Health and Social Care Cloud Security – Good Practice Guide

This material is for general guidance only. Recipients are responsible for exercising their own professional judgement in using the material.

Whilst efforts were taken to ensure that the information contained in this document is both clear and accurate at the time of publication, NHS Digital cannot guarantee that this information will be suitable for the recipient's own hosting and infrastructure requirements, or their procurement/commercial/legal context.

Accordingly, NHS Digital accepts no responsibility for any losses or damages arising from the use of this material.

1 Introduction

The UK Government introduced a 'cloud first' policy for public sector IT in 2013. The use of cloud services was also endorsed in the National Information Board's Personalised Health and Care 2020 framework, published in November 2014.

A paper jointly published by the Department of Health and Social Care, NHS England, NHS Digital and NHS Improvement on 19 January 2018 states that NHS and social care organisations can safely locate health and care data, including confidential patient information, in the public cloud including solutions that make use of data off-shoring. The paper provides advice and guidance regarding the safeguards that should be put in place to do so.

NHS Digital have built upon this advice and guidance to develop more detailed materials to enable a systematic approach to evaluate risk and applying proportionate controls. This document explains the process and provides details on what proportionate controls should be put in place.

2 Overview of the Method

This Good Practice Guideline (GPG) is a four-step process. It should be used at the start of any digital project to understand the risk of the data that needs to be stored and processed and the safeguards that must be put in place to do so. The steps are as follows:-

- Step 1 - **Understand** the data you are dealing with
- Step 2 – **Assess** the risks associated with the data
- Step 3 – **Implement** appropriate controls
- Step 4 – **Monitor** the implementation and ongoing risks

3 Step 1 - Understand

The first step is to understand the data that you are dealing with.

1. List all the data fields/attributes that will be stored or processed by the system.
2. Quantify how much data is under consideration.
3. Consider how long the data will be held in the system.

4. Understand the Service Classification[1] of the system (Bronze | Silver | Gold | Platinum). This relates to the availability SLAs and will be used to determine the cloud security approach for availability and integrity. The service classification is normally agreed between the owning Programme and Service management.
5. Carefully assess the data fields/attributes and decide which Data Type(s)[2] this relates to.
6. Armed with this information, use the *NHS Digital Data Risk Model* to calculate the risk classification of the data.
7. Ensure that you document the outputs of the above, specifically:-
    a. Retain the list of data types/attributes.
    b. Record the rationale for selecting the data type(s).
    c. Retain the completed risk model.

The *Health and Social Care Cloud Risk Framework* document lists the different Data Types, scale and persistency along with descriptions and examples. This will help you with steps 1 to 5 above.

The *NHS Digital Data Risk Profile Tool* calculates a score based on the type of data, the amount of data and for how long the data is held. This score is then translated into a Risk Classification and will be used in the next steps of the process.
The risk classification is used to help you understand:-

- the risk profile and the associated governance that we would expect you to undertake.
- the controls that are needed to be put in place to mitigate the risk.

4 Step 2 - Assess

This step is about assessing the risk and identifying governance requirements for putting the data in the cloud. At the end of this step, you should have decided as to whether you want to use public cloud to host your system.

4.1 Risk Appetite

Different organisation and programmes will have different appetites towards risk and this appetite may vary over time.

[1] Refer to appendix B.
[2] Refer to the document: *Health and Social Care Cloud Risk Framework* for details of data types.

- Class I defines the lowest level of risk.
- Class V defines the highest level of risk.

However, proportionate controls are available to help mitigate these risks, regardless of whether the risk is classified as Class I or Class V. These are detailed in Step 3. Understand your organisation's risk appetite, implement controls and monitor their effectiveness as part of your ongoing governance process.

4.2 Governance

Using the Risk Classification obtained in step 1, refer to the table below to understand the governance expectation.

Risk Profile Level	Expectation
Class I	All organisations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organisations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes described in Part 3, requiring approval by CIO / Caldicott Guardian level.
Class IV	At this level, it may become more difficult to justify that the benefits of the using public cloud outweigh the risks. However, a case may still be made, requiring approval by CIO / Caldicott Guardian, and be made visible to the organisation's Board. Specialist advice and guidance should be sought.
Class V	Operating services at this level would require board-level organisational commitment, following specialist advice and guidance.

4.3 Other Considerations

Security is not the only aspect that you should consider when moving to cloud. Other elements to think about include:-

4.3.1 Public Perception

There is some degree of public concern over the use of computing environments that are well-known to be publicly-consumable and used for a wide variety of small and large scale uses. There may be a lack of trust as to the effectiveness of the people, technical and process controls that are intended to reduce the risks of confidentiality and breach to manageable levels. You must be comfortable with any challenge that comes from the public and the media. And if there is a security incident, then the question will be raised as to why public cloud was used.

4.3.2 Lock-in and migration

If you build your infrastructure using standard and widely available components such as virtual machines (VMs) and storage it will ease any migration to another provider. However, vendor specific components are attractive as they may provide lower cost options and facilitate faster delivery. Be conscious of any trade-off. Consider the impact of the necessity of migrating potentially large quantities of data to launch a service, and the potential future impact of increased data scale if ever you wished to, or needed to, migrate to an alternative.

4.3.3 Data Repatriation

Consider how any data within the system can be retrieved and returned to you when the contract for cloud services expires. Discuss with your intended provider how you wish your data to be transferred back into your custody. Ensure such facilities and associated timescales are agreed and included within the contract. You should also seek assurances from your cloud provider that any copies of your data will be deleted, overwritten or otherwise rendered inaccessible.

4.3.4 Existing situation

When considering moving systems into public cloud, it is worth considering the “As-Is” hosting solution. If you have an existing high risk but low security solution, then the perceived risks of moving into a public cloud may be mitigated.

4.3.5 Complex Systems

Systems may host a variety of different data types, which hold different risk profiles. It may be appropriate to consider hosting some subsystems on public cloud whilst hosting other subsystems elsewhere.

4.3.6 Data residency and sovereignty

Some cloud providers may store or process data offshore, which may improve resilience and reduce costs. Processing data in cloud services is legally complex, regardless of where the data is being processed. Data must only be hosted within the European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield. Further guidance is available from the Information Commissioner's Office.

4.3.7 Fair Processing

Regardless of the where services are hosted, all organisations processing personal data must do so fairly and lawfully. This is set out in the first data protection principle of the Data Protection Act 1998. Fair processing includes providing details of:

- your identity and, if you are not based in the UK, the identity of your nominated UK representative;
- the purpose or purposes for which you intend to process the information; and
- any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

4.4 Documentation

It is important that a complete set of documentation is kept for audit purposes to prove that appropriate due diligence has been taken with regards to where and how data is hosted. Therefore, document:-

1. The governance decision to use the cloud (e.g. meeting minutes).
2. Responses to all other considerations listed above.

4.5 Contracts

All Cloud contracts need to be robust and clearly compliant with UK law. It is essential that you have documentation that details what duties and obligations have been agreed.

5 Step 3 - Implement

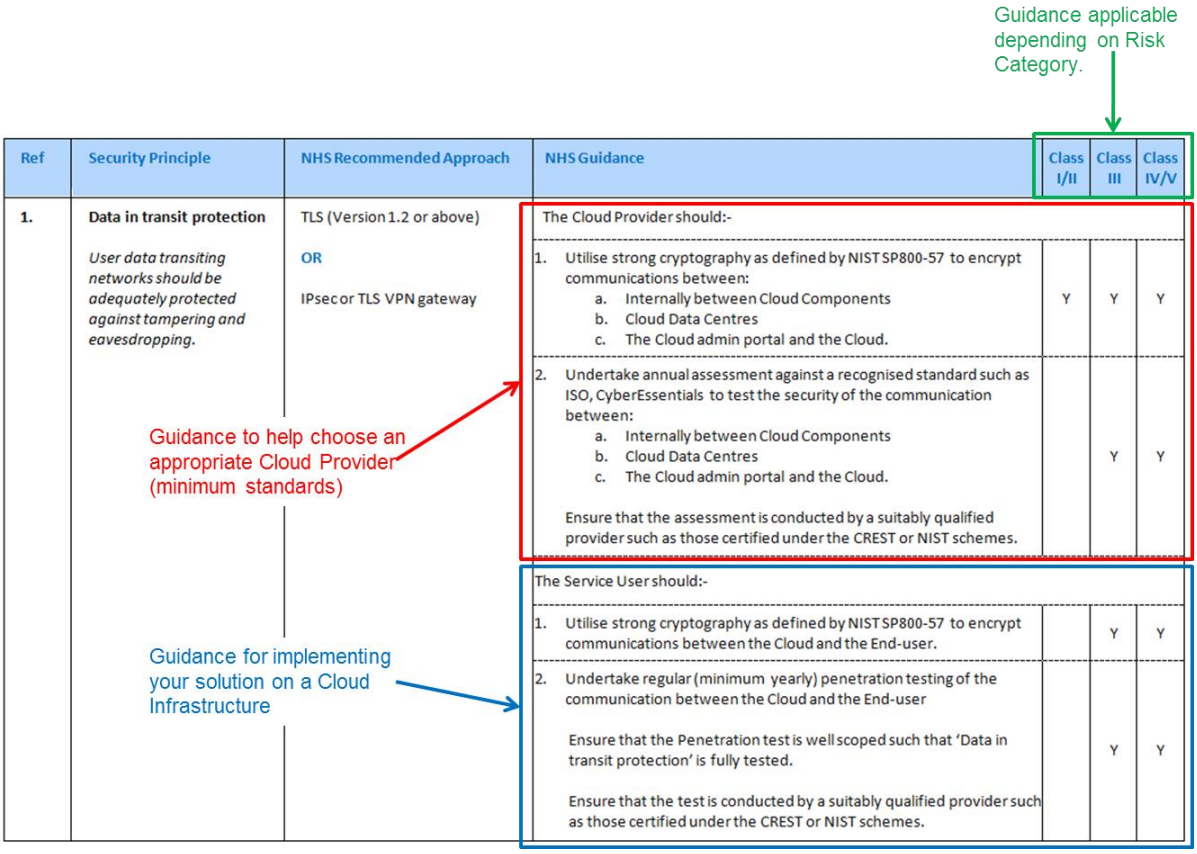
Having decided that you wish to utilise public cloud to host your system, you need to:-

- select a cloud provider that meets the required security standards, and

- apply the security controls that are under your responsibility.

Using public cloud necessitates a joint responsibility to security. The cloud provider must ensure that their service is appropriately secure, and you must have confidence in it. Similarly, the users have a responsibility to ensure how they implement the solution is appropriately secure. This is often referred to as the *joint responsibility model*.

Appendix A lists the minimum standards the cloud provider must meet and how you should implement the solution. These are structured around the National Cyber Security Centre's (NCSC) 14 Cloud Security Principles. Against each principle is the recommended approach and specific guidance, dependant on the risk classification[3].



Ref	Security Principle	NHS Recommended Approach	NHS Guidance	Class I/II	Class III	Class IV/V
1.	**Data in transit protection** *User data transiting networks should be adequately protected against tampering and eavesdropping.*	TLS (Version 1.2 or above) **OR** IPsec or TLS VPN gateway	The Cloud Provider should:-			
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between: a. Internally between Cloud Components b. Cloud Data Centres c. The Cloud admin portal and the Cloud.	Y	Y	Y
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the security of the communication between: a. Internally between Cloud Components b. Cloud Data Centres c. The Cloud admin portal and the Cloud. Ensure that the assessment is conducted by a suitably qualified provider such as those certified under the CREST or NIST schemes.		Y	Y
			The Service User should:-			
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user.		Y	Y
			2. Undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user Ensure that the Penetration test is well scoped such that 'Data in transit protection' is fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST or NIST schemes.		Y	Y

5.1 Select a cloud provider

Choose a cloud provider that meets the minimum security standards as specified in the table. Each of the 14 principles will have a section entitled "The cloud provider should:-" This lists a set of minimum standards. However, you only need to adopt the standard that corresponds to your risk score. For example, if your risk score is

[3] Principle *2.6 - Physical resilience and availability* uses the service category (B)ronze, S(ilver), G(old) and (P)latinum, rather than Cat I to V, to determine which minimum standards / controls that need to be in place.

Class II, then in the above example the Cloud provider only needs to meet requirement 1. However, if your risk score is Class IV then they need to meet requirements 1 and 2.

You can buy cloud services through the G-Cloud Framework on the Digital Marketplace. Cloud services are listed on the Digital Marketplace alongside information and evidence submitted by vendors on how they perform against the National Cyber Security Centre's Cloud Security Principles. You may need to request further information from the supplier to be confident that they meet the recommended standards.

5.2 Apply security controls

Similarly, you must implement controls in-line with the recommendations in the table. Each of the 14 principles will have a section entitled "The service user should:-" This lists a set of minimum implementation standards. However, you only need to adopt the standard that corresponds to your risk score. For example, if your risk score is Class II, then in the above example you have no controls to apply. However, if your risk score is Class IV then you need to meet requirements 1 and 2.

5.3 Documentation

It is important that a complete set of documentation is kept for audit purposes to prove that appropriate due diligence has been taken with regards to where and how data is hosted. Therefore, document and retain:-

1. Evidence that the supplier meets the standard.
2. Evidence that you have implemented the controls.
3. Cloud contract(s), showing that they are clearly compliant with UK law and what duties and obligations have been agreed.

6 Step 4 - Monitor

Like any other system, once implemented you cannot forget about security and risk. It needs to be proactively monitored and managed.

6.1 Manage known risk

If there are any residual risks, then these need to be document and pro-actively managed.

6.2 Monitor cloud service

Cloud services offered by providers are most likely to continually evolve. You need to make sure that your vendor keeps you informed of any changes that may affect, in a detrimental way, the security of your system and data.

Similarly, your vendor should supply updated proof of certifications and assessments on a regular basis.

6.3 Monitor controls

The service user is responsible for implementing and maintaining certain security controls. These should be reviewed / audited on a regular basis.

7 Document Control

7.1 Copyright

7.2 Related References, Links and Documents

These documents will provide additional information:-

NHS and social care data: off-shoring and the use of public cloud services
Health and Social Care Cloud Risk Framework
Health and Social Care Data Risk Model

8 Appendix A - Detailed Advice and Guidance

The table below is based on the National Cyber Security Centre's (NCSC) advice for Implementing the Cloud Security Principles. These principles have been examined within the context of health and social care and a recommended implementation approach has been specified. Further, guidance has also been listed against each principle, detailing what the Cloud Provider should do/provide. It also lists what the Cloud Service User should do to safeguard data.

This guidance assumes an Infrastructure as a Service (IaaS) model is being utilised and the split of responsibilities between the Cloud Provider and Cloud Service User reflects this. When a SaaS model is utilised then the split would need to be adjusted with the SaaS provider taking more of the responsibilities.

For clarity, the "Cloud Provider" is the organisation that is providing the cloud service. The "Service User" refers to the customer-side architect / developer / programmer / IT Pro / etc that is developing and maintaining the system in the public cloud.

The specific guidance is only applicable if there is a "Y" in the category field that matches the data risk category as defined by the risk tool. Section 2.6 - Physical resilience and availability – is an exception. The "Y" relates to the Service Classification[4], being either Bronze, Silver, Gold or Platinum.

[4] Refer to appendix B for an explanation of Service Categories.

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	Class I/II	Class III	Class IV/V
1.	**Data in transit protection** *User data transiting networks should be adequately protected against tampering and eavesdropping.*	TLS (Version 1.2 or above) **OR** IPsec or TLS VPN gateway	The Cloud Provider should:-			
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud.	Y	Y	Y
			2. Undertake annual assessment against a recognised standard such as ISO to test the security of the communication: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud. Ensure that the assessment is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user.		Y	Y
			2. Undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user Ensure that the Penetration test is well scoped such that 'Data in transit protection' is fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
Ref	Security Principle	NHS Recommended Approach	NHS Guidance	Class I/II	Class III	Class IV/V

2.	**Asset protection and resilience** *User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.*					
2.1	**Physical location and legal jurisdiction** *In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.* *You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation.*	Known locations for storage, processing and management	The Cloud Provider must:-			
			1. Provide cloud infrastructure (which includes all hardware, software, networks and the physical data centres that house it all) within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.	Y	Y	Y
			2. Provide independent validation that the data centres are actually physically located within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.	Y	Y	Y
			3. State the legal jurisdiction(s) to which your data is subject to.	Y	Y	Y
			The Service User should:-			
			1. Only use Cloud Infrastructures to store and process data that are physically located within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.	Y	Y	Y
			2. Review the Cloud Provider's T&Cs to ensure they are compliant with the Data Protection Act (DPA) and the General Data Protection Regulation (GDPR).	Y	Y	Y

2.2	**Data centre security** *Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.*	Conforms to a recognised standard	The Cloud Provider should:-			
			1. Hold and maintain certification to ISO 27001. Prove that the scope of certification includes the physical security of the data centres. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Y	Y
2.3	**Data at rest protection** *To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.*	Encryption of all physical media	The Cloud Provider should:-			
			1. Provide encryption facilities to ensure that no data is written to storage in an unencrypted form.	Y	Y	Y
			2. Provide secure key management service providing strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1'. The service must provide detailed audit reporting on access of the keys.	Y	Y	Y
			3. Confirm that the encryption utilises strong cryptography as defined by the current version of NIST SP800-57.	Y	Y	Y
			4. Undertake annual assessment against a recognised standard such as ISO or FIPS 140-2 to test the encryption. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			

			1. Ensure that the encryption is appropriately configured when you implement the system on your chosen cloud provider.	Y	Y	Y
			2. Ensure keys are managed by the data controller. Keys can be stored either locally or in an HSM service provided by the cloud supplier. The key management solution should utilise strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1	Y	Y	Y
2.4	**Data sanitisation** *The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.*	Explicit overwriting of storage before reallocation	The Cloud Provider should:-			
			1. Provide assertions regarding their data sanitisation approach.	Y	Y	Y
			2. Show that the specified data sanitation approach has been validated by a suitably qualified independent third party.		Y	Y
2.5	**Equipment disposal** *Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.*	A recognised standard for equipment disposal is followed **OR**	The Cloud Provider should:-			
			1. Hold certification to CSA CCM v3.0 OR ISO/IEC 27001. Prove that the scope of certification validates the secure equipment disposal. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		Y	Y
		A third-party destruction service is used	The Cloud Provider should:-			
			1. Ensure the security of the equipment and prove the chain of custody until the equipment is successfully destroyed.		Y	Y
			2. Demonstrate that the third-party services have been assessed against a recognised standard, such as the CESG Assured Service (Destruction) scheme.		Y	Y

			Prove that the scope of the assessment validates the secure equipment disposal and chain of custody. Demonstrate that the assessment was performed by a suitably qualified expert party such as those certified under the CREST scheme.			

2.6	**Physical resilience and availability** *Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.*	The service provider commits to a Service Level Agreement (SLA) **AND** Analysis of the design	**Service Classification (See appendix A):**	**B**	**S**	**G/P**
			The Cloud Provider should:-			
			1. Provide a contractual commitment to SLAs, with remedies available should the SLA be missed.	Y	Y	Y
			2. Prove that the data centres are certified to Uptime Institute Tier 2 or equivalent qualified provider such as those certified under the CREST scheme.	Y		
			3. Prove that the data centres are certified to Uptime Institute Tier 3 or equivalent qualified provider such as those certified under the CREST scheme.		Y	Y
			4. Provide two or more "availability zones" / Data Centres in-line with the requirements in 2.1.		Y	Y
			The Service User should:-			
			1. Design for failure. Solutions should be architected for cloud such that they are resilient regardless of the underlying cloud infrastructure.	Y	Y	Y
			2. Use at least one availability zone / Data Centre.	Y		
			3. Have resilient network links to the zone / Data Centre.	Y		
			4. Use multiple availability zones / Data Centres.		Y	
			5. Have resilient network links to each zone / Data Centres.		Y	
			6. Use different cloud vendors or multiple regions from the same vendor.			Y
			7. Have resilient network links to each region / vendor.			Y

			8. Ensure their system has DDoS protection. This may be provided by the Cloud vendor or a third party.			Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
3.	**Separation between users** *A malicious or compromised user of the service should not be able to affect the service or data of another.*	Virtualisation technologies (e.g. a hypervisor) provide separation between users **OR** Other software provides separation between users	The Cloud Provider should:-			
			1. Provide Supplier Assertions regarding their approach to user/customer environment separation.	Y	Y	Y
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'separation between users/ customer environment'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			3. Hold and maintain certification to ISO27017 for the Cloud Platform. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Undertake end-to-end Penetration testing of the solution.		Y	Y
			2. Implement a GPG13 compliant Protective Monitoring solution.			Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
4.	**Governance framework** *The service provider should have a security governance framework which*	Conformance with a recognised standard	The Cloud Provider should:-			
			1. Hold and maintain certification to CSA's STAR programme OR ISO/IEC 27001. Demonstrate that certification was performed by a suitably qualified		Y	Y

	coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.		expert party such as those certified under the CREST scheme.			
			2. Prove that the scope of certification includes the governance framework goals set out below: a. A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. b. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. c. Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. d. Processes to identify and ensure compliance with applicable legal and regulatory requirements.			Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
5.	**Operational security** *The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.*					
5.1	**Configuration and change**	Conformance with a recognised	The Cloud Provider should:-			

	management *You should ensure that changes to the system have been properly tested and authorised. Changes should not unexpectedly alter security properties*	standard	1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001. Prove that the scope of certification includes configuration and change management processes. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		Y	Y
			The Service User should:-			
			1. Maintain an accurate inventory of the assets which make up the service, along with their configurations and dependencies.	Y	Y	Y
			2. Ensure changes to the service are assessed for potential security impact, and the implementation of changes are managed and tracked through to completion.	Y	Y	Y
5.2	**Vulnerability management** *You should identify and mitigate security issues in constituent components*	Conformance with a recognised standard	The Cloud Provider should:-			
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001, ISO/IEC 27017. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Y	Y
			2. Manage vulnerabilities in a manner that aligns with ISO 30111 and show ISO / CSA compliance to validate the process.	Y	Y	Y
			3. Prove that mitigations for discovered vulnerabilities are implemented for the server-less devices, hypervisors and supporting infrastructure, within the NCSC best practice timescales set out below:- a. 'Critical' vulnerabilities should be mitigated within 24 hours b. 'Important' vulnerabilities should be mitigated within 2 weeks.	Y	Y	Y

			c. 'Other' vulnerabilities mitigated within 8 weeks. If compensating controls are in place to reduce the vulnerability risk, the timescales can be adjusted accordingly.			
			The Service User should:-			
			1. Undertake patching or vulnerability management for the guest operating system and application components, within the NCSC best practice timescales set out below:- a. 'Critical' patches should be deployed within 24 hours b. 'Important' patches should be deployed within 2 weeks of a patch becoming available c. 'Other' patches deployed within 8 weeks of a patch becoming available	Y	Y	Y
			Undertake regular (min yearly) penetration testing. Ensure that the Penetration test is well scoped such that 'security vulnerabilities in the Operating system and components above' are fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
5.3	**Protective monitoring** *You should put measures in place to detect attacks and unauthorised activity on the service*	Conformance with a recognised standard	The Cloud Provider should:-			
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001 and ISO/IEC 27017 Prove that the scope of certification includes protective monitoring controls showing that:- a. The service generates adequate audit events to support effective identification of suspicious activity b. These events are promptly analysed to identify potential compromises or inappropriate use of your service c. The service provider takes prompt and appropriate action to		Y	Y

			address incidents Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.			
			The Service User should:-			
			1. Put in place appropriate monitoring solutions to identify attacks against their applications or software.		Y	Y
5.4	Incident management *Ensure you can respond to incidents and recover a secure, available service*		The Cloud Provider should:-			
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001. Prove that the scope of certification includes incident management controls in detail showing that:- a. Incident management processes are in place for the service and are actively deployed in response to security incidents b. Pre-defined processes are in place for responding to common types of incident and attack c. A defined process and contact route exists for reporting of security incidents by consumers and external entities d. Security incidents of relevance to the Service User will be reported in acceptable timescales and formats Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Y	Y
			2. Demonstrate robust, well tested and rehearsed incident management procedures.	Y	Y	Y
			The Service User should:-			
			1. Put in place monitoring solutions to identify attacks against their applications or software.		Y	Y

			2. Have an incident management process to rapidly respond to attacks.		Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
6.	**Personnel security** *Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.*	Personnel screening performed but does not conforms with BS7858:2012	The Cloud Provider should:-			
			1. Operate a personnel screening process that aligns with BS7858:2012 and show ISO / CSA compliance to validate the process. Demonstrate that the assessment was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		Y	Y
			The Service User should:-			
			1. Ensure IT admin staff are strongly authenticated.		Y	Y
			2. Have a suitable auditing solution is in place to record all IT admin access to data and hosting environments.		Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
7.	**Secure development** *Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.*	Independent review of engineering approach against recognised secure development standard	The Cloud Provider should:-			
			1. Hold and maintain certification to: a) CESG CPA Build Standard, OR b) ISO/IEC 27034, OR c) ISO/IEC 27001, OR d) CSA CCM v3.0. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		Y	Y

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	Class I/II	Class III	Class IV/V
8.	**Supply chain security** *The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.*	Assessed through application of appropriate standard	The Cloud Provider should:-			
			1. Hold and maintain certification to: a) ISO/IEC 27001, or b) ISO/PAS 28000:2007 Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.		Y	Y
			2. Prove that the scope of certification includes supply chain security showing:- a) How your information is shared with, or accessible to, third party suppliers and their supply chains. b) How the service provider's procurement processes place security requirements on third party suppliers. c) How the service provider manages security risks from third party suppliers. d) How the service provider manages the conformance of their suppliers with security requirements. e) How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.			Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
9.	**Secure user management** *Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital*					

	part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.					
9.1	**Authentication of [admin] users to management interfaces and support channels** *In order to maintain a secure service, [admin] users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.*	Strong authentication in place, which is subject to regular exercising	The Cloud Provider should:-			
			1. Provide Supplier Assertions regarding their approach to strong authentication.	Y	Y	Y
			2. List all the channels by which the service provider would accept management or support requests from you (telephone phone, web portal, email etc.).	Y	Y	Y
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'Authentication of users to management interfaces and support channels'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Ensure that a list of authorised individuals from your organisation who can use those mechanisms is maintained and regularly reviewed.	Y	Y	Y
			2. Use 2FA to obtain access to the system.		Y	Y
			3. Configure logging of access attempts.		Y	Y
			4. Regularly review the access attempts to identify unusual behaviour		Y	Y
9.2	**Separation and access control within management interfaces**	Access control implemented in software, subject to regular testing	The Cloud Provider should:-			
			1. Provide Supplier Assertions regarding how management interfaces	Y	Y	Y

	Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If [admin] users are not adequately separated within management interfaces, one [admin] user may be able to affect the service, or modify the data of another.		are protected and what functionality they expose.			
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'Access Control to management Interfaces'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Ensure that authorised individuals from your organisation who can use those mechanisms are managed by the 'principle of least privilege', typically using a RBAC mechanism.	Y	Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
10.	**[End User] Identity and authentication** *All access to service interfaces should be constrained to authenticated and authorised [end user] individuals.*	Two factor authentication **OR**	The Cloud Provider should:-			
			1. Allow users to authenticate with a username and either a hardware/software token, or 'out of band' challenge (e.g. SMS)		Y	Y
			2. Provide details of the authentication scheme.		Y	Y
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the '2FA'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
		TLS client certificate **OR**	The Cloud Provider should:-			
			1. Show that they use TLS 1.2 or above with an X.509v3 client certificate that identifies an individual user.		Y	Y

			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'TLS 1.2+ using an X.509v3 client certificate' Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Ensure the secure creation and management of certificates.		Y	Y
			2. Ensure there are safeguards in place on end user devices to protect them.		Y	Y
			3. Implement processes to revoke lost or compromised credentials.		Y	Y
		Identity federation with your existing identity provider	The Cloud Provider should:-			
			1. Provide support for federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.		Y	Y
			2. Provide details of the authentication scheme.		Y	Y
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'identity federation'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Only use this approach if their existing identity provider uses two-factor authentication.		Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**

11.	**External interface protection** *All access to service interfaces should be constrained to authenticated and authorised individuals.*	Internet **AND/OR** Community network **AND/OR** Private network	The Cloud Provider should:-			
			1. Implement a Protective Monitoring solution.		Y	Y
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'external interface protection'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Ensure their system has Web Application Firewall (WAFs) protection. This may be provided by the Cloud vendor or a third party.		Y	Y
			2. Ensure that the implemented design protects data by ensuring it is at least two 'firewall' hops from the external network, architected in such a way that the compromise of one firewall will not affect the other.		Y	Y
			3. Correctly implement firewall rulesets using the *"Deny All" First* and then *Add Exceptions* principle.	Y	Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
12.	**Secure service administration** *Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant*	Known service management architecture	The Cloud Provider should:-			
			1. Provide Supplier Assertions regarding their service management architecture.	Y	Y	Y
			2. Ensure access is only available over a secure channel.	Y	Y	Y
			3. Limit management actions to authorised staff.	Y	Y	Y
			4. Audit all management actions.	Y	Y	Y

	impact, including the means to bypass security controls and steal or manipulate large volumes of data. *The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.*		5. Regularly (daily) review the logs to identify any irregular activities.		Y	Y
			6. Have separate user accounts for administration and normal user activities. They should not user their administration accounts for normal business activities.	Y	Y	Y
			7. Not be able to browse the internet or open their external email in the same processing context as they manage systems.	Y	Y	Y
			8. Protect the integrity of the end user devices used to manage the service.	Y	Y	Y
			9. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'secure service administration'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
13.	**Audit information for users** *You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a*	Data made available	The Cloud Provider should:-			
			1. Record system events in near real-time to provide an audit log.	Y	Y	Y
			2. Ensure that the audit logs are tamperproof.	Y	Y	Y
			3. Ensure that the retention period for the logs can be defined by the customer.	Y	Y	Y
			4. Provide a secure facility to forward / export the logs off the cloud infrastructure.	Y	Y	Y

	direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.		5. Provide facilities to allow logs pertaining to their own systems to be human readable.	Y	Y	Y
			6. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'auditing facility'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y
			The Service User should:-			
			1. Use the audit data as part of an effective pro-active monitoring regime.	Y	Y	Y
Ref	**Security Principle**	**NHS Recommended Approach**	**NHS Guidance**	**Class I/II**	**Class III**	**Class IV/V**
14.	**Secure use of the service** *The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.*	Enterprise managed devices **AND/OR** Partner managed devices **AND/OR** Unknown devices	The Service User should:-			
			1. Use a security hardened master operating system image to build guest servers.	Y	Y	Y
			2. Utilise integrated security monitoring and policy management facilities to help detect threats and weaknesses, due to poor design or mis-configuration.	Y	Y	Y
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'security monitoring'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		Y	Y

9 Appendix B

The IT Services that are offered by NHS Digital are assigned a Service Classification. This approach reduces the complexity of service offerings and provides guidelines to making informed service choices for new services. The following table provides summary details for each of the four Service Classifications.

Service Classification	Service Characteristics
Platinum	• Typically, critical national services. • Absence of system leads to complete failure of dependent systems and services with a high possibility of clinical safety issues. • Service interruption results in severe reputational damage. • 24x7x365 Support required. • Service Availability – 99.9%. • DR Recovery target 2 hours. • Monthly MI reporting. • Example service – Spine.
Gold	• Predominantly transactional services. • Absence of system leads to operational difficulties that can be coped with for a limited period. • Absence of system may lead to increased risk to clinical care. • 8-6 Mon to Sat Support required. • Service Availability – 99.9%. • DR Recovery Target 4 hours. • Monthly MI reporting. • Example service – POS/DSCRO
Silver	• Predominantly data capture, batch processing. • Absence of system leads to operational difficulties, but these are manageable for an extended period. E.g. 1 day. • Absence of system may lead to a slight increase in clinical risk Business Hours Support (8am-6pm) Mon-Fri (not BH). • Service Availability – 99.5%. • DR Recovery optional - dependent on outcome of business impact analysis. • Monthly MI reporting. • Existing service – SUS, HES.
Bronze	• Business Hours Support (8am-6pm) Mon-Fri (not BH). • Service Availability – 98%. • DR Recovery optional- dependent on outcome of business impact analysis. • Ad Hoc MI reporting. • Existing service – Parliamentary questions/publications.