Cyber Assessment Framework–aligned Data Security and Protection Toolkit

Strengthening Assurance – Independent Assessment and Audit Framework

Creating a culture
of Improvement

Information and
Technology
for better health and care

FINAL

30/12/2024

Objective B – Protecting against cyber-attack and data breaches

Description

Proportionate security measures are in place to protect information, systems and networks supporting essential functions from cyber-attack and data breaches.

Overview of the underlying Principles

Principle B1: Policies, processes and procedures

Principle B2: Identity and access control

Principle B3: Data security

Principle B4: System security

Principle B5: Resilient networks and systems

Principle B6: Staff awareness and training

Principle B1: Policies, processes and procedures

Description

The organisation defines, implements, communicates and enforces appropriate policies, processes and procedures that direct its overall approach to securing information, systems and data that support operation of essential functions.

Overview of the underlying Contributing outcomes

Contributing outcome B1.a – Policy, process and procedure development

Contributing outcome B1.b – Policy, process and procedure implementation

Outcome B1.a – Policy, process and procedure development

Description

You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of 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. Your policies and processes are absent or incomplete. NA#2. Policies and processes are not applied universally or consistently. NA#3. People often or routinely circumvent policies and processes to achieve business objectives. NA#4. Your organisation's security governance and risk management approach has no bearing on your policies, processes and procedures. NA#5. System security is totally reliant on users' careful and consistent application of manual security processes. NA#6. Policies, processes and procedures have not been reviewed in response to major changes (such as technology or regulatory framework),	PA#1. Your policies, processes and procedures document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. PA#2. You review and update policies, processes and procedures in response to major cyber security incidents and data breaches. PA#3. Your IG policies, processes and procedures are aligned with national policies and legal frameworks.	A#1. You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Information assurance principles are integrated and embedded throughout these policies, processes and procedures and key performance indicators are reported to your executive management. A#2. Your organisation's policies, processes and procedures are developed to be practical, usable and appropriate for your essential function(s) and your technologies. A#3. Policies, processes and procedures that

or within a suitable period.

NA#7. Policies, processes and procedures are not readily available to staff, too detailed to remember, or too hard to understand.

NA#8. Your IG policies, processes and procedures are not aligned with national policies and legal frameworks.

rely on user behaviour are practical, appropriate and achievable.

A#4. You review and update policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident or data breach.

A#5. Any changes to the essential function(s) or the threat it faces triggers a review of policies, processes and procedures.

A#6. Your systems are designed so that they remain secure even when user security policies, processes and procedures are not always followed.

A#7. Your IG policies, processes and procedures are aligned with national policies and legal frameworks.

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. **Policies , procedures and processes** - Obtain the policies, processes and procedures relevant to security governance, risk management, technical security and regulatory compliance, and assess whether:
   a) The organisation has undergone a process (such as reviewing its suite of policies, processes and procedures against the outcomes of the CAF-aligned DSPT) to ensure all necessary areas are covered to reasonably mitigate known security and information risk. The organisation should be able to justify how it has reached its conclusion; (PA#1)
   b) The contents are appropriate for the type of organisation, and include key elements such as roles and responsibilities, laws and regulations to follow and the risk appetite of the organisation; (PA#1)
   c) The organisation has aligned its policies, processes and procedures to national policies (such as the National Data Opt Out) and legal frameworks (such as the National data opt out). The organisation should be able to demonstrate how it has identified relevant national policies and legal frameworks and appropriately incorporated them. (PA#3, A#7)
2. **Update following major incidents and data breaches** - Discuss with management the process for identifying changes required to policies, procedures and processes following major cyber security incidents and data breaches, and the process for getting those changes approved and implemented. Obtain evidence from the last major cyber security incidents and/or data breach and assess whether the process was followed. (PA#2, A#4)

Additional approach to testing – Achieved

1. **Policies, procedures and processes** - Obtain the overarching security governance and risk management approach, technical security practice and specific regulatory compliance documentation. In addition to the controls assessed in step 1 of “partially achieved” assess whether:
   a) The organisation has identified a set of key information governance principles (for example accountability, transparency) and cyber security principles (such as least privilege, application security), and has undergone a process to ensure its policies, processes and procedures reflect the best practical ways of fulfilling these principles. The organisation should be able to justify how it has reached its conclusion; (A#1)
   b) Policies, processes and procedures are mapped to relevant essential functions and technologies. The organisation has a scheduled or efficiently reactive review process when new technologies are implemented to identify and remediate areas

where confusion may arise as to how the policies, processes and procedures would be practically applied; (A#2)

   c) The organisation can explain which policies, procedures and processes are relevant to which staff groups, and has developed them to be practical, appropriate and achievable with the behaviours of those staff groups in mind; (A#3)

2. **Key performance indicators** - Discuss how the organisation has derived key performance indicators for relevant policies, processes and procedures (for example from security incidents, technical measurements, surveys, patient feedback). Verify whether these indicators are reported to executive management. (A#1)
3. **Regular document review** - Obtain and inspect evidence of the organisation's policies, processes and procedures being reviewed on a regular basis. Verify that the organisation has a justified rationale for the review intervals they have chosen. (A#4)
4. **Review following a change in circumstances** - Obtain and inspect evidence showing that documents are reviewed following any changes to the essential functions, or changes to the threats faced by those functions. (A#5)
5. **Failsafe measures** - Discuss with the organisation what failsafe measures they have implemented to ensure systems remain secure in scenarios where policies, procedures and processes are not followed. Obtain evidence of the design and implementation of those failsafes. (A#6)

Suggested documentation – Partially Achieved

- policies, processes and procedures relevant to security governance, risk management, technical security and regulatory compliance.
- evidence of policies, processes and procedures being updated following major cyber security incidents and data breaches.

Additional documentation – Achieved

- Evidence of key information governance and cyber security principles being considered.
- Evidence of mapping policies, processes and procedures to essential functions and technologies.
- Evidence of assessing applicability of policies, processes and procedures to staff groups.
- Evidence of key performance indicators (KPI) reporting to executive management.
- Evidence of regular review of documentation.
- Evidence of review of documentation following any changes to the essential functions, or changes to the threats faced by those functions.
- Evidence of design and implementation of failsafe measures.

Outcome B1.b – Policy, process and procedure implementation

Description

You have successfully implemented your information assurance policies, processes and procedures and can demonstrate the benefits achieved.

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. Policies, processes and procedures are ignored or only partially followed. NA#2. How your policies, processes and procedures support the resilience of your essential function(s) is not well understood. NA#3. Staff are unaware of their responsibilities under your policies, processes and procedures. NA#4. You do not attempt to detect breaches of policies, processes and procedures. NA#5. Policies, processes and procedures lack integration with other organisational policies, processes and procedures. NA#6. Your policies, processes and procedures are not well communicated across your organisation.	PA#1. Most of your policies, processes and procedures are followed and their application is monitored. PA#2. Your policies, processes and procedures are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness. PA#3. All staff are aware of their responsibilities under your policies, processes and procedures. PA#4. All breaches of policies, processes and procedures with the potential to adversely impact the essential function(s) are fully	A#1. All your policies, processes and procedures are followed, their correct application and effectiveness is evaluated. A#2. Your policies, processes and procedures are integrated with other organisational policies, processes and procedures, including HR assessments of individuals' trustworthiness. A#3. Your policies, processes and procedures are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities. A#4. Appropriate action is taken to address all breaches of policies,

	investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address.	processes and procedures with potential to adversely impact the essential function including aggregated breaches.

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 provide 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 of the application of policies, processes and procedures** - Ascertain what activities the organisation performs, such as spot checks and/or KPIs, to monitor the application of their policies, processes and procedures. Verify that the organisation has appropriate assurance that most are being followed. (PA#1)
2. **Policies, processes and procedures integration** - Discuss with the organisation how it has ensured its policies, processes and procedures related to information assurance are aligned with those from separate disciplines such as HR. Obtain and inspect documents to confirm that, where appropriate, they are cross-referenced and aligned in terms of their content. (PA#2, A#2)
3. **Staff awareness** - Discuss with the organisation how it makes all staff aware of their responsibilities under the organisation's policies, processes and procedures. (IGP PA#3)
4. **Investigation of breaches** - Discuss with management the investigation process for breaches of policies, processes and procedures with the potential to adversely impact the essential functions, and obtain evidence that this process is followed adequately. (PA#4)
5. **Breach tracking and remediation** - Assess the process for tracking and assessing other breaches of policies, processes and procedures that do not have the potential to adversely impact the essential functions, and verify that action is taken to address the risk created by those breaches. Obtain evidence that this process is followed adequately. (PA#4)

Additional approach to testing – Achieved

1. **Evaluating the application of policies, processes and procedures** – In additional to the checks outlined in step 1 of "partially achieved", verify that the organisation has assurance that all policies, processes and procedures are being followed. Also obtain evidence that the organisation uses its monitoring activities to make its policies, processes and procedures more effective. (A#1)
2. **Communication to staff** - Verify that the organisation has considered which policies, processes and procedures apply to which staff groups, and tailored their approach to effectively communicate the associated responsibilities to each group. Obtain evidence to show that staff at all levels of the organisation are aware of their responsibilities, for example by meeting with a sample of staff and enquiring of their understanding of their responsibilities. (A#3)
3. **Remediation of aggregated breaches** - In addition to the checks outlined in steps 4 and 5 of Partially achieved, verify that the organisation has a scheduled or efficiently

reactive process for reviewing sets of policy, process and procedure violations with a view to identifying patterns and acting upon its findings. (A#4)

Suggested documentation – Partially achieved

- Evidence of monitoring of the application of policies, processes and procedures.
- Evidence of integration between the policies, processes and procedures of different teams and departments.
- Evidence showing how staff are made aware of policies, processes and procedures.
- Investigation process for breaches of policies, processes and procedures, and evidence that the process is followed.
- Process for tracking and assessing breaches of policies, processes and procedures, and evidence that the process is followed.

Additional documentation – Achieved

- Evidence of monitoring activities being used to improve policies, processes and procedures.
- Evidence of successful segmented communication approach to staff members.
- Evidence of analysis and remediation of aggregated breaches.

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

Contributing outcome B2.a – Identity verification, authentication and authorisation

Contributing outcome B2.b – Device management

Contributing outcome B2.c - Privileged user management

Contributing outcome B2.d - Identity and access management (IdAM)

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	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	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.

does not follow up to date best practice.	have access to essential function(s) information, systems and 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	A#4. You use additional authentication mechanisms, such as multi-factor 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.

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 (CAF).

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:
    c) understands, documents, risk-assesses, and internally approves (at board level or as delegated) all exceptions, with annual review
    c) 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 Partially achieved, approach to testing, obtain documentation which outlines the different roles which require higher levels of verification for example 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. (A#4)

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. (A#4)

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. (A#4)

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)

e) 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)

4. **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 6 months. (A#5)

Suggested documentation – Mandatory policy requirement

- Evidence of authentication controls in place for user access to systems
- Procedures for application of MFA
- 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

Outcome B2.b – Device management

Description

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).

The expectation for this contributing outcome is **Not 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. Users can connect to your network and information systems supporting your essential function(s) using devices that are not corporately owned and managed. NA#2. Privileged users can perform privileged operations from devices that are not corporately owned and managed. NA#3. You have not gained assurance in the security of any third-party devices or networks connected to your systems. NA#4. Physically connecting a device to your network and information systems gives that device access without device or user authentication.	PA#1. Only corporately owned and managed devices can access your essential function(s) networks and information systems. PA#2. All privileged operations are performed from corporately owned and managed devices. These devices provide sufficient separation, using a risk-based approach, from the activities of standard users. 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	A#1. All privileged operations performed on your network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations. A#2. You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your network and information systems, or you only allow third-party devices or networks that are dedicated to supporting your network and information systems to connect. A#3. You perform certificate-based device identity management and only allow known devices

any risks identified.

PA#4. The act of connecting to a network port or cable does not grant access to any systems.

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

to access systems necessary for the operation of your essential function(s).

A#4. You perform regular scans to detect unknown devices and investigate any findings.

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 provide 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. **Device access to network and information systems** - Assess what procedural and technical controls the organisation has in place to ensure that only corporately owned and managed devices can access essential functions networks and information systems. (PA#1)
2. **Privileged operations** - Verify that "privileged operations" have been appropriately defined in the context of activities performed on the organisation's systems and networks, and that technical and procedural controls have been implemented to ensure these are only performed from corporately owned and managed devices. Obtain evidence that these devices have been configured and protected for privileged operations. (PA#2)
3. **Third-party devices** - Discuss with the organisation what security checks they perform on third-party devices before they are allowed to connect to the organisation's network. Verify that the checks are sufficient to minimise the risks associated with those third-party devices identified by the organisation. (PA#3)
4. **Physical connections** - Discuss with management whether there are technical controls in place to ensure that physical connections, for example via network port or cable, do not grant access to any systems, and require additional authentication for access to be granted. Obtain evidence that those controls are implemented as part of the default build of devices. (PA#4)
5. **Investigation of unknown devices** - Verify that the organisation is able to detect unknown devices on its network, such as through network scanning, and deploys this capability where it identifies a need. (PA#5, A#4)

Additional approach to testing – Achieved

1. **Highly trusted devices** – In addition to the controls assessed in step 2 of Partially achieved, check that the organisation has satisfied that the privileged devices should not be used for any other activity outside the privileged operations they are protected and configured for. Assess that appropriate technical and physical security controls secure those devices to ensure that only privileged users are able to access and use them. Test a sample of those controls to ensure they give appropriate security assurance. (A#1)
2. **Independent or professional assurance** - Assess whether the organisation obtains independent and professional assurance of the security of third-party devices or networks before they connect to the organisation's network and information systems, and obtain the latest assurance documentation. Alternatively, assess what technical and procedural controls are in place to ensure that the only third-party devices that are able to connect to the organisation's network are ones used for specifically

designated functions supporting networks and information systems and nothing else. Verify that the controls are appropriate. (A#2)

3. **Certificate-based identity** - Discuss with the organisation whether they have implemented certificate-based identity management, and assess their encryption methods to ensure that it is robust and tamper-proof. (A#3)
4. **Regular network scanning** - Discuss with management whether network scans take place regularly. Obtain evidence of such scans, and verify that investigations of unknown devices take place. (A#4)

Suggested documentation – Partially Achieved

- Procedural and technical controls for limiting network and system access to corporate devices.
- Procedures for privileged operations.
- Approach to validating the security properties of third-party devices.
- Evidence of risk assessment of third-party devices.
- Evidence of technical controls in place to ensure that physical connections do not grant access to any systems.
- Evidence of network scans identifying unknown devices and investigation of the unknown device.

Additional documentation – Achieved

- Latest independent or professional assurance documentation.
- Procedural and technical controls for limiting network and system third-party device access to those dedicated to specific functions.
- Evidence of certificate-based identity management implementation.
- Procedures for regular network scanning.

Outcome B2.c – Privileged user management

Description

You closely manage privileged user access to networks and information systems supporting your essential function(s).

The expectation for this contributing outcome is **Not 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. The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration, etc) supporting your essential function(s) are not known or not managed.	PA#1. All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor authentication (MFA).	A#1. Privileged user access to network and information systems supporting your essential function(s) is carried out from dedicated separate accounts that are closely monitored and managed.
NA#2. Privileged user access to network and information systems supporting your essential function(s) is via weak authentication mechanisms for example the use of simple passwords only.	PA#2. The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are known and managed. This includes third parties.	A#2. The issuing of temporary, time-bound rights for privileged user access and external third-party support access is in place.
NA#3. The list of privileged users has not been reviewed recently for example within the last 12 months.	PA#3. Activity by privileged users is routinely reviewed and validated (for	A#3. Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.
NA#4. Privileged user access is granted on a system-wide basis rather than by role or function.		A#4. All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.

NA#5. Privileged user access to your essential function(s) is via generic, shared or default name accounts. NA#6. Where there are “always on” terminals which can perform privileged actions (such as in a control room), there are no additional controls (such as physical controls) to ensure access is appropriately restricted. NA#7. There is no logical separation between roles that an individual may have and hence the actions they perform. (For example, access to corporate email and privilege user actions).	example at least annually). PA#4. Privileged users are only granted specific privileged user access rights which are essential to their business role or function.

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 provide 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. **Strong authentication** - Assess whether the organisation has implemented multi-factor authentication, or another form of strong authentication such as hardware token or biometric tools, for privileged user access to network and information systems supporting essential functions. Obtain evidence of the implementation of this technology. (PA#1)
2. **Identities of privileged users** - Assess the methodology for identifying privileged users with access to networks and information systems supporting essential functions, including third-parties. Verify that the organisation's procedures, and agreements with suppliers where appropriate, prevent anyone having privileged access without being individually identified. (PA#2)
3. **Review of privileged user activity** - Verify that "privileged user activity" has been appropriately defined in the context of activities performed on the organisation's systems and networks. Discuss with management whether there is a process in place for reviewing privileged user activity, and assess whether this process includes all privileged users, whether the frequency of reviews is clearly defined, and whether suspicious activity is investigated. Obtain evidence that this process is followed, and investigation of suspicious activity takes place. (PA#3)
4. **Privileged access rights process** - Assess the process for granting privileged access rights to users. Verify that the organisation can determine which specific privileged access rights are needed for which privileged roles and functions based on business need. Obtain evidence of privileged access requests and assess whether they were adequately reviewed and approved according to the process. (PA#4)

Additional approach to testing – Achieved

1. **Dedicated account for privileged activity** - Assess whether privileged users are required to use a dedicated separate account to access network and information systems supporting essential functions. Obtain evidence to show that these accounts are closely monitored and managed. (A#1)
2. **Time-bound rights** - Assess whether the organisation has reasonably defined scenarios where time-bound rights for privileged access should be granted over permanent rights. Assess whether there are procedural and technical controls in place that ensure these rights are issued in scenarios that meet the criteria. Obtain a list of privileged user and third-parties that have met the criteria and pick a sample to test whether these controls are effectively implemented. (A#2)
3. **Joiners, movers, leavers** - Discuss the joiners, movers, leavers process with management and assess whether privileged user access is reviewed and updated

when a user joins, moves or leaves the organisation. Obtain a list of privileged users and verify that any change in circumstances triggers a review of access rights. (A#3)

4. **Analysis of privileged user activity** – In addition to the controls assessed in step 3 of Partially achieved, assess the organisation's procedures for monitoring, reviewing and validating privileged user activity should cover all privileged user activity and happen on an ongoing basis, allowing any suspicious actions to be quickly identified and investigated regardless of when they occur. Obtain evidence of how the organisation achieves this. (A#4)

Suggested documentation – Partially Achieved

- Evidence of implementation of multi-factor authentication, or another form of strong authentication.
- Procedures to identify and manage privileged user identities.
- Evidence of reviews of privileged user activity, including investigation of suspicious activity.
- Procedures for segmenting privileged access rights by individual roles and business need.

Additional documentation – Achieved

- Evidence of dedicated accounts for privileged operations which are closely monitored and managed.
- Procedure for issuing temporary, time-bound privileged access rights.
- Joiners, movers, leavers process.
- Evidence of ongoing review and validation of privileged user activity, including investigation of suspicious activity.

NHS England

Outcome B2.d – Identity and access management (IdAM)

Description

You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems 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. Greater rights are granted than necessary. NA#2. Identity validation and requirement for access of a user, device or systems is not carried out. NA#3. User access rights are not reviewed when users change roles. NA#4. User access rights remain active when users leave your organisation. NA#5. Access rights granted to devices or systems to access other devices and systems are not reviewed on a regular basis (at least annually). NA#6. When issues are raised about staff not having appropriate access to information, these are not promptly resolved.	PA#1. You follow a robust procedure to verify each user and issue the minimum required access rights. PA#2. You regularly review access rights and those no longer needed are revoked. PA#3. User access rights are reviewed when users change roles via your joiners, leavers and movers process. PA#4. All user, device and system access to the systems supporting the essential function(s) is logged and monitored, but it is not compared to other log data or access records. PA#5. When issues are raised about staff	A#1. You follow a robust procedure to verify each user and issue the minimum required access rights, and the application of the procedure is regularly audited. A#2. User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually. A#3. All user, device and systems access to the systems supporting the essential function(s) is logged and monitored. A#4. You regularly review access logs and correlate this data with other access records and expected activity. A#5. Attempts by unauthorised users, devices or systems to

	not having appropriate access to information, these are resolved without undue delay.	connect to the systems supporting the essential function(s) are alerted, promptly assessed and investigated. A#6. When issues are raised about staff not having appropriate access to information, these are resolved without undue delay.

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 provide 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. **Minimum required access rights -** Assess whether the organisation has defined minimum required access rights for different user groups. Ascertain whether there is a procedure in place to verify each new user's identity and issue them with minimum access rights according to their role. Obtain evidence that the procedure is implemented and followed. (PA#1)
2. **User access right review** - Assess whether user access rights are reviewed regularly, with the expected frequency of review being clearly documented, and also when users change roles via the joiners, leavers and movers process. Obtain evidence that user access rights are reviewed regularly and when users change roles, and that access rights are updated as required. (PA#2, PA#3, A#2)
3. **Logging of user, device and system access** - Assess the organisation's capability to log all user, device and system access to the systems supporting the essential functions. Obtain evidence that the log is monitored regularly, with suspicious activity being investigated. (PA#4, A#3)
4. **Resolution of access issues** - Discuss with the organisation the process for raising and resolving issues about staff not having appropriate access to information (either too much access, or too little access), and whether this process includes a target timeframe for resolving the issue. Obtain the list of tickets that have been raised about staff not having appropriate access to information, and inspect a sample to verify whether the target timeframe was met. (PA#5, A#6)

Additional approach to testing – Achieved

1. **Auditing of minimum access rights** – In addition to the controls assessed in step 1 of Partially achieved, assess whether the procedure approach to testing is regularly audited by the organisation, and obtain evidence of this audit taking place, with resulting actions being implemented. (A#1)
2. **Correlation of log data** - Assess whether user, device and system access logs are correlated with log data for their other activities on the system. Obtain evidence of this correlation and analysis taking place. (A#4)
3. **Unauthorised access alert and investigation** - Discuss with management if there are monitoring tools in place to alert the organisation of attempts by unauthorised users, devices or systems to connect to the systems supporting the essential functions. Obtain the list of alerts generated by this tool and use a sample to assess whether those alerts are promptly assessed by the organisation and investigated. For alerts that resulted in a true positive, obtain evidence of actions being agreed and implemented to remove and/or block access of unauthorised user. (A#5)

Suggested documentation – Partially Achieved

- Documentation of minimum access rights for different user groups.
- Procedures for verifying user identities.
- Evidence that user access rights are reviewed and updated regularly and when users change roles.
- Evidence of user, device and system access being logged, monitored regularly and investigated where appropriate.
- Procedures for raising and resolving issues relating to staff having inappropriate access to information.

Additional documentation – Achieved

- Procedures for auditing application of minimum access rights.
- Evidence of review of access logs against expected activity.
- List of unauthorised access alerts generated by the monitoring tool.
- Evidence of actions being agreed and implemented following unauthorised access alerts.

Principle B3: Data security

Description

Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of network and information systems.

Overview of the underlying Contributing outcomes

Contributing outcome B3.a – Understanding data

Contributing outcome B3.b – Data in transit

Contributing outcome B3.c - Stored data

Contributing outcome B3.d – Mobile data

Contributing outcome B3.e - Media/equipment sanitisation

Outcome B3.a – Understanding data

Description

You have a good understanding of data important to the operation of your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to 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. You have incomplete knowledge of what data is used by and produced in the operation of the essential function(s). NA#2. You have not identified the important data on which your essential function(s) relies. NA#3. You have not identified staff members with access to data important to the operation of the essential function(s). NA#4. You have not clearly articulated the impact of data compromise or inaccessibility. NA#5. Your record of processing activities (ROPA) or information asset register (IAR) or registers are incomplete or out of date. NA#6. Information asset owners and information asset	PA#1. You have identified and catalogued all the data important to the operation of the essential function(s) or that would assist an attacker. This includes maintaining a record of processing activities (ROPA) and an information asset register (IAR) which are updated whenever significant changes occur. PA#2. You have identified and catalogued who has access to the data important to the operation of the essential function(s). PA#3. You regularly review location, transmission,	A#1. You have identified and catalogued all the data important to the operation of the essential function(s), or that would assist an attacker. This includes maintaining a record of processing activities (ROPA) and an information asset register (IAR) which are reviewed and kept up to date. A#2. You have identified and catalogued who has access to the data important to the operation of the essential function(s). A#3. You maintain a current understanding of the location, quantity and quality of data important to the operation of the essential function(s). A#4. You take steps to remove or minimise unnecessary copies

administrators have not been appointed.	quantity and quality of data important to the operation of the essential function(s). PA#4. You regularly review location, transmission, quantity and quality of data important to the operation of the essential function(s). PA#5. You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data. PA#6. You occasionally validate these documented impact statements. PA#7. You have appointed information asset owners and information asset administrators.	or unneeded historic data. A#5. You have identified all mobile devices and media that may hold data important to the operation of the essential function(s). A#6. You maintain a current understanding of the data links used to transmit data that is important to your essential function(s). A#7. You understand the context, limitations and dependencies of your important data. A#8. You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data. A#9. You validate these documented impact statements regularly, at least annually. A#10. You have appointed information asset owners and information asset administrators.

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 provide 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. **ROPA and IAR** - Obtain and inspect the organisation's record of processing activities (ROPA) and an information asset register (IAR), and assess whether they contain appropriate information, and whether they are updated whenever significant changes occur. Obtain examples of updates taking place after significant changes occur.
   a) As per ICO guidance, the ROPA should include as a minimum the organisation's name and contact details, whether it is a controller or processor, the purposes of processing, description of the categories of individual and personal data, categories of recipient of personal data, details of transfers to third countries, including a record of the transfer mechanism safeguards, retention schedules and description of the technical and organisational security measures in place. (PA#1, A#1)
   b) As per ICO guidance, the IAR should include as a minimum the software and hardware assets of the organisation, asset owners, asset location, retention periods and security measures deployed. (PA#1, A#1)
   c) From the ROPA and IAR, and through discussion with management, assess whether information asset owners and information asset administrators have been appointed. (PA#7, A#10)
2. **Other data important to essential functions** - Assess whether, either as an addition to the IAR or as a separate document, the organisation has catalogued, documented and maintained up-to-date information about the location and security arrangements of other data supporting the essential functions, including:
   a) Operational data (such as finance data); (PA#1, A#1)
   b) Technical data; (PA#1, A#1)
   c) Security impacting data (such as network and system designs). (PA#1, A#1)
3. **Access to data** - In documents provided for steps 1 and 2, assess whether individuals or staff groups with access to this data are identified and catalogued. (PA#2, A#2)
4. **Data reviews** - Obtain evidence to show that, where it is practical and appropriate to do so, the data identified in documents provided for steps 1 and 2 is monitored, with scheduled or efficiently reactive reviews taking place to verify the location, transmission, quantity and quality of the data. (PA#3)
5. **Mobile devices and media** - In documents provided for steps 1 and 2, assess whether mobile devices and media that hold data important to the operation of the essential functions have been identified. (PA#4, A#5)
6. **Scenario impact on essential functions** - Establish whether impacts on the essential functions of unauthorised data access, modification or deletion have been documented for data assets catalogued in steps 1 and 2. (PA#5, A#8)

7. **Validating impact** - Obtain evidence that reviews have taken place at suitable intervals to confirm whether the scenario impacts identified by the organisation in step 5 remain valid, and that updates have been made where scenario impacts were found to be inaccurate. (PA#6)

Additional approach to testing – Achieved

1. **ROPA and IAR reviews** - In addition to the approach to testing in step 1 of Partially achieved, verify that the ROPA and IAR are reviewed on a regular basis, and obtain evidence of such reviews. (A#1)
2. **Understanding of the location, quantity and quality of data** - In addition to the controls assessed in step 4 of Partially achieved, verify that the organisation's reviews are systematic and ongoing, such that any changes to location, transmission, quantity and quality of data are quickly identified and updates made to associated documentation. (A#3)
3. **Copies and historic data** - Establish how the organisation monitors the existence of copies and historic data, and assess this process to identify any gaps. Obtain evidence that this process includes removing or minimising unnecessary copies or unneeded historic data, and obtain evidence that this activity takes place regularly. (A#4)
4. **Data links** - Establish how the organisation monitors the data links used to transmit data that is important to essential functions, and assess whether the process has controls in place to be warned of changes in the data links, supporting the maintenance of a current understanding of those links. (A#6)
5. **Context, limitations and dependencies of important data** - Assess whether the documentation provided by the organisation for steps 1 and 2 of Partially achieved, identifies dependencies of all catalogued data, and gives adequate context of how the data supports the organisation's essential functions. Verify that the organisation has identified the areas of documents provided for steps 1 and 2 of Partially achieved, where there are limitations to the data, for example where the organisation has indicated on an appropriate register that it holds network schematics, but also documents that it knows these schematics to be out of date due to a recent office move. (A#7)
6. **Regularly validating impact** - In addition to activities outlined in step 7 of Partially achieved, verify that scenario impacts are validated on an annual basis at minimum. (A#9)

Suggested documentation – Partially Achieved

- Record of processing activities (ROPA) and an information asset register (IAR).
- Evidence of updates to the ROPA and IAR after significant changes.
- Documentation cataloguing other data important to essential functions (held as part of the IAR or separately).
- Evidence of individuals or staff groups with access to essential functions data being identified.
- Evidence of essential functions data being monitored to verify location, transmission, quantity and quality.
- Evidence of mobile devices and media being identified in essential functions data.
- Documentation of scenario impacts of unauthorised data access, modification or deletion on essential functions.
- Evidence of occasional reviews to validate scenario impacts.

Additional documentation – Achieved

- Evidence of regular review of the ROPA and IAR.
- Evidence of essential functions data being monitored on a systematic and ongoing basis to verify location, transmission, quantity and quality.
- Evidence of monitoring of copies and historical data, followed by minimisation and removal where appropriate.
- Procedures for monitoring data links.
- Evidence of context, limitations and dependencies of essential functions data being identified and understood.
- Evidence of regular reviews to validate scenario impacts.

Outcome B3.b – Data in transit

Description

You have protected the transit of data important to the operation of your essential function(s). This includes the transfer of data to third parties.

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 all your data links are, or which carry data important to the operation of the essential function(s). NA#2. Data important to the operation of the essential function(s) travels without technical protection over non-trusted or openly accessible carriers. NA#3. Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.	PA#1. You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s). PA#2. You apply appropriate technical means (such as cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.	A#1. You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s). A#2. You apply appropriate physical and / or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied. A#3. Suitable alternative transmission paths are available where there is a significant risk of impact on the operation of the essential function(s) due to resource limitation (for example transmission equipment or function failure, or important data being blocked or jammed).

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 provide 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. **Identification of data links** – Verify that the organisation has identified all the data links that carry data important to the operation of essential functions. These should include:
   a) Physical communications (such as sending confidential patient information by mail); (PA#1, A#1)
   b) Electronic information transfers (such as email and automated transmissions); (PA#1, A#1)
   c) Network traffic between end user devices, infrastructure devices and servers. (PA#1, A#1)
2. **Protecting data links** - Assess whether proportionate security measures have been implemented and documented for each data link identified in step 1. Obtain evidence to show that these security measures are effective. (PA#1, A#1)
3. **Non-trusted or openly accessible carriers** - Establish with the organisation whether it has identified the data flows that travel over non-trusted or openly accessible carriers, and whether it has implemented appropriate technical means (for example cryptography for electronic information, securely packaging post for physical information) to protect this data. (PA#2)

Additional approach to testing – Achieved

1. **Testing technical measures** - In addition to the controls assessed in step 2 of Partially achieved, obtain evidence that the organisation has tested its technical measures for protecting data that travels over non-trusted or openly accessible carriers, and assess the confidence that the organisation has in their robustness. (A#2)
2. **Alternative transmission paths** - Establish with management whether it has identified and assessed the risk of resource limitation on important data flows, and whether it has put in place suitable alternative transmission paths where a significant risk of impact on the operation of essential functions was identified. (A#3)

Suggested documentation – Partially Achieved

- Documentation identifying important data links and security measures to protect them.
- Documentation identifying data flows that travel over non-trusted or openly accessible carriers.
- Evidence of technical measures to protect data that travels over non-trusted or openly accessible carriers.

Additional documentation – Achieved

- Evidence of testing technical measures for protecting data that travels over non-trusted or openly accessible carriers.
- Documentation identifying critical transmission paths, dependencies and suitable alternatives.

Outcome B3.c – Stored data

Description

You have protected stored soft and hard copy data important to 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. You have no, or limited, knowledge of where data important to the operation of the essential function(s) is stored. NA#2. You have not protected vulnerable stored data important to the operation of the essential function(s) in a suitable way. NA#3. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	PA#1. All copies of data important to the operation of your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy. PA#2. You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion. PA#3. If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.	A#1. All copies of data important to the operation of your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy. A#2. You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion. A#3. If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied. A#4. You have suitable, secured backups of data to allow the operation of the essential function(s) to continue should the

PA#4. You have suitable, secured backups of data to allow the operation of the essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.

original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.

A#5. Necessary historic or archive data is suitably secured in storage, which may include off-site archives.

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 provide 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. **Documenting stored data** - Verify that the organisation has documented data it holds (both physical and electronic) which supports the operation of its essential functions. Where the same data is held in multiple locations or on multiple systems, establish whether the organisation has a legitimate business need for doing so. (PA#1, A#1)
2. **Data on less secure systems** - Verify the organisation has defined reasonable criteria for designating less secure systems, and identified systems which fall under this category. If any of these systems store data which is important to the operation of essential functions, obtain evidence of procedural or technical controls in place to ensure the data is provided with limited detail or as read-only copies. Test a sample of data on less secure systems to check the controls are effectively implemented. (PA#1, A#1)
3. **Protecting data** - Establish with the organisation what physical and technical controls are in place to protect stored data identified in step 1 from unauthorised access, modification or deletion. Assess whether the controls are suitable and proportionate. (PA#2, A#2)
4. **Cryptographic protections** - Establish whether cryptographic protections are used for data identified in step 1 and obtain evidence that they have been technically and procedurally applied in a suitable way to protect the data. (PA#3)
5. **Backup copies of data** - Discuss with the organisation whether they have backups of data to allow the operation of essential functions to continue should the original data not be available, which may include offline or segregated backups, or appropriate alternative forms of the data such as paper copies. Assess the suitability of the backup copies of data, and security measures to ensure these would be operational in the event that original data copies were compromised. (PA#4, A#4)

Additional approach to testing – Achieved

1. **Testing of cryptographic protections** – In addition to the controls assessed in step 4 of Partially achieved, obtain evidence to show that the cryptographic protections have been tested, giving the organisation justified confidence in the robustness of the protection applied. (A#3)
2. **Archive storage** - Assess how necessary historic or archive data is stored, and whether suitable security measures are implemented, for example, off-site storage. Obtain evidence of those security measures. (A#5)

Suggested documentation – Partially Achieved

- Documentation identifying stored data (both physical and electronic).
- Identification of a business need where the same data is stored in more than one location or system.
- Documentation identifying the organisation’s less secure systems.
- Evidence of data being held with limited detail or in read-only form on less secure systems.
- Physical and technical controls to protect important stored data from unauthorised access, modification or deletion.
- Evidence of cryptographical protections and their procedural and technical application.
- Evidence of suitable back-up copies of important data.

Additional documentation – Achieved

- Evidence of testing of cryptographic protections.
- Evidence of historic or archive data being securely stored.

Outcome B3.d – Mobile data

Description

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

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

Indicators of good practice (IGP) achievement levels

Not Achieved	**Partially Achieved**	**Achieved**
At least one of the following is true:	All the following statements are true:	All the following statements are true:
NA#1. You don’t know which mobile devices may hold data important to the operation of the essential function(s). NA#2. You allow data important to the operation of the essential function(s) to be stored on devices not managed by your organisation, or to at least equivalent standard. NA#3. Data on mobile devices is not technically secured, or only some is secured.	PA#1. You know which mobile devices hold data important to the operation of the essential function(s). PA#2. Data important to the operation of the essential function(s) is stored on mobile devices only when they have at least the security standard aligned to your overarching security policies. PA#3. Data on mobile devices is technically secured.	A#1. Mobile devices that hold data that is important to the operation of the essential function(s) are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place. A#2. Your organisation can remotely wipe all mobile devices holding data important to the operation of essential function(s). A#3. You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

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 provide 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. **Data held in mobile devices** - Verify that the organisation has documented which mobile devices (or groups of devices) hold data important to the operation of essential functions. (PA#1)
2. **Security requirements for mobile data** - Verify that the organisation has established procedures for ensuring that before important data is accessed or stored via mobile devices, the mobile devices must have met the standard of the organisation’s overarching security policies. Obtain evidence of how this procedure is practically applied. (PA#2)
3. **Technical security** - Establish with the organisation whether there are a minimum set of technical security controls which must be applied to all mobile devices before important data can be accessed or stored on them. Obtain a sample of mobile devices and verify that the controls have been applied. (PA#3)

Additional approach to testing – Achieved

1. **Management of mobile devices** – In addition to the controls assessed in step 1 of Partially achieved, verify that all mobile devices holding important data are corporately owned or managed. (A#1)
2. **Configuration, policies and procedures** - Obtain evidence of the configurations applied to different categories of mobile devices holding important data, and verify the criteria the organisation has used to determine that the configurations represent best practice for each respective mobile device platform. Verify that the configurations are bolstered by technical and procedural policies to further protect mobile data. (A#1)
3. **Remote wiping** - Establish whether the organisation can remotely wipe any mobile device holding data important to the operation of essential functions if it is lost. Obtain evidence that this capability is effectively used following staff reports of lost mobile devices. (A#2)
4. **Minimising mobile data** - Verify that the organisation has agreed and documented principles to minimise the amount of data being held on each category of mobile devices. Assess whether the organisation’s technical and procedural controls for mobile devices effectively enforce the agreed principles to ensure that the minimal amount of data is accessible or stored on a mobile device, which may include automatic deletion of data where appropriate. (A#3)

Suggested documentation – Partially Achieved

- Documentation of mobile devices holding data important to the operation of essential functions.
- Procedures for ensuring mobile devices meet security policy standards ahead of accessing or storing important data.
- Evidence of a minimum set of technical security controls being applied to mobile devices.

Additional documentation – Achieved

- Evidence of all mobile devices holding important data being corporately owned or managed.
- Evidence of configurations and policies for protecting mobile data on different platforms.
- Procedures for performing remote wiping of mobile devices.
- Procedures for minimising data on mobile devices.

Outcome B3.e – Media/equipment sanitisation

Description

Before re-use and / or disposal you appropriately sanitise devices, equipment and removable media holding data important to 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. Some or all devices, equipment or removable media that hold data important to the operation of the essential function(s) are disposed of without sanitisation of that data.	PA#1. Data important to the operation of the essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal.	A#1. You catalogue and track all devices that contain data important to the operation of the essential function(s) (whether a specific storage device or one with integral storage). A#2. Data important to the operation of the essential function is removed from all devices, equipment or removable media before reuse and / or disposal using an assured product or service.

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 provide 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. **Data removal** - Establish whether there are established procedures for sanitising all devices, equipment and removable media holding essential functions data before reuse and/or disposal. Obtain evidence that the procedures are followed by the organisation. (PA#1)

Additional approach to testing – Achieved

1. **Identifying and documenting devices** - Verify that the organisation has identified and documented all devices that contain data important to the operation of essential functions, including removable media assets. Assess whether the documentation includes key information such as the owner of the device, its location and the type of data contained on the device. (A#1)
2. **Assured data removal** – In addition to the activities detailed in step 1 of Partially achieved, obtain evidence that the pre activities undertaken are carried out by an assured product or service. (A#2)

Suggested documentation – Partially Achieved

- Procedures for sanitising all devices, equipment and removable media holding essential functions data before reuse and/or disposal.

Additional documentation – Achieved

- Documentation identifying all devices, including storage devices, holding essential functions data.
- Evidence of the use of an assured product or service for media sanitisation.

Principle B4: System security

Description

Network and information systems and technology critical for the operation of essential functions are protected from cyber-attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

Overview of the underlying Contributing outcomes

Contributing outcome B4.a – Secure by design

Contributing outcome B4.b – Secure configuration

Contributing outcome B4.c - Secure management

Contributing outcome B4.d - Vulnerability management

Outcome B4.a – Secure by design

Description

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 function(s) should not be impacted by the exploitation of any single vulnerability.

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. Systems essential to the operation of the essential function(s) are not appropriately segregated from other systems.	PA#1. You employ appropriate expertise to design network and information systems.	A#1. You employ appropriate expertise to design network and information systems.
NA#2. Internet access is available without restriction or business need from network and information systems supporting your essential function(s).	PA#2. You design strong boundary defences where your networks and information systems interface with other organisations or the world at large.	A#2. Your network and information systems are segregated into appropriate security zones (for example systems supporting the essential function(s)are segregated in a highly trusted, more secure zone).
NA#3. Data flows between the network and information systems supporting your essential function(s)and other systems are complex, making it hard to discriminate between legitimate and illegitimate / malicious traffic.	PA#3. You design simple data flows between your networks and information systems and any external interface to enable effective monitoring.	A#3. The networks and information systems supporting your essential function(s) are designed to have simple data flows between components to support effective security monitoring.
NA#4. Remote or third-party accesses circumvent some network controls to gain more direct access to network and information systems supporting the essential function(s).	PA#4. You design to make network and information system recovery simple.	A#4. The networks and information systems supporting your essential function(s) are designed to be easy to recover.
	PA#5. All inputs to network and	

	information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	A#5.	Content-based attacks are mitigated for all inputs to network and information systems that affect the essential function(s) (for example via transformation and inspection).

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 provide 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. **Expertise in network design** - Obtain evidence of how the organisation's network and information systems have been designed. Verify that appropriate deliberate design choices have been made, employing cyber security expertise, to make the network less vulnerable to compromise and easier to recover in the event of an incident. (PA#1, A#1)
2. **Boundary defences** - Obtain the network architecture documentation. Assess whether, for each point where the organisation's networks and information systems interface with other organisations or the world at large, there is a technical solution in place (such as a firewall, authentication protocol, intrusion detection or prevention system) which blocks unapproved connections, manages access and validates message format and content. (PA#2)
3. **Simple data flow** - Obtain evidence that the organisation has designed data flows between its network and any external interfaces in a way which enables it to easily validate message format and content. (PA#3)
4. **Complexity of recovery** - Obtain evidence of deliberate design decisions the organisation has made whilst building and developing their network to simplify recovery processes. Verify that the organisation's design decisions reasonably contribute towards simpler, faster or less resource-intensive recovery of their systems. (PA#4, A#4)
5. **Boundary network protocols** - In addition to step 2, verify that the organisation's technical solutions automatically check and validate all inputs to network and information systems supporting essential functions wherever practically possible. Alternatively, assess whether monitoring is in place for content-based attacks aimed at network and information systems supporting essential functions. (PA#5)

Additional approach to testing – Achieved

1. **Security zones** - Obtain evidence that the organisation's network has been designed with the segregation principle in mind, dividing their networks and systems into zones according to the security requirements of the assets within them. The organisation should have:
   a) Undertaken a risk analysis to determine the criticality and security considerations of assets in each zone (A#2)
   b) Implemented technical and physical solutions in each zone according to the security considerations and requirements of the assets (A#2)
   c) Deployed their most critical assets in their most secure network zones, such that if other areas of the network were impacted, those assets could continue to be secure and in operation. (A#2)

2. **Simple internal data flow** - In addition to step 3 of Partially achieved, verify that the organisation has designed simple data flows within and between internal systems. (A#3)
3. **Content-based attacks** - Assess whether the organisation has controls that effectively mitigate content-based attacks irrespective of source, and do not rely only on monitoring or control only at the network perimeter. Obtain evidence of the effectiveness of those controls. (A#5)

Suggested documentation – Partially Achieved

- Network architecture documentation.
- Evidence of deliberate design choices to make the network less vulnerable to compromise and easier to recover.
- Evidence of boundary defences in place.
- Data flow mapping.
- Sample of monitoring report or dashboards.
- Evidence of deliberate design choices to simplify recovery process.
- Evidence of automatic checking and validation of all inputs to important networks and information systems.
- Evidence of monitoring in place for content-based attacks.

Additional documentation – Achieved

- Security zone risk analysis.
- Evidence of technical and physical solutions being applied proportionately to zone security levels.
- Evidence of boundary protection solutions being applied proportionately to data flow sources.
- Evidence of controls for mitigating content-based attacks.

Outcome B4.b – Secure configuration

Description

You securely configure the network and information systems that support 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. You haven't identified the assets that need to be carefully configured to maintain the security of the essential function(s). NA#2. Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential function(s). NA#3. Configuration details are not recorded or lack enough information to be able to rebuild the system or device. NA#4. The recording of security changes or adjustments that effect your essential function(s) is lacking or inconsistent. NA#5. Generic, shared, default name and built-in accounts have not been removed or disabled.	PA#1. You have identified and documented the assets that need to be carefully configured to maintain the security of the essential function(s). PA#2. Secure platform and device builds are used across the estate. PA#3. Consistent, secure and minimal system and device configurations are applied across the same types of environment. PA#4. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential function are approved and documented.	A#1. You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the essential function(s). For example, maintain security configurations, patching, updating according to good practice. A#2. All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment. A#3. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. A#4. You regularly review and validate that your network and information systems have the expected,

	PA#5. You verify software before installation is permitted. PA#6. Generic, shared, default name and built in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.	secured settings and configuration. A#5. Only permitted software can be installed. A#6. Standard users are not able to change settings that would impact security or the business operation. A#7. If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated. A#8. Generic, shared, default name and built in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.

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 provide 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. **Asset configuration** - Inspect documentation relevant to how the organisation configures its assets. Assess whether:
   a) The organisation has identified **the** assets **for which configuration profiles need to be created to maintain** the security of its essential functions. (PA#1)
   b) The organisation has documented appropriate configuration profiles for those assets, ensuring consistent configurations are used across similar environments. (PA#3)
2. **Applying configurations to assets** - Obtain a sample of the organisation's assets and verify that the configurations profiles documented in step 1 have been correctly applied. (PA#3)
3. **Secure builds** - Assess whether the organisation has defined and documented a collection of secure baseline builds for different devices across its estate. From the list of platform and devices, obtain a sample to verify that the builds, though not necessarily all matching the most up-to-date build profile, match to an approved baseline build in the organisation's documentation. (PA#2)
4. **Changes and adjustments to security configurations** - Assess whether the organisation has procedures to ensure that changes to security configurations are approved and documented. Obtain and inspect documentation related to configuration change approvals to verify the procedures are being followed. (PA#4)
5. **Software verification** - Establish whether there is a process for considering and approving software prior to permitting its installation. Obtain evidence that this process is followed. (PA#5)
6. **Removal of generic accounts** - Assess whether the organisation has identified and documented generic, shared, default name and built-in accounts used across its systems and networks. Obtain evidence that one of the following statements applies to each generic, shared, default name or built-in account:
   a) The account has been removed, disabled, or the password has been changed (PA#6, A#8)
   b) The account is robustly restricted through technical or procedural controls, such that no staff members can access or perform meaningful actions on information, systems or networks supporting essential functions without first individually identifying themselves (PA#6, A#8)

Additional approach to testing – Achieved

1. **Active configurations management** - In addition to step 1 of ‘Partially Achieved’, verify that:
   a) The organisation has a scheduled or efficiently reactive process to ensure that configuration profiles are reviewed and updated based on changes in the organisation’s environment. Obtain evidence of such changes being identified and triggering an update to configurations. (A#3)
   b) The organisation has procedures for ensuring that the latest approved configurations are applied to its assets without undue delay. (A#1)
   c) The organisation is tracking the configuration status of all configurable assets. Where the latest configuration profiles have not been applied, legitimate justifications are provided and realistic plans for future implementation are documented. Obtain a sample of the organisation’s assets and verify that the configuration status of each one matches the organisation’s documentation. (A#1)
2. **Secure builds** - In addition to step 2 of ‘Partially achieved’, verify that the organisation has procedures for ensuring that its most up-to-date baseline builds, or the latest known good configuration version for that environment, are applied to devices and platforms without undue delay. Obtain a sample of devices or platforms to verify the builds are correctly implemented. (A#2)
3. **Validation** - Establish whether there is a scheduled or efficiently reactive review schedule in place to validate that network and information systems have the expected, secured settings and configuration. Obtain evidence of this review taking place. (A#4)
4. **Allow list of software** - Establish whether the organisation has documented a list of software that can be installed, and has implemented technical controls to disable all other software from being installed. Obtain this software list and verify that only that software can be installed, for example by asking a member of staff to try to install another software. (A#5)
5. **Actions of standard users** - Establish whether the organisation has appropriately defined and documented settings which would impact security or the operation of essential functions if changed by users. Review the controls in place for standard users, and verify that they are prevented from changing such settings. (A#6)
6. **Automated decision-making** - Enquire of management and establish whether automated decision-making technologies are in use. If yes, assess the organisation’s understanding of their operation, and verify whether decisions can be replicated. Test this replication for a sample of decisions. (A#7)

Suggested documentation – Partially Achieved

- Documented configuration profiles for assets supporting the operation of essential functions.
- Evidence of operating environment being considered for configurations.
- Baseline builds for different devices.
- Procedures for approving and documenting changes to security configurations.
- Procedures for assessing the security of a software before deployment.
- Evidence of generic, shared, default name and built-in accounts being removed, disabled, password changed or robustly restricted through technical controls.

Additional documentation – Achieved

- Procedures for reviewing and updating configurations profiles based on changes in the environment.
- Procedures to applying latest configurations to assets.
- Evidence that configurations are applied to all assets, and configuration statuses tracked.
- Evidence of baseline builds being correctly applied to all devices.
- Procedures for validating application of configurations settings to devices.
- Software allow list.
- Evidence of security impacting settings changes being identified and controls implemented to prevent standard user access.
- Evidence of any automated decision-making technologies in use being understood and their decisions replicated.

Outcome B4.c – Secure management

Description

You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.

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 systems and devices supporting the operation of the essential function(s) are administered or maintained from devices that are not corporately owned and managed.	PA#1. Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from devices sufficiently separated, using a risk-based approach, from the activities of standard users.	A#1. Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.
NA#2. You do not have good or current technical documentation of your networks and information systems.	PA#2. Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.	A#2. You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.
	PA#3. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and	A#3. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

physical measures
as necessary.

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 provide 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. **Administration of systems and devices** – Obtain evidence confirming that:
   a) The organisation understands which systems and devices support the operation of essential functions. (PA#1)
   b) The organisation holds a list of authorised privileged users who hold responsibility and unique permissions for administering and maintaining systems and devices, with an approval process for new authorisations. (PA#1)
   c) Systems and devices can only be administered or maintained from devices which are sufficiently separated through technical and procedural controls from the activities of standard users. (PA#1)
2. **Technical knowledge about networks and information systems** - Obtain and inspect network diagrams and other documentation related to technical knowledge about networks and information systems, and assess whether those documents are regularly reviewed and updated. (PA#2, A#2)
3. **Malware and unauthorised software** - Assess the organisation’s technical, procedural and physical measures for identifying, investigating and removing malware or unauthorised software. Ascertain how the organisation has made their determination that the measures they have in place provide sufficient protection. (PA#3, A#3)

Additional approach to testing – Achieved

1. **Privileged Access Workstations** – In addition to step 1 of ‘Partially Achieved’, establish whether there are devices in the organisation that are dedicated to the administration or maintenance of systems and devices. Assess whether those devices are appropriately secured, with only privileged users being able to access and use them, and verify that they are solely dedicated to administration or maintenance operations. (A#1)
2. **Secure storage** - In addition to step 2 of ‘Partially Achieved’, assess how the documentation is stored, and whether it is adequately secure. Obtain evidence of this security measures in place. (A#2)

Suggested documentation – Partially Achieved

- Documentation identifying systems and devices supporting essential functions.
- List of privileged users and procedures for authorising privileged access.
- Evidence of separation of devices used for system administration and maintenance.
- Procedures for reviewing and updating network diagrams and other technical documentation relating to networks and information systems.
- Procedures and defensive measures against malware and unauthorised software.

Additional documentation – Achieved

1. Evidence of devices being specifically configured and dedicated solely to administration and maintenance operations.
2. Evidence of security measures in place for stored network diagrams and other technical documentation relating to networks and information systems.

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 promptly by patching for example. PA#3. Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.	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 promptly by patching for example. 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

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

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

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’ for the 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 B5: Resilient networks and systems

Description

The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the operation of essential functions.

Overview of the underlying Contributing outcomes

Contributing outcome B5.a – Resilience preparation

Contributing outcome B5.b – Design for resilience

Contributing outcome B5.c - Backups

Outcome B5.a – Resilience preparation

Description

You are prepared to restore the operation of your essential function(s) following adverse impact.

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 have limited understanding of all the elements that are required to restore operation of the essential function(s). NA#2. You have not completed business continuity and disaster recovery plans for network and information systems, including their dependencies, supporting the operation of the essential function(s). NA#3. You have not fully assessed the practical implementation of your business continuity and disaster recovery plans.	PA#1. You know all networks, information systems and underlying technologies that are necessary to restore the operation of the essential function(s); and understand their interdependence. PA#2. You know the order in which systems need to be recovered to efficiently and effectively restore the operation of the essential function(s).	A#1. You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, examples include, manual fail-over, table-top exercises, or red-teaming. A#2. You use your security awareness and threat intelligence sources to identify new or heightened levels of risk, which result in immediate and potentially temporary security measures to enhance the security of your network and information systems (for example in response to a widespread outbreak of very damaging malware).

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 provide 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. **Knowledge for restoring essential functions -** obtain evidence to verify that:
   a) The organisation has documented all networks, information systems and underlying technologies that are necessary to restore the operation of the essential function(s). (PA#1)
   b) The organisation has identified which essential functions are supported by which networks, information systems and underlying technologies. (PA#1)
2. **Technical understanding for bringing systems back online** - obtain evidence that the organisation understands the order in which systems within its network(s) can technically be brought back online given the interdependencies between them. (PA#2)

Additional approach to testing – Achieved

1. **Business continuity and disaster recovery plans** - inspect the organisation's business continuity and disaster recovery plans. Verify that the organisation has conducted and documented testing exercises supporting the delivery of roles and responsibilities outlined in the plans. Assess whether:
   a) The testing exercises conducted were sufficient to give the organisation assurances about the practicality, effectiveness and completeness of their business continuity and disaster recovery plans. (A#1)
   b) The test methods used were appropriate to make a robust assessment of the duties outlined in the business continuity plan and disaster recovery plans. (A#1)
2. **Heightened risk identification** - establish with management the process for leveraging the organisation's security awareness and threat intelligence sources to identify new or heightened levels of risk. Assess the reporting lines for this process to ensure that management can act quickly on new information, and assess whether the temporary security measures to be put in place have been documented for a range of scenarios. Obtain evidence from the latest identified risks showing that this process was adequately followed. (A#2)

Suggested documentation – Partially Achieved

- Documentation identifying networks, information systems and technologies necessary for restoring the operation of essential functions.
- Evidence of interdependencies between essential functions and networks, systems and technologies being identified.

Additional documentation – Achieved

- Business continuity and disaster recovery plans.
- Evidence of testing exercises conducted related to business continuity and disaster recovery plans.
- Procedures for identifying heightened levels of risk and implementing mitigating actions.

Outcome B5.b – Design for resilience

Description

You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

The expectation for this contributing outcome is **Not 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. Network and information systems supporting the operation of your essential function(s) are not appropriately segregated. NA#2. Internet services, such as browsing and email, are accessible without restriction or business need from network and information systems supporting the essential function(s). NA#3. You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function(s).	PA#1. Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (for example they reside on the same network as the rest of the organisation but within a demilitarised zone (DMZ)). Internet services are not accessible from network and information systems supporting the essential function(s) unless there is a clear business need and with appropriate restrictions. PA#2. Resource limitations (such as network	A#1. Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by appropriate technical and physical means (such as separate network and system infrastructure with independent user administration). Internet services are not accessible from network and information systems supporting the essential function(s). A#2. You have identified and mitigated all resource limitations, such as bandwidth limitations and single network paths. A#3. You have identified and mitigated any geographical constraints or weaknesses. (For example, systems that

bandwidth, single network paths) have been identified but not fully mitigated.		your essential function(s) depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers).
	A#4.	You review and update assessments of dependencies, resource and geographical limitations and mitigation's when necessary.

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 provide 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. **Asset segregation** - Obtain network architecture documentation and assess whether network and information systems supporting the operation of essential functions are logically separated from business systems, for example by locating them in a demilitarised zone (DMZ). (PA#1)
2. **Access to internet services** - For any network and information systems supporting essential functions with access to internet services, verify that:
   a) The organisation has procedures ensuring internet services are only used where there is a 'clear business need' with supporting documentation covering:
      i) acceptable use of the internet. (PA#1)
      ii) which staff member groups have a legitimate business need to access the internet. (PA#1)
      iii) how legitimate internet access is managed. (PA#1)
   b) The organisation has 'appropriate restrictions' in place, with documented solutions to:
      i) Monitor and analyse incoming and outgoing internet traffic. (PA#1)
      ii) Block or filter out harmful content. (PA#1)
      iii) Block unapproved connections. (PA#1)
      iv) Manage internet access. (PA#1)
3. **Resource limitation** - Assess whether the organisation has:
   a) Reviewed its network infrastructure and identified single points of failure which risk causing major disruption to the network if compromised, such as single network paths. (PA#2)
   b) Documented, reviewed and accepted the associated risks. (PA#2)
   c) Developed an improvement plan to upgrade networks and systems where the risk they pose exceeds the risk appetite of the organisation. (PA#2)

Additional approach to testing – Achieved

1. **Technical and physical segregation** - Obtain network architecture documentation and assess whether the organisation has applied appropriate technical and physical means to separate its networks and systems supporting essential functions from other business and external systems, for example by locating them on a separate network with independent user administration. (A#1)
2. **Remediating resource limitations** - In addition to step 2 of 'Partially achieved', assess whether the organisation has implemented actions to remediate all single points of failure identified. (A#2)

3. **Geographical constraints** - Establish whether the organisation has identified, documented and mitigated geographical constraints, such as all the organisation’s servers being in the same location. Assess whether appropriate solutions have been implemented to mitigate the associated risks. (A#3)
4. **Regular review of assessments** - Obtain evidence to show that there is a scheduled or efficiently reactive process for reviewing and updating assessments of network dependencies, resource and geographical limitations and applied mitigations. Verify that responsible owners have reviewed and updated their assigned assessments at the appropriate intervals. (A#4)

Suggested documentation – Partially Achieved

- Network architecture documentation.
- Evidence of a clear business need and restrictions being applied to networks and systems with internet access.
- Documentation identifying single points of failure, associated risks and proposed mitigations.

Additional documentation – Achieved

- Evidence of technical and physical segregation of networks supporting essential functions.
- Evidence of single points of failure being remediated.
- Evidence of geographical constraints and mitigations.
- Evidence of scheduled review process for assessments relating to network resilience.

Outcome B5.c – Backups

Description

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).

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** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function(s). NA#2. Backups are not frequent enough for the operation of your essential function(s) to be restored effectively. NA#3. Your restoration process does not restore your essential function(s) in a suitable time frame.	PA#1. You have appropriately secured backups (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event. PA#2. You routinely test backups to ensure that the backup process functions correctly and the backups are usable.	A#1. Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event. A#2. Backups of all important data and information needed to recover the essential function are made, tested, documented and routinely reviewed.

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 provide 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. **Backup plan** - obtain and inspect the organisation's procedures for backups. Assess whether they have planned for extreme event scenarios, such as a widespread hardware failure or cyber attack.
   a) Verify that the organisation's arrangements for backups ensure that backups are accessible to recover in those scenarios. (PA#1)
   b) Assess whether, in those same scenarios, the organisation would be able to access what they need to effectively utilise their backups, including data, configuration information, software, equipment, processes and knowledge. (PA#1)
2. **Backup testing** - obtain evidence that backups are tested to ensure the backup process functions correctly and the backups are usable. (PA#2)

Additional approach to testing – Achieved

1. **Procedures for backup** - verify that the organisation's back up procedures are comprehensive, supported by documentation, detailing frequency, ongoing security and maintenance, automated backups processes (which have been implemented in areas where appropriate), and the organisation's testing regime. (A#1)
2. **Secure sites** - in addition to step 1 of 'Partially achieved', establish whether the organisation's backups are secured at centrally accessible or secondary sites to recover from an extreme event. (A#1)
3. **Backup test reviews** - in addition to step 2 of 'Partially achieved', obtain evidence to show that the results of the backup tests are regularly reviewed, with issues identified resulting in remediating actions. Obtain evidence of this review process and action implementation. (A#2)

Suggested documentation – Partially Achieved

- Procedures for accessing and deploying backups after extreme event scenarios.
- Backup tests.

Additional documentation – Achieved

- Documentation of comprehensive procedures for backups.
- Evidence of secure sites being used for backups storage.
- Evidence of results of backup tests being reviewed and acted upon.

Principle B6: Staff awareness and training

Description

Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to information, systems and networks supporting the operation of essential functions.

Overview of the underlying Contributing outcomes

Contributing outcome B6.a – Culture

Contributing outcome B6.b – Training

Outcome B6.a – Culture

Description

You develop and maintain a positive culture around information assurance.

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. People in your organisation don’t understand what they contribute to the security and governance of the essential function(s).	PA#1. Your executive management understand and widely communicate the importance of a positive culture around information assurance. Positive attitudes, behaviours and expectations are described for your organisation.	A#1. Your executive management clearly and effectively communicates the organisation's priorities and objectives around information assurance to all staff. Your organisation displays positive security and governance attitudes, behaviours and expectations.
NA#2. People in your organisation don’t know how to raise a concern about the security and governance of information, systems and networks.	PA#2. All people in your organisation understand the contribution they make to the security and governance of information, systems and networks supporting your essential function(s).	A#2. People in your organisation raising potential security incidents and issues are treated positively.
NA#3. People believe that reporting issues may get them into trouble.	PA#3. All individuals in your organisation know who to contact and where to access more information about information assurance. They	A#3. Individuals at all levels in your organisation routinely report concerns or issues about information assurance and are recognised for their contribution to keeping the organisation and its information secure.
NA#4. Your organisation’s approach to the security and governance of information, systems and networks is perceived by staff as hindering the business of the organisation.		A#4. Your management is seen to be committed to and actively involved in information assurance.

know how to raise a security issue.	A#5.	Your organisation communicates openly about information assurance with any concern being taken seriously.
	A#6.	People across your organisation participate in activities to improve information assurance, building joint ownership and bringing knowledge of their area of expertise.

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 provide 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. **Culture** - obtain evidence of how the organisation's executive management communicates the importance of a positive culture around information assurance, for example, through campaigns they have sponsored, initiatives they have supported and communications they have issued. Assess whether the organisation's methods of promotion ensure that all levels of staff are made aware of these information assurance endorsements. (PA#1)
2. **Staff contribution** - discuss with a sample of staff members what things they need to do and be aware of in their role in order to keep information safe, and whether they understand the contribution they make to securing and protecting patient information, including appropriate use of IT systems. This understanding could come from training for information governance and security, communication from management, clauses in their contracts or policies detailing their responsibilities. (PA#2)
3. **Raising a security issue** - discuss with the organisation their process for raising a security issue, including potential incidents, near misses or general concerns.
   a) Verify that this process is documented. (PA#3)
   b) Establish whether this process is widely shared with staff, for example through official communication, training or as part of a new joiner pack of policies. (PA#3)
4. **Accessing important information** - assess what methods the organisation uses to make clear to staff members:
   a) Where they can locate important information relating to cyber security and IG procedures. For example, a procedural document telling them how to securely send information to external organisations and patients. (PA#3)
   b) Who they can speak to when they are unsure about cyber security and IG procedures. For example, details of the organisation's IT team or Data Protection Officer. (PA#3)

Additional approach to testing – Achieved

1. **Priorities and objectives for information assurance** - in addition to step 1 of 'Partially achieved', obtain evidence that:
   a) Priorities and objectives for information assurance have been defined and documented (A#1)
   b) Positive security and governance attitudes, behaviours and expectations are displayed by executive management and the organisation, for example through championing of information governance and cyber security achievements and encouraging a culture of improvement (A#1, A#4).

2. **Positive treatment of staff raising incidents and issues** - discuss with the organisation how they encourage positive treatment of people who raise concerns about potential security or data protection incidents. Ask a sample of staff members whether they feel they would be treated positively if they raised a concern about a potential security or data protection incident. (A#2)
3. **Process for reporting concerns or issues** - discuss with management the process for staff to report concerns or issues about information assurance, and obtain evidence that it is followed appropriately. Assess whether the process is sufficient to ensure that:
    a) Concerns or issues are investigated and acted on quickly, and communication takes place with the person that raised the alert initially; (A#3, A#5)
    b) The person raising the alert is recognised for their contribution to keeping the organisation and its information secure; (A#3)
    c) Staff are protected from retaliation or negative treatment for raising an issue or concern; (A#2, A#3)
4. **Activities to improve information assurance** - discuss with the organisation the opportunities available for staff to participate in activities to improve information assurance, for example lunch-and-learns, official training and blogs. Obtain evidence that those activities are not just an occasional one-off, and are attended by all levels of staff. (A#6)

Suggested documentation – Partially Achieved

- Evidence of executive management endorsements and communications promoting the importance of a positive culture around information assurance.
- List of all staff members and the relevant training, communications and procedures they have access to.
- Procedures for raising security issues.
- Procedures for informing staff where to find important cyber security and IG-related information and contacts.

Additional documentation – Achieved

- Documentation showing information governance priorities and objectives.
- Evidence of campaigns and initiatives showing positive security governance attitudes, behaviours and expectations from executive management.
- Evidence of encouragement of positive staff treatment following reports of security issues.
- Evidence of concerns being taken seriously, recognition of positive behaviours and protection from retaliations being incorporated into procedures for raising concerns.
- Evidence of activities to promote information assurance awareness.

Outcome B6.b – Training

Description

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.

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** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. There are teams who operate and support your essential function(s) that lack any information assurance training. NA#2. Information assurance training is restricted to specific roles in your organisation. NA#3. Information assurance training records for your organisation are lacking or incomplete.	PA#1. You have defined appropriate information assurance training and awareness activities for all roles in your organisation, from executives to the most junior roles. PA#2. You use a range of teaching and communication techniques for information assurance training and awareness to reach the widest audience effectively. PA#3. Information assurance information is easily available.	A#1. All people in your organisation, from the most senior to the most junior, follow appropriate information assurance training paths. A#2. Each individual's information assurance training is tracked and refreshed at suitable intervals. A#3. You routinely evaluate your information assurance training and awareness activities to ensure they reach the widest audience and are effective. A#4. You make information assurance information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

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 provide 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. **Information assurance training and awareness** - assess whether appropriate training and awareness activities have been defined for each role, or groups of roles, based on their activities and responsibilities within the organisation. (PA#1)
2. **Range of teaching and communication** - obtain evidence that the organisation has, as part the development of the training needs analysis, ensured its methods of training and raising awareness are appropriate for the staff groups they need to reach. Where specific methods have been chosen, for example digital modules, activity-based training or certified courses, verify that the organisation understands its rationale for their effectiveness which takes into account the roles and responsibilities of the target audience. (PA#2)
3. **Obtaining information assurance information** - verify whether the organisation has made it easy for staff to find relevant cyber security and IG information, such as by having a centrally accessible repository or an easily navigable intranet hub with signposting to relevant topics. (PA#3)

Additional approach to testing – Achieved

1. **Staff training paths** - in addition to step 1 in ‘Partially achieved’, verify that skills and knowledge are identified for staff to achieve over time as part of undertaking the training activities designated by the organisation. (A#1)
2. **Tracking of training completion** - obtain evidence that the organisation has a way of tracking which training has been undertaken by which staff members, and alerting those staff members to refresh their training at suitable intervals. (A#2)
3. **Evaluating effectiveness of training** - discuss with the organisation the process for evaluating the effectiveness of training and awareness activities, which can be scheduled or efficiently reactive. For example, evaluations could be informed by staff feedback, new national requirements or changes in the technology used by the organisation. Obtain the results of the latest evaluation process and verify that actions resulting from the evaluation were assigned to an owner and are being progressed. (A#3)
4. **Availability and use of information and good practice guidance** - in addition to step 3 of ‘Partially achieved’, through discussions with the organisation, assess whether they have made good practice guidance available on topics identified as being important for staff members to understand for good data security and protection. Verify that the organisation is able to give examples it is aware of where these resources have been referenced or used by colleagues. (A#4)

Suggested documentation – Partially Achieved

- Documented training and awareness activities for all staff roles.
- Procedures for considering and approving training methods.
- Evidence of easily available information assurance information.

Additional documentation – Achieved

- Evidence of specific training goals, skills, knowledge being identified.
- Procedures for tracking and refreshing individuals' training cycles.
- Procedures for evaluating effectiveness of training and awareness activities.
- Evidence of good practice guidance being made available on key topics and used by staff members.