NHS England

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

17/12/24

Objective A – Managing risk

Description

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage risks to the security and governance of information, systems and networks supporting essential functions.

Overview of the underlying Principles

Principle A1: Governance

Principle A2: Risk management

Principle A3: Asset management

Principle A4: Supply chain

Principle A1: Governance

Description

The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security and governance of information, systems and networks.

Overview of the underlying Contributing outcomes

Contributing outcome A1.a – Board direction

Contributing outcome A1.b – Roles and responsibilities

Contributing outcome A1.c – Decision-making and approval

Contributing outcome A1.a – Board direction

Description

You have effective organisational information assurance management led at board level and articulated clearly in corresponding policies.

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

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board level. NA#2. Board level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance. NA#3. The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level. NA#4. Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	*Partial achievement is not possible for this contributing outcome*	A#1. Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of your essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. A#2. Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function(s) take place, based on timely and accurate information and informed by expert guidance. A#3. There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level. A#4. Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks 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 provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Information governance and security policies** - assess whether the organisation's information governance and security policies have been clearly documented. The policies should cover:
    a) the approach to the security and governance of information, systems and networks supporting the operation of essential function(s). (A#1)
    b) a communication process to ensure that all relevant staff are aware of the contents of the policies. (A#1)
    c) reporting lines up to the accountable board level member(s). (A#3)
2. **Information governance and security groups** - obtain evidence that key findings and decisions made by expert groups responsible for information, systems and networks feed into discussions at board level. (A#2)
3. **Board meetings** - obtain the terms of reference and minutes of the organisation's board and assess whether security and governance of information, systems and networks is regularly discussed. (A#3)
4. **Board strategy and action plans** - assess whether action plans relating to the security and governance of information, systems and networks are put in place to implement the direction set by the Board. These action plans should have named owners and clear timelines. Verify that progress is monitored, and timelines are being adhered to. (A#4)

Suggested documentation list

- Policies relating to the security and governance of information, systems and networks
- Evidence of information governance and security group findings and decisions being discussed at board level
- Terms of reference and minutes from board meetings
- Board level strategy and action plans relating to the security and governance of information, systems and networks

Contributing outcome A1.b – Roles and responsibilities

Description

Your organisation has established roles and responsibilities for the security and governance of information, systems and networks at all levels, with clear and well-understood channels for communicating and escalating risks.

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

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. NA#2. Staff are assigned security or information governance responsibilities but without adequate authority or resources to fulfil them. NA#3. Staff are unsure what their responsibilities are for the security and governance of the essential function(s). NA#4. Not all staff contracts clearly set out their responsibilities for the security and governance of information, systems and networks.	*Partial achievement is not possible for this contributing outcome.*	A#1. Key roles and responsibilities for the security and governance of information, systems and networks supporting your essential function(s) have been identified. These are reviewed regularly to ensure they remain fit for purpose. A#2. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. A#3. There is clarity on who in your organisation has overall accountability for the security and governance of information, systems and networks supporting your essential function(s). A#4. All staff contracts contain clear clauses confirming their responsibilities for the security and governance of information, systems and networks.

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

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

Suggested approach to testing

1. **Key roles and responsibilities** – assess how the organisation has assigned responsibilities to each key role in a way that ensures there are no gaps in its critical information governance and cyber security activities. (A#1)
2. **Regular review** - verify that the organisation has a process for reviewing key roles and responsibilities to ensure they remain suitable for maintaining the security and governance of its information, systems and networks. Obtain evidence that the reviews occur in a scheduled or efficiently reactive manner to identify and address potential gaps in the organisation's cyber security and IG activities without undue delay. (A#1)
3. **Job descriptions** - obtain the job descriptions of key staff, such as Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Caldicott Guardian, Information security/cyber security lead. Assess whether appropriate qualifications and/or experience requirements are required for these roles. (A#2)
4. **Reporting resourcing issues -** assess whether the organisation has procedures in place for reporting risks relating to inadequate time, authority and resources for carrying out information governance and cyber security duties so these can be considered by responsible decision-makers. (A#2)
5. **Overall accountability** – obtain the name of the individual with overall accountability for the security and governance of information, systems and networks. Verify that their responsibilities have been appropriately documented. (A#3)
6. **Staff contracts** - obtain an example staff contract and assess whether they contain clear clauses confirming their responsibilities for the security and governance of information, systems and networks. (A#4)

Suggested documentation list

- Documentation of key roles and responsibilities
- Evidence of review process for roles and responsibilities
- Job descriptions
- Procedures for reporting resourcing issues
- Name of individual with overall accountability
- Staff contract sample

Contributing outcome A1.c – Decision-making and approval

Description

You have senior-level accountability for the security and governance of information, systems and networks, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks related to the operation of your essential function(s) are considered in the context of other organisational risks.

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

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. What should be relatively straightforward risk decisions are constantly referred up the chain or not made. NA#2. Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate. NA#3. Decision-makers are unsure of what senior management's risk appetite is or only understand it in vague terms such as "averse" or "cautious". NA#4. Organisational structure causes risk decisions to be made in isolation for example engineering and IT don't talk to each other about risk. NA#5. Risk priorities are too vague to make meaningful distinctions between them. (such as almost all risks are rated 'medium' or 'amber').	*Partial achievement is not possible for this contributing outcome.*	A#1. Senior management have visibility of key risk decisions made throughout the organisation. A#2. Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function(s), as set by senior management. A#3. Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need. A#4. Risk management decisions are regularly reviewed to ensure their continued relevance and validity. A#5. Risk decisions are joined up between different departments.

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

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

Suggested approach to testing

1. **Decision-making process** - obtain evidence that:
    a. a board-approved risk appetite has been established (A#2)
    b. decision-makers are able to explain how they make effective decisions in the context of the risk appetite (A#2)
    c. it is clear which staff members are responsible for making decisions about which areas of risk (A#2, A#3)
2. **Escalation to board** - assess whether there are criteria and procedures for escalating key risk decisions to the board, and obtain evidence that this escalation takes place when required. (A#1)
3. **Skills, knowledge, tools and authority –** verify how the organisation has ensured that staff members responsible for making decisions in different risk areas are most appropriately positioned and equipped to fulfil their decision-making responsibilities. (A#3)
4. **Risk registers** - obtain the organisation's risk registers and assess whether their contents align with the organisation's procedures for decision-making. (A#3)
5. **Risk register review** - verify that the organisation has a process for reviewing risk management decisions to ensure they remain relevant and valid. Obtain evidence that the reviews occur in a scheduled or efficiently reactive manner to identify and address potential issues with risk decisions. (A#4)
6. **Siloed risk decisions** - verify that decision-makers have a criteria for deciding where other departments need to be consulted on risk decisions. Obtain evidence that decision-makers have involved other departments where appropriate. (A#5)

Suggested documentation list

- Risk appetite statement
- Responsibilities for decision-making in different risk areas
- Procedures for reporting key risk decisions to the board
- Procedures for delegating risk decisions
- Risk registers
- Procedures for risk register review
- Procedures for involving other departments in risk decisions

Principle A2: Risk management

Description

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

Overview of the underlying Contributing outcomes

Outcome A2.a – Risk management process

Outcome A2.b – Assurance

Contributing outcome A2.a – Risk management process

Description

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

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

Indicators of good practice (IGP) achievement levels

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

NA#6.	Systems and risks are assessed in isolation, without consideration of dependencies and interactions with other systems or risks in other areas of the business. For example interactions between IT and operational technology environments, or finance risks and the impact on information governance.		decision -makers and accountable individuals.		understanding of the information and vulnerabilities in the systems and networks supporting your essential function(s), as well as a good understanding of your data processing activities in all areas of your organisation. This includes evaluation of repeated or significant near misses.
NA#7.	Security and IG requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function(s).	PA#5.	You conduct risk assessments (including DPIAs) when significant events potentially affect the essential function(s), such as replacing a system, commencing new or changing high-risk data processing, or a change in the cyber security threat.	A#5.	The output from your risk management process is a clear set of requirements that will address the risks in line with your organisational approach to security and IG more widely.
NA#8.	Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve. These risks may be out of date or incomplete.	PA#6.	You perform threat analysis and understand how generic threats apply to your organisation.	A#6.	Significant conclusions reached in the course of your risk management process are communicated to key decision-makers and accountable individuals.
		PA#7.	Your risk process clearly demonstrates how your organisation's processing complies with data protection principles and relevant legislation, including the right to a private life.	A#7.	Your risk assessments (including DPIAs) are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use or processing, and new threat information.
				A#8.	The effectiveness of your information and security risk management process is reviewed periodically, and improvements made as required.
				A#9.	You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider Critical National Infrastructure.
				A#10.	Your risk process clearly demonstrates how your organisation's processing

		complies with data protection principles and relevant legislation, including the right to a private life.

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

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

Suggested approach to testing – Partially Achieved

1. **Risk management processes** - verify that:
   a) The organisation has comprehensive processes for identifying, analysing, prioritising and managing information governance and cyber security risk (PA#1, A#1)
   b) There is a specific process which the organisation adheres to for conducting risk assessments when significant events occur that could affect the organisation's essential functions (PA#5, A#7)
   c) There is a specific process which the organisation adheres to for conducting DPIAs before beginning any type of processing which is likely to result in a high risk to the rights and freedoms of individuals (PA#5, A#7)
   d) The organisation's adherence to agreed processes are reflected in the organisation's risk management documentation such as risk registers and risk assessments (PA#1, A#1)
2. **Risk management documentation** - verify whether the documents show:
   a) Data protection by design and by default, incorporated in the process; (PA#1, A#1)
   b) Consideration of data protection principles and relevant legislation, including the right to private life where applicable. (PA#7, A#10)
3. **Understanding information and vulnerabilities** – obtain and inspect the organisation's risk registers and a sample of the organisation's risk assessments. Verify that:
   a) For projects involving personal information, the nature of personal and sensitive information is appropriately considered as part of risk management processes (PA#2)
   b) For projects involving changes to systems and networks, vulnerabilities are appropriately considered as part of risk management processes (PA#2)
4. **Risk management actions** - obtain the outputs of the risk management process discussed in step 1 and step 3, and assess whether the outputs include clear requirements and mitigation to address risks in line with the organisation's approach to cyber security and IG more widely. (PA#3, A#5)
5. **Communicating to accountable individuals** - verify that the organisation has established thresholds for situations where outputs of risk management processes should be communicated to key decision-makers and accountable individuals. Obtain evidence that this communication occurs where it is needed. (PA#4, A#6)
6. **Threat analysis** - assess how the organisation has incorporated threat intelligence into its cyber risk management processes. (PA#6, A#9)

Additional approach to testing – Achieved

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

Suggested documentation – Partially Achieved

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

Additional documentation - Achieved

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

Contributing outcome A2.b – Assurance

Description

You have gained confidence in the effectiveness of the security and governance of your technology, people, and processes relevant to 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	Achieved All the following statements are true:
NA#1. A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value. NA#2. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. NA#3. Assurance is assumed because there have been no known problems to date.	*Partial achievement is not possible for this contributing outcome*	A#1. You validate that the security and governance measures in place to protect information, systems and networks are effective and remain effective for the lifetime over which they are needed. A#2. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential function(s). A#3. Your confidence in the security and governance as it relates to your technology, people, and processes can be justified to, and verified by, a third party. A#4. Security and governance deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. A#5. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

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 – Mandatory policy requirement

Assurance policy – it is mandated via the NHS Standard Contract and the DSPT requirement that organisations annually complete a DSPT audit/independent assessment. Organisations must have due regard to the findings and provide them to their board and within their DSPT submission. The provision of an independent assessment following the guidance in this document meets this directive policy requirement.

Suggested approach to testing

1. **Security and governance measures** - assess how the organisation validates that its cyber security and IG controls are working effectively. Obtain evidence that the organisation's validation processes can effectively identify weak points, and that plans are put in place to remedy those weak points. (A#1)
2. **Selection of assurance methods** – discuss the various assurance methods in use at the organisation, and understand how they were assessed against other methods and validated as the appropriate methods to be used. (A#2)
3. **Independent assurance** - obtain evidence of how the organisation uses third-parties to assure its technology, people and processes, for example, by inspecting documentation of previous DSPT audits. (A#3)
4. **Deficiency remediation** – assess whether deficiencies identified by assurance activities are assessed by responsible decision-makers, and clear remediation actions are delegated to named owners. Obtain evidence that this process leads to remediation of deficiencies identified without undue delay. (A#4)
5. **Review of assurance methods** - verify that the organisation has a scheduled or efficiently reactive process for reviewing its assurance methods which ensures that they remain appropriate. (A#5)

Suggested documentation

- Procedures for assurance of cyber security and information governance controls
- Evidence of validation and selection of assurance methods
- Evidence of previous DSPT audits or equivalent independent assurance
- Action plans for remediating deficiencies
- Procedures for reviewing assurance methods

Principle A3: Asset management

Description

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

Overview of the underlying Contributing outcomes

Outcome A3.a – Asset management

Contributing outcome A3.a – Asset management

Description

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

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

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. Inventories of assets relevant to the essential function(s) are incomplete, non-existent, or inadequately detailed. NA#2. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and operational technology). NA#3. Information assets, which could include personally identifiable information and / or important / critical data, are stored for long periods of time with no clear business need or retention policy. NA#4. Knowledge critical to the management, operation, or recovery of the essential function(s) is held by one or two key individuals with no succession plan. NA#5. Asset inventories are neglected and out of date. NA#6. Your information asset register (IAR) or registers are incomplete or out of date.	*Partial achievement is not possible for this contributing outcome*	A#1. All assets relevant to the secure operation of essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. This includes maintaining an information asset register (IAR) which is reviewed and kept up to date. A#2. Dependencies on supporting infrastructure (such as power, cooling etc) are recognised and recorded. A#3. You have prioritised your assets according to their importance to the operation of the essential function(s). A#4. You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of the essential function(s). A#5. Assets relevant to the essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

NA#7.	Information asset owners and information asset administrators have not been appointed.		A#6.	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 provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Asset inventory** – review the organisation's document(s) or tool(s) for cataloguing assets. Cataloguing may all be done in the organisation's Information Asset Register, or may be achieved via a combination of the Information Asset Register with other documents and tools for different asset types. Obtain evidence to verify that the following criteria are met:
   a) Comprehensive coverage of the organisation's information assets, hardware assets, software assets, connected medical devices, systems storing personal data and systems storing business and commercial data. (A#1)
   b) Indication of the relevance of each asset to the organisation's essential function(s). (A#1)
   c) Recognition of asset dependencies on supporting infrastructure (A#2)
   d) A system of prioritisation that indicates which assets are most important to the operation of the organisation's essential function(s); (A#3)
   e) An assigned staff member who is responsible for managing each asset, including information asset owners and administrators for information assets. Verify how the organisation has made these staff members aware of their roles and responsibilities. (A#4, A#6)
2. **Managing with cyber security in mind** – verify that the organisation is able to use its asset management procedures for security purposes, such as identifying anomalous or unsupported devices, cross-referencing vulnerabilities against devices and software on its networks, and ensuring suitable controls are applied wherever assets are reused, transferred or disposed of. (A#5)

Suggested documentation

- Information assets register
- Other document(s) or tool(s) for cataloguing assets
- Evidence of consideration and prioritisation of essential functions
- Evidence of asset dependencies on supporting infrastructure being recognised
- Evidence of asset managers and owners being assigned
- Procedures for reviewing and updating asset inventories
- Evidence of asset management procedures facilitating effective cyber security

Principle A4: Supply chain

Description

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

Overview of the underlying Contributing outcomes

Outcome A4.a – Supply chain

Contributing outcome A4.a – Supply chain

Description

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

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

Indicators of good practice (IGP) achievement levels

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

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

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

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

Suggested approach to testing – Partially Achieved

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

Additional approach to testing – Achieved

1. **Detailed supplier risks** – obtain evidence that the organisation has identified and documented risks posed by suppliers to a deep level of detail. Verify that the organisation interrogates these risks as part of its risk assessment and procurement processes before onboarding suppliers. The risk considerations should include specific IG and cyber risks which emerge as a result of the supplier's sub-contractors, the supplier's partnerships and the supplier's geographic location. (A#1)
2. **Supply chain risk management -** obtain evidence that the risks documented in step 1 have been discussed and reviewed by responsible decision-makers within the organisation. Where subversion of suppliers' services would cause unacceptable consequences, mitigations should have been discussed, with short-term and long-term plans for remediation. (A#2)
3. **Assurance against sophisticated attacks** - verify what assurances the organisation obtains from suppliers to ensure that they meet the organisation's security and IG requirements. The assurances should be sufficient to confirm that information shared with the supplier is appropriately protected from sophisticated attacks. (A#3)
4. **Contract management plan** – verify whether the organisation has a contract management plan in place which allows for regular review of important contracts. (A#4)
5. **Roles and responsibilities** - obtain the list of supplier contracts and obtain a sample. Verify that the customer/supplier ownership of responsibilities are laid out in those contracts. (A#5)
6. **Network connections and data sharing** - obtain evidence that the organisation understands and documents third-party connections to its network and data sharing with third-parties. Assess the supplier management processes the organisation has in place for ensuring that these connections and data being shared are necessary and proportionate for the services being provided and obtain evidence that these processes are followed. (A#6)
7. **Incident management process** - obtain and inspect the organisation's incident management process and assess whether suppliers' roles and responsibilities are documented. Request evidence of assurance the organisation has received from their most critical suppliers of mutual support during incidents. (A#7)
8. **Changes in services** - verify that the organisation has a scheduled or efficiently reactive process for liaising with other teams to keep track of changes to services that impact cyber security and information governance-related understandings and agreements with suppliers. Obtain evidence that this process is followed and changes are made where necessary without undue delay. (A#8)
9. **Certification and right to audit** - verify that as part of the organisation's procurement processes, there is a requirement for supplier certifications to be obtained prior to the contract being signed. For the suppliers who the organisation has identified as most critical to the operation of its essential functions, contracts should also include a right to audit, based on specific parameters relevant to the services being provided. (A#10)

Suggested documentation – Partially Achieved

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

Additional documentation – Achieved

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