed supplier risks** – Obtain evidence that the organisation has identified and documented risks posed by suppliers to a deep level of detail. Verify that the organisation interrogates these risks as part of its risk assessment and procurement processes before onboarding suppliers. The risk considerations should include specific IG and cyber risks which emerge as a result of the supplier's sub-contractors, the supplier's partnerships and the supplier's geographic location. (A#1)
2. **Supply chain risk management -** Obtain evidence that the risks documented in step 1 have been discussed and reviewed by responsible decision-makers within the organisation. Where subversion of suppliers' services would cause unacceptable consequences, mitigations should have been discussed, with short-term and long-term plans for remediation. (A#2)
3. **Assurance against sophisticated attacks** - Verify what assurances the organisation obtains from suppliers to ensure that they meet the organisation's security and IG requirements. The assurances should be sufficient to confirm that information shared with the supplier is appropriately protected from sophisticated attacks. (A#3)
4. **Contract management plan** – Verify whether the organisation has a contract management plan in place which allows for regular review of important contracts. (A#4)
5. **Roles and responsibilities** - Obtain the list of supplier contracts and obtain a sample. Verify that the customer/supplier ownership of responsibilities are laid out in those contracts. (A#5)
6. **Network connections and data sharing** - Obtain evidence that the organisation understands and documents third-party connections to its network and data sharing with third-parties. Assess the supplier management processes the organisation has in place for ensuring that these connections and data being shared are necessary and proportionate for the services being provided, and obtain evidence that these processes are followed. (A#6)
7. **Incident management process** - Obtain and inspect the organisation's incident management process, and assess whether suppliers' roles and responsibilities are documented. Request evidence of assurance the organisation has received from their most critical suppliers of mutual support during incidents. (A#7)
8. **Changes in services** - Verify that the organisation has a scheduled or efficiently reactive process for liaising with other teams to keep track of changes to services that impact cyber security and information governance-related understandings and agreements with suppliers. Obtain evidence that this process is followed and changes are made where necessary without undue delay. (A#8)

9. **Certification and right to audit** - Verify that as part of the organisation's procurement processes, there is a requirement for supplier certifications to be obtained prior to the contract being signed. For the suppliers who the organisation has identified as most critical to the operation of its essential functions, contracts should also include a right to audit, based on specific parameters relevant to the services being provided. (A#10)

Suggested documentation – Partially Achieved

- Documentation showing supplier risks to essential functions
- Lists of suppliers and sub-contractors
- Supplier contracts
- Documentation showing third-party connections
- Evidence of international data transfers being considered as part of supplier management processes
- Supplier assurances regarding their cyber security and information governance practices
- Incident management process documentation

Additional documentation – Achieved

- Documentation showing detailed supplier risks to essential functions
- Procedures for supplier risk management
- Contract management plan
- Procedures for managing third-party connections and data sharing
- Supplier assurances of incident support
- Procedures for cross-organisational tracking of changes in services
- Evidence of right to audit for critical suppliers

Principle B2: Identity and access control

Description

The organisation understands, documents and manages access to information, systems and networks supporting the operation of essential functions. Individuals (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.

Overview of the underlying contributing outcomes

Principle B2.a – Identity verification, authentication and authorisation

Outcome B2.a – Identity verification, authentication and authorisation

Description

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Initial identity verification is not robust enough to provide an acceptable level of confidence of a users' identity profile. NA#2. Authorised users and systems with access to information, systems and networks on which your essential function(s) depends cannot be individually identified. NA#3. Unauthorised individuals or devices can access information or networks on which your essential function(s) depends. NA#4. The number of authorised users and systems that have access to your information, systems and networks are not limited to the minimum necessary. NA#5. Your approach to authenticating users, devices and systems does not follow up to date best practice.	PA#1. Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function(s). PA#2. All authorised users and systems with access to information, systems and networks on which your essential function(s) depends are individually identified and authenticated. PA#3. The number of authorised users and systems that have access to essential function(s) information, systems and	A#1. Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function(s). A#2. Only authorised and individually authenticated users can physically access information and logically connect to your networks or information systems on which your essential function(s) depends. A#3. The number of authorised users and systems that have access to all your information, systems and networks supporting the essential function(s) is limited to the minimum necessary. A#4. You use additional authentication mechanisms, such as multi-factor

	networks is limited to the minimum necessary. PA#4. You use additional authentication mechanisms, such as multi-factor authentication (MFA), for privileged access to all network and information systems that operate or support your essential function(s). PA#5. You individually authenticate and authorise all remote access to all your networks and information systems that support your essential function(s). PA#6. The list of users and systems with access to information, systems and networks supporting and delivering the essential function(s) is reviewed on a regular basis, at least annually. PA#7. Your approach to authenticating users, devices and systems follows up to date best practice.	authentication (MFA), for all user access, including remote access, to all network and information systems that operate or support your essential function(s). A#5. The list of users and systems with access to information, systems and networks supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months. A#6. Your approach to authenticating users, devices and systems follows up to date best practice.

As documented in the Introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below provide guidance on how to conduct testing but should be adapted depending upon evidence provided by NHS providers to show how they meet the outcomes.

Suggested approach to testing – Mandatory policy requirement

1. **MFA policy** – Through a combination of testing samples of user access to systems, inspecting relevant documentation and asking to see assurances the organisation has acquired from suppliers (depending on what is practical for the area being assessed) verify that the organisation has enforced multi-factor authentication (MFA) on:
   a) all remote user access to all systems, subject to exceptions permitted in the NHS England MFA policy
   b) all privileged user access to externally-hosted systems, subject to exceptions permitted in the NHS England MFA policy
   c) all privileged user access to all other systems, subject to fully assessing the implications of any alternative course of action, and subject to the exceptions permitted in the NHS England MFA policy.
2. **Permitted exceptions** - Verify that any reliance on permitted specific exceptions follows the requirements set out in the MFA policy, namely that the organisation:
   a) understands, documents, risk-assesses, and internally approves (at board level or as delegated) all exceptions, with annual review
   b) has and is actively pursuing plans to minimise or eliminate completely the exceptions; and
   c) retains documentary evidence for audit purposes and provides a summary within its DSPT submission.

Suggested approach to testing – Partially Achieved

1. **Identity verification -** Ascertain the organisation's process for verifying the identity of employees before they are allowed access to physical or electronic information. The process should include:
   a) pre-employment checks to appropriately identify individuals (PA#1)
   b) a minimum level of identity verification for all staff members such as the NHS Employment Check or Baseline Personnel Security Standards (PA#1)
   c) consideration of the level of access they will have to physical or electronic information before allowing access (PA#1)
   d) consideration of specific roles which may require more stringent background checks or security clearances, such as those with more sensitive or privileged access such as an IT admin role (PA#1)

2. **Verification of temporary staff members:** If applicable, verify that the organisation has obtained assurances from any external staffing agencies it uses that temporary staff members' identities are verified before deployment. (PA#1)
3. **User authentication** - Verify that the organisation has robust processes for authenticating users. This process should include ensuring the verified user identity is authenticated through an appropriate authentication method such as a password, biometrics data, etc. This could include password complexity requirements, number of attempts allowed and whether a large number of failed attempts is flagged to the IT team. It should also include any additional security required for admin-level users, and may also include additional security such as MFA. Obtain logs to verify that the process is adequately implemented. (PA#2)
4. **Limiting user access** - Obtain the list of user groups with access to information and systems supporting the essential function, and assess whether their level of access is appropriate based upon their role. Verify that the organisation has established specific business cases for different levels of access, and that new users are assessed against business cases prior to access being granted. (PA#3, A#3)
5. **Multi-Factor Authentication** - Obtain evidence that additional authentication mechanisms, such as multi-factor authentication (MFA), is used for privileged access to all network and information systems that operate or support essential functions, in line with NHSE MFA policy. Verify the implementation of this control, for example by checking in-person or via screenshare with a privileged user that MFA is required when they try to log in. Request a sample of privileged users to test that MFA is required for access. (PA#4)
6. **Remote login** - Obtain and inspect the remote login process, and assess whether users are required to authenticate before accessing the organisation's network. Assess the authentication method in use for remote login and verify that is it at least as strong as on-site login. Obtain evidence that remote authentication is in place or all users. (PA#5)
7. **Access rights review** - Obtain and inspect the list of users and systems with access to information, systems and networks supporting and delivering the essential functions. Obtain a sample of these and verify that their access rights have been reviewed in the last year. (PA#6)
8. **Alignment to best practices** - Obtain the authentication policy (or equivalent) and verify that it is aligned to best practices, for example OWASP and NIST. (PA#7, A#6)

Additional approach to testing – Achieved

1. **Identity verification** - In addition to the controls assessed in step 1 of the Partially Achieved approach to testing, obtain documentation which outlines the different roles which require higher levels of verification e.g. user admins. Test a sample of anonymised privileged users which should meet higher verification standards and test if they have undertaken them. (A#1)

2. **Physical security** - Obtain the physical security policy (or equivalent) and assess the controls in place to ensure the security of the systems and information on which essential services rely. This should include limiting access to buildings and rooms that contain servers and endpoints which could be used to access the organisation's network, but also authenticating access to those buildings and rooms, ensuring that clear accountability is given for any activity taking place. While on-site, verify the implementation of these security controls. (A#2)
3. **Multi-Factor Authentication** - Obtain the cyber security policy (or equivalent), and assess whether the use of MFA is mandated for all users across the organisation, including remote access, to all network and information systems that operate or support essential function(s). The organisation must meet the requirements of the NHSE MFA Policy and be able to evidence this through the following:
    a) Organisations must enforce Multi-Factor Authentication (MFA) on all remote user access to all systems. This can be evidenced though testing a sample of remote user access for a sample of systems.
    b) Organisations must enforce MFA on all privileged user access to externally-hosted systems. This can be evidenced though testing a sample of privileged user access to a sample of externally hosted systems. This should include organisational and third-party privileged access.
    c) Organisations should enforce MFA on all privileged user access to all other systems. This can be evidenced though testing a sample of privileged user access for a sample of systems.
    d) Permitted exceptions to these requirements are detailed in the MFA policy. Review document exceptions to the policy which have been approved by an appropriate body and in line with the NHS MFA Policy exemption guidance. (A#4)
4. Verify that this control has been implemented by obtaining a list of users and verifying their access to network and information systems that operate or support essential function(s). (A#4)
5. **Access rights review** - Obtain and inspect the list of users and systems with access to information, systems and networks supporting and delivering the essential functions. Obtain a sample of these and verify that their access rights have been reviewed in the last six months. (A#5)

Suggested documentation – Mandatory policy requirement

- Evidence of authentication controls in place for user access to systems
- Procedures for application of multi-factor authentication
- Assurances from suppliers
- Documentation of permitted exceptions
- Action plans for minimising and eliminating permitted specific exceptions

Suggested documentation – Partially Achieved

- Procedures and third-party assurances for identity verification
- Authentication policy (or equivalent documentation showing user authentication processes are in place);
- List of user groups with access to information, systems and networks that essential functions depend on;
- Business cases for new users;
- Evidence of MFA for privileged users;
- Remote login documentation;
- Evidence of remote authentication;
- Evidence of access rights review for users and systems with access to information, systems and networks supporting and delivering the essential functions.

Additional documentation – Achieved

- List of anonymised privileged users;
- Physical security policy (or equivalent);
- Evidence of MFA for all users

Principle B4: System security

Description

As documented in the Introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework. The approach and documentation list described below provide guidance on how to conduct testing but should be adapted depending upon evidence provided by NHS providers to show how they meet the outcomes.

Overview of the underlying contributing outcomes

Outcome B4.d – Vulnerability management

Outcome B4.d – Vulnerability management

Description

You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. You do not understand the exposure of your essential function(s) to publicly-known vulnerabilities. NA#2. You do not mitigate externally-exposed vulnerabilities promptly. NA#3. You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential function(s). NA#4. You have not suitably mitigated systems or software that is no longer supported. NA#5. You are not pursuing replacement for unsupported systems or software.	PA#1. You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities. PA#2. Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and externally-exposed vulnerabilities are mitigated (e.g. by patching) promptly. PA#3. Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period. PA#4. You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology. PA#5. You regularly test to fully understand the	A#1. You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities. A#2. Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly. A#3. You regularly test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing. A#4. You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential function(s).

	vulnerabilities of the networks and information systems that support the operation of your essential function(s).	

As documented in the Introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below provide guidance on how to conduct testing but should be adapted depending upon evidence provided by NHS providers to show how they meet the outcomes.

Suggested approach to testing – Mandatory policy requirement

1. **Implementing high severity alerts** – Verify that:
   a) Organisations have, and reliably apply, appropriate procedures for deciding whether to follow the advice within a high severity alert, with any decisions not to follow the advice being taken at board level (or as delegated).
   b) Implementation decisions are reported using the NHS England 'Respond to an NHS cyber alert' service within 14 days of the alert being issued
2. **Sample testing** - Review a sample of high severity alerts for decisions and implementation action. Where a decision has been made not to follow the advice within an alert, verify that it was made by a person or committee with appropriate authorisation. Where a decision has been made to follow the advice, verify that appropriate activity has occurred or is planned. Confirm that each decision has been reported to NHS England within 14 days of the alert being issued.

Suggested approach to testing – Partially Achieved

1. **Threat intelligence gathering** - Ascertain how the organisation gathers threat intelligence, and which sources of threat intelligence it uses. Obtain evidence that the organisation cross-checks threat intelligence it receives against its own systems to understand its exposure to publicly known vulnerabilities. (PA#1, A#1)
2. **Vulnerability management process** - Assess whether there is a documented process in place to:
   a) Receive, track and analyse announced vulnerabilities for all software packages, network and information systems used to support essential functions; (PA#2)
   b) Prioritise the vulnerabilities based on the risk they pose to the organisation; (PA#2)
   c) Mitigate externally-exposed vulnerabilities within a defined timeframe, which should be based on the risk assessment in step 2.b. (PA#2)
   d) Perform a risk-based assessment that dictates which severity level of vulnerabilities can have temporary mitigations applied to them, and how long those mitigations can be in place before the vulnerability must be fully remediated. (PA#3)
   e) Scan the organisation's network to identify vulnerabilities, including how frequently those scans take place. (PA#5)

3. **Sample testing of vulnerabilities** - Obtain the list of announced vulnerabilities that have been recorded by the organisation and sample test whether the process in step 2 is being adequately followed. (PA#2)
4. **Temporary mitigations** - Obtain the list of vulnerabilities and sample test whether the process for applying temporary mitigations is being adequately applied. (PA#3)
5. **Migration to supported technology** - Obtain and inspect the list of unsupported systems and software, and assess whether:
   a) There is a plan in place to migrate the system or software to a supported technology; (PA#4)
   b) Temporary mitigations have been discussed, approved and are being implemented. (PA#4)
6. **Network scanning** - Obtain a sample of network scans to verify if the expected frequency is followed. Assess whether the vulnerability management process includes a process for analysing and prioritising the identified vulnerabilities. (PA#5)

Additional approach to testing – Achieved

1. **Vulnerability management process** - In addition to the controls assessed in step 2 of the Partially Achieved approach to testing, verify that internal vulnerabilities are also mitigated within a defined timeframe, which should be documented within the vulnerability management process. (A#2)
2. **External scanning** - In addition to the controls assessed in step 6 of the Partially Achieved approach to testing, assess whether the vulnerability management process requires the organisation to verify its understanding with a third-party, such as the asset supplier, NCSC or auditors. (A#3)
3. **Asset support** - Obtain the list of networks and information systems supporting essential functions, and assess whether the end-of-life (EOL) and/or end-of-support (EOS) dates have been documented. Discuss with management whether there is a documented process in place for planning end-of-life for critical systems, for example by renewing the support contract or migrating to newer versions. If this document exists, inspect it and assess whether it includes key contact (internal and external), and how long before the EOL/EOS this process should be started. (A#4)

Suggested documentation – Mandatory policy requirement

- Evidence of procedures for implementing high severity alerts issued by NHS England
- Sample of evidence of implementing high severity alerts issued by NHS England
- Sample of documented decisions for high severity alerts issued by NHS England

Suggested documentation – Partially Achieved

- Procedures for gathering and analysing threat intelligence;
- Vulnerability management process;
- List of announced vulnerabilities;
- Evidence of temporary mitigations being applied;
- List of unsupported systems and software;
- Evidence of plans to migrate unsupported systems or software;
- Sample of network scans.

Additional documentation – Achieved

- Evidence of internal vulnerabilities being remediated;
- Evidence of third-party testing of network and information system vulnerabilities;
- Process for planning end-of-life for critical systems.

Principle C1: Security monitoring

Description

The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Overview of the underlying contributing outcomes

Outcome C1.a – Monitoring coverage

Contributing outcome C1.a – Monitoring coverage

Description

The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Data relating to the security and operation of your essential function(s) is not collected. NA#2. You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential function(s), such as known malicious command and control signatures (for example, because applying the indicator is difficult or your log data is not sufficiently detailed). NA#3. You are not able to audit the activities of users in relation to your essential function(s). NA#4. You do not capture any traffic crossing your network boundary including as a minimum IP connections.	PA#1. Data relating to the security and operation of some areas of your essential function(s) is collected but coverage is not comprehensive. PA#2. You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures. PA#3. Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour. PA#4. You monitor traffic crossing your network boundary (including internet protocol (IP) address connections as a minimum).	A#1. Monitoring is based on an understanding of your networks, common cyber-attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function(s) (such as the presence of malware, malicious emails, user policy violations). A#2. Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s). A#3. You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures. A#4. Extensive monitoring of user activity in relation to the operation of essential function(s) enables you to detect policy violations and an

		agreed list of suspicious or undesirable behaviour. A#5. You have extensive monitoring coverage that includes host-based monitoring and network gateways. A#6. All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Monitoring coverage** – Enquire with the organisation which data sources it collects security logs for. Obtain and inspect documentation provided by the organisation showing how it has prioritised these sources based on risks to its essential functions. (PA#1)
2. **Security monitoring activities** – Inspect documents provided by the organisation relating to its security monitoring activities and/or discuss with management, which evidence how it:
    a) Detects the presence or absence of indicators of compromise (IoCs). The organisation should be able to demonstrate how IoCs would be easily detected. (PA#2, A#3)
    b) Monitors user activity. At least some user activity should be monitored, based on risk or agreed list of suspicious or undesirable behaviours. (PA#3)
    c) Monitors traffic crossing the network boundary. As a minimum, IP address connections should be monitored. (PA#4)

Additional approach to testing – Achieved

1. **Security monitoring strategy** – Obtain and inspect documents provided by the organisation to demonstrate that it has a comprehensive strategy for security monitoring which has been specifically targeted towards:
    a) the key risks the organisation has identified to its essential functions (A#1)
    b) the organisation's own network architecture (A#1)
    c) the attack techniques to which the organisation is most susceptible, based on its architecture (A#1)
2. **Security event and incident sampling –** Obtain the list of security incidents, checking how frequently incidents are identified and raised based on the organisation's monitoring data. From this list, inspect a sample of incidents to ascertain how much detail was provided through the monitoring logs, and whether this detail was enough to support identification of more sophisticated threat through monitoring and treat hunting. (A#2)
3. **User monitoring** – Obtain and inspect the list of suspicious or undesirable behaviour that is used to monitor user behaviours against. Obtain evidence that this monitoring takes place. (A#4)

4. **Security event monitoring** – Inspect documents provided by the organisation relating to its security monitoring coverage and assess whether:
    a) The organisation collects security logs from a wide enough range of sources to ensure that it is able to detect potential security incidents across all critical networks and systems. (A#5)
    b) Extensive monitoring is performed on network gateways. (A#5)
    c) Host-based monitoring is performed on devices which the organisation has identified as critical. (A#5)
5. **Maintaining comprehensive monitoring** - Verify documents provided by the organisation which demonstrate its process for evaluating new systems being added to its networks and determining whether they should be monitored as data sources. (A#6)

Suggested documentation – Partially Achieved

- Documents showing data sources being monitored and rationale
- Procedures for detecting IoCs
- Procedures for monitoring users
- Procedures for monitoring network boundary traffic

Additional documentation – Achieved

- Security Monitoring Strategy;
- List of security incidents;
- Documents showing extensive monitoring coverage
- Procedures for considering new systems as potential monitoring sources

Principle D1: Response and recovery planning

Description

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.

Overview of the underlying contributing outcomes

Outcome D1.a – Response plan

Contributing outcome D1.a – Response plan

Description

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.

The expectation for this contributing outcome is **Partially Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Your incident response plan is not documented. NA#2. Your incident response plan does not include your organisation's identified essential function(s). NA#3. Your incident response plan is not well understood by relevant staff. NA#4. Your incident response plan does not cover your obligations as a controller or processor.	PA#1. Your response plan covers your essential function(s). PA#2. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks and incidents only. PA#3. Your response plan is understood by all staff who are involved with your organisation's response function. PA#4. Your incident response plan is documented and shared with all relevant stakeholders. PA#5. Your response plan covers your obligations as a controller or processor. PA#6. Your response plan includes notifying impacted system partners.	A#1. Your incident response plan is based on a clear understanding of the security risks to information, systems and networks supporting your essential function(s). A#2. Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and breaches of individuals' rights and of possible attacks and breaches, previously unseen. A#3. Your incident response plan is documented and integrated with wider organisational business plans and supply chain response plans, as well as dependencies on supporting infrastructure (such as power, cooling etc). A#4. Your incident response plan is communicated and understood by the business areas involved

		with the operation of your essential function(s). A#5. Your incident response plan covers your obligations as a controller or processor. A#6. Your response plan includes notifying impacted system partners.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework.

The approach and documentation list described below are a suggestion to the independent assessors, and do not have to be followed stringently.

Suggested approach to testing – Partially Achieved

1) **Incident Response plans** - Obtain and inspect the incident response plans, assessing whether:
   a) It shows that the organisation's essential functions have been considered, with specific business areas and key contacts named who hold responsibility for those functions in the event of an incident. (PA#1)
   b) Scenarios have been identified and documented for known attacks and incidents. (PA#2)
   c) The roles and responsibilities of staff within the response function have been clearly documented and assigned. (PA#3)
   d) It includes a section on the obligations of the organisation as controller or processor of personal data for the reporting of incidents. This section should show the organisation's awareness of relevant data protection obligations, and how they will comply with them during an incident. It should also identify the stakeholders to be informed, such as the Information Commissioner's Office (ICO), and the timelines and procedure for informing them, for example through the Data Security and Protection Toolkit (DSPT) reporting portal.(PA#5)
   e) The response plans includes the requirement to notify impacted system partners (PA#6)
2) **Sharing with relevant stakeholders-** Obtain evidence that the incident response plan(s) has been approved by a relevant group and distributed to the response team. (PA#4).
3) **Personal data** – Review the latest report of an incident involving personal data and verify that procedures were followed appropriately. (PA#5)
4) **System partners** – A list of system partners exists, with key contacts for each to enable notification. (PA#6, A#6)

Additional approach to testing – Achieved

1) **Incident Response plan** - Obtain and inspect the incident response plan, assessing whether:
   a) It covers all stages of the incident response lifecycle, including preparation, detection, containment, eradication, recovery, and post-incident activities, for the most likely scenarios as dictated by risk assessments. (A#2)
   b) Dependencies on supporting infrastructure have been identified and documented. This also includes dependencies on suppliers and technology. (A#3)

c) It is integrated with other relevant policies and processes, for example the incident review process and business continuity policy. (A#3)
d) Its location is well-known and easily accessible to staff. (A#4)

2) **Risk assessments or risk management report**– Assess whether a risk assessment has been undertaken for each essential function, with the risks accounted for in the incident response plan(s). The risks identified should inform the response plan activities. (A#1)
3) **Staff knowledge** – Assess whether relevant staff have read and understood the document. This should also include third parties where relevant. Is there evidence of understanding, such as briefing sessions, emails, meeting minutes etc. (A#4)

Suggested documentation list – Partially Achieved

- Incident response plan(s);
- Evidence of incident response plan being approved and distributed to relevant staff members
- Report of the latest incident involving personal data;
- Evidence of communication plans / channels with system partners to coordinate incident response.

Additional documentation for Achieved level

- Image of policy repository (shared on screen)
- Risk assessment for each essential function
- Evidence of cross-organisational understanding of the incident response plan(s)

Principle E2: Upholding the rights of individuals

Description

The organisation respects and supports individuals in exercising their information rights.

Overview of the underlying contributing outcomes

Outcome E2.b - Consent

Contributing outcome E2.b - Consent

Description

You have a good understanding of requirements around consent and privacy, including the common law duty of confidentiality, and use these to manage consent.

The expectation for this contributing outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. Relevant staff members are not familiar with the common law duty of confidentiality or privacy rights or do not understand when they need to ask for consent. NA#2. You either do not have a policy or procedures in place, or are unsure whether your existing policy or procedures are adequate to ensure that consent is managed appropriately. NA#3. Information provided to patients and service users about their consent under the common law duty of confidentiality is either not given or unclear. NA#4. You do not have a process for refreshing consent when necessary.	*Partial achievement is not possible for this contributing outcome*	A#1. Relevant staff members understand consent under the common law duty of confidentiality, when they can rely on implied consent, and when they need to ask for or refresh existing explicit consent. A#2. Your organisation has a policy and procedures to ensure that consent is managed appropriately, including any decisions made by the Caldicott Guardian. A#3. Information provided to patients and service users about the use and sharing of information and consent is appropriate and clear.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Public information on consent** - Obtain the organisation's transparency materials and exemplar communications with the public relating to consent for information sharing. Assess whether:
   a) They cover common scenarios where consent will be asked before information sharing (A#3)
   b) Any written materials use clear and plain language, avoiding the use of technical terms and acronyms (A#3)
   c) The organisation has defined appropriate written and verbal methods for asking for consent for information sharing which staff members can refer to when needed (A#3) Clear headings and sub-headings (A#3)
2. **Consent policies and procedures** - Inspect any documents provided by the organisation relating to their policies and procedures for managing consent and assess whether they cover:
   a) the different scenarios where consent may be used as the organisation's basis for using and sharing information under UK GDPR and the Common Law Duty of Confidentiality (A#2)
   b) the organisation's processes for obtaining, withdrawing and maintaining a record of consent (A#2)
   c) the responsibilities of staff members for making justifiable decisions when deciding whether to seek patient consent, including when to involve Caldicott Guardian or equivalent senior staff members (A#2)
3. **Staff training** - obtain documents provided by the organisation showing how it has assured that staff are aware of how to appropriately manage requirements relating to consent, and assess whether they cover:
   a) the common law duty of confidentiality, tailored to the level of understanding required for a person's job role:
      i) for non-IG staff roles, this could be scenario-based awareness of situations where they have the implied consent of a patient, for example for direct care, and other situations where explicit consent may be needed, for example where information is being used to reasons outside of direct care (A#1)
      ii) for IG staff roles, this could be documentation showing how the common law duty of confidentiality has been considered by IG teams in previous decisions relating to whether or not to seek a patient's consent (A#1)
   b) how to appropriately obtain and keep records of consent where consent is needed (A#2)


NHS
England

Suggested documentation

- Documents showing organisation’s policies and processes relating to consent
- Public materials about consent (for example, privacy information)
- Records of consent
- Training materials
- Documents from steering group meetings

Principle E3: Using and sharing information

Description

The organisation uses and shares information appropriately.

Overview of the underlying contributing outcomes

Outcome E3.b – Using and sharing information for direct care

Contributing outcome E3.a – Using and sharing information for direct care

Description

You lawfully and appropriately use and share information for direct care.

The expectation for this contribution outcome is **Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. Relevant staff members do not understand what direct care is, the activities it covers and when they should use and share information to facilitate it. NA#2. Information is not always used or shared when it is needed for direct care. NA#3. Information being used or shared for direct care is either inadequate or excessive. NA#4. You are unsure whether individuals would reasonably expect their information to be used or shared in all instances where your organisation does so. NA#5. There are no arrangements in place for routine information sharing for direct care. NA#6. There is no process to share data for non-routine ad hoc direct care purposes, or it is not always followed.	*Partial achievement is not possible for this contributing outcome*	A#1. Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it. A#2. Information is used or shared for direct care when it is needed. A#3. Information which is used or shared for direct care is relevant and proportionate. A#4. When information is used or shared for direct care, individuals' reasonable expectations and right to respect for a private life are considered. A#5. Your organisation has a process in place to enable appropriate non-routine ad hoc data sharing for direct care purposes. A#6. There are appropriate arrangements in place for information sharing for direct care.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Policies and procedures** - Obtain and inspect documents provided by the organisation showing how they manage information sharing for direct care and assess whether they cover:
   a) scenarios where direct care information sharing can be handled by non-IG staff roles (A#2)
   b) scenarios where direct care information sharing requires escalation to IG team or equivalent (A#2, A#6)
   c) how they ensure information sharing is necessary and proportionate (A#3)
   d) how they ensure individuals' reasonable expectations and right to respect for a private life are considered in sharing decisions where relevant (A#4)
2. **Staff awareness** - Obtain evidence of how the organisation:
   a) identifies relevant staff roles who need to have an understanding of processes for direct care information sharing (A#1)
   b) makes relevant staff aware of scenarios where they should share information for direct care (A#1, A#2)
   c) makes relevant staff aware of scenarios where they should escalate direct care information sharing decisions to IG team or equivalent (A#1, A#2)
   d) makes relevant staff aware of their obligation to only share information which is proportionate and relevant (A#3)
3. **Data sharing arrangements** - Verify that:
   a) the organisation has agreed internal thresholds for direct care information sharing, which, when met, trigger a review of whether an arrangement such as a data sharing agreement, a sharing framework, a Data Protection Impact Assessment (DPIA), etc. is needed or would be beneficial (A#6)
   b) the organisation has procedures for ensuring that sharing arrangements for direct care appropriately cover the nature of the information being shared, ensuring sharing is appropriate and proportionate, and clarifying roles and responsibilities in the sharing (A#3, A#6)

Suggested documentation

- Evidence of policies and procedures for direct care information sharing
- Training needs analysis and materials used for staff awareness
- Documents related to data sharing arrangements for direct care