Cookbook for Regional Interoperability Detailed Design Paper #016

Securing the YHCR

PRELIMINARY DRAFT

Version 1.0 – 26th May 2019

Abstract Interoperability Cookbook Anchor Points

Section	Title
8	Security

Table of Contents

Version Control

Version	Release Date	Released By	Reason for Release
1.0	26/05/2019	R Hickingbotham	Preliminary draft

Reviewers

Initials	Name	Role	Organisation

1 Introduction

1.1 Purpose of this Document

This document is one of a series of design papers which underpin the Abstract of a Cookbook for Regional Interoperability (the Abstract Cookbook). These papers, in their totality, describe the technical components and the standards which form the YHCR System of Systems. They are intended as a basis for developing or procuring software and so are expressed at a level of precision which is intended to avoid ambiguity but with a consequence that they are focussed to technical readers.

Design papers are anchored to topics which are discussed in the Abstract Cookbook. They are elaborations of the concepts which were first introduced by the abstract and new content is further detail rather than variations of previously established core principles.

This document (design paper 016 - “Securing the YHCR”) expands on the considerations in the Abstract Cookbook in relation to data protection, boundary protection, and business continuity.

The YHCR is a body which relies heavily on IT to provide services which are essential to everyday life. This puts it within the scope of the EUs Network and Infrastructure Systems (NIS) directive which was adopted into UK statute in May 2018. NIS is intended to establish a common level of security for network and information systems. It also provides a framework for enforcement and penalties for non-compliance.

1.2 About the NIS Directive

The National Cyber Security Centre (NCSC) are the national technical authority under the NIS Regulations, and are therefore responsible for supporting operators of essential services and the competent authorities by publishing guidance and acting as a source of technical expertise.

The Department of Health and Social Care will be responsible for overseeing the operation of the NIS Regulations within the sector. This includes taking enforcement action where necessary. NHS Digital will produce guidance for operators and provide technical support to the Department.

Under the NIS Regulations, operators of essential services are required to report any network and information systems incident which has a ‘significant impact’ on the continuity of the essential service that they provide. NHS Digital will perform an investigation to establish whether there has been a contravention of the principles set out by NIS and if so, may fine the operator.

There are 14 principles of the NHS which are classified in 4 objectives:

- Objective A: Managing Security Risk.
- Objective B: Protecting Against Cyber Attack.
- Objective C: Detecting Cyber Security Events.
- Objective D: Minimising the Impact of Cyber Security Incidents.

The National Cyber Security Centre (NCSC) has interpreted the principles in terms of indicators of good practise and has published these in its Cyber Assessment Framework (CAF). Following with the indicators of good practice is a basic indication of compliance with NIS and so these must be a guiding force in the design of the YHCR, its governance structures, and its operating procedures.

1.3 Relationship Between this Document and the CAF

This document is primarily intended to provide a design which addresses security risks. Here security risks are defined as:

- the risk of loss of data;
- the risk of unauthorised access to data;
- the risk of data corruption;
- the risk of loss of service.

The document uses the CAF as a checklist to ensure completeness. Complying with the CAF is more than software and infrastructure design. The CAF also prompts for cyber security aware organisational structures and operating processes. These topics are outside of the scope of this document. NIS objectives A “Managing Security Risk” and D “Minimising the Impact of Cyber Security Incidents” are wholly aligned to people and process and are not part of the checklist. The scope of this paper is defined by Objectives B “Protecting Against Cyber Attack” and C “Detecting Cyber Security Events”. These last two objectives, and the associated NHCS guidelines are included as appendices to this paper.

1.4 Domain of Responsibility and Domain of Interest

What constitutes the boundary of the YHCR is not immediately clear nor is the extent of the responsibility of the organisation which operates the YHCR has for security weakness in organisations connecting to the YHCR or the actions of the people they employ. The YHCR is a service which is used to connect data providers with data consumers. Whilst some data may be persisted centrally, access to that data will in the main will be from data consumers and users over which the YHCR has no control.

This document offers a definition for the demarcation of responsibilities between the organisation that operates the YHCR and the organisations that provide to it or consume data from it. Ratification of this definition is the responsibility of the LHCRE Programme Board, and this could be seen as necessary to comply with the NIS security principles for Objective A “Managing Security Risk”.

The definition uses the concepts of:

- **Domain of Responsibility**: assets which comprise the YHCR and for which the organisation operating the YHCR operates and defines the scope of the YHCR for the purpose of the NIS directive.
- **Domain of Interest**: assets which are operated by organisations connecting to the YHCR which, if the subject of a security breach, would impact the service available from the YHCR or could lead to data loss, corruption or leakage from other organisations connecting to the YHCR.

The YHCR's domain of responsibility, here, is defined to be:

1. The regional software that facilitates relationships between data providers and data consumers including: the Identity and Access Management Server (design paper 005), the FHIR Aggregator (design paper 010), PIX/MPI (design paper 004), the Regional FHIR Store (design paper 018) and any other software hosted centrally.
2. The infrastructure which hosts regional software and the networks which enable data consumers to connect to the regional software and the regional software to connect to the IP address and port of data provider endpoints.
3. Data held centrally including master resources for patients, organisations, locations and practitioners; audit transactions; endpoint registration data; patient data maintained in the regional FHIR store.
4. The people and processes which support the regional software and infrastructure; apply software updates; onboard contributors to the YHCR; investigate potential misuse; and monitor the YHCR.

Within the domain of responsibility, the organisation that operates the YHCR has a potential liability for any security breach, misuse, or outage, caused by any of the above assets.

The domain of responsibility ends at the IP address at the data provider or data consumer connecting with the YHCR and at this point the domain of interest begins. The domain of interest includes all software, infrastructure, data, people and processes within data providers and data consumers. Any security breach, misuse, or outage caused by any of these assets is the responsibility of, and potential liability rests with, the organisations that are acting as data providers or consumers.

The domain of responsibility and domain of interest are illustrated below:

§omain of interest is so called because breaches in this domain have the potential to impact the service offered by the YHCR and also to cause reputational damage to the YHCR. A possible treatment of these dependencies for the purpose of the NIS directive is view data providers and data consumers as the "Supply Chain". In which case the YHCR has an obligation as set out below.

"*The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers.*"

This document, and other design papers, set out mechanisms for promoting and ensuring compliance with good cyber security practices for data providers and data consumers.

Refer to, in particular, design paper 014 - "Governance for Data Providers", paper 015 - "Governance for Data Consumers", paper 020 - "Onboarding Data Providers", and paper 022 - "Onboarding Data Consumers".

1.5 Relationship of this Document with Other Standards

The following standards form the basis for this document:

- The Transport Layer Security (TLS) Protocol Version 1.2 - RFC 5246.
- The Transport Layer Security (TLS) Protocol Version 1.3 - RFC 8446.

- NCSC Cyber Assessment Framework (CAF)

1.6 Intended Users of the This Document

This document is a reference guide for developers and operators of YHCR regional infrastructure, data providers and data consumers

2 Boundary Protection

Boundary protection is a key mitigation to security risks for the YHCR. it ensures that only authorised participants are able to connect and exchange data. To protect the boundary of the domain of responsibility the YHCR must be able to:

- identify those organisations who are authorised to use its services;
- ensure that inbound connections into YHCR service emanate from an IP address operated by an authorised participant;
- ensure that outbound connection from the YHCR are to an IP address operated by the organisation to which the connection was intended;
- identify and investigate a potential breach of these conditions.

In relation to the domain of interest the responsibility of the YHCR extends to:

- publishing conditions of membership which establish the terms on which data provider and data consumers will operate;
- auditing compliance with conditions of membership;
- monitoring for non-compliance;
- continuous testing of compliance where feasible.

2.1 A Secure Public Network

The YHCR must be able to operate securely using public cloud hosting for regional infrastructure and services. However, the network endpoints which represent regional services, data provider services, and connection points from data consumers must operate privately and must not be accessible to anyone outside the membership of the YHCR. The YHCR will achieve this by using a public key infrastructure with the following features.

2.1.1 The YHCR Membership Registry

The YHCR will maintain a registry of participating organisations. The contents of the registry will be accessible by participants from a RESTful service, the implementation of which is described in design papers 020 – “Onboarding Data Providers” and 021 – “Onboarding Data Consumers”.

Participants will be classified as:

- known to the YHCR but with no access rights;
- onboarding to the YHCR, the participant has access to sandpit services;
- full member of the YHCR, the participant has access to live services.

The YHCR administrating organisation will be registered as a participant. Other participants will be classified as data providers, data consumers or both. Access rights will be enforced through the use of certificates. A senior officer (usually the CIO) will be recorded for each participating organisation. Reliance will be placed on the identity of the senior officer and contact details will be verified.

2.1.2 YHCR as a Certificate Authority

The YHCR will operate as a root certificate authority and will sign certificates which are used by data providers and data consumers to secure endpoints. Separate certificates will be issued to the administrating organisation, data consumers, and data providers. A data consumer will also use a certificate signed by the YHCR root CA for signing claims made to IAM (design paper 005 – "Identity and Access Management Service".

The YHCR will publish its public key certificate for outbound connections.

Regional services, data providers, and data consumers will secure listening ports and will only accept connections from YHCR certificate holders as follows:

Service	Acceptable Connections			
	YHCR	Provider	Consumer	Admin.
IAM authorisation service			X	
IAM validate token service		X		
IAM revoke token service		X	X	X
Data provider FHIR service	X		(1)	
Data provider asynchronous results	X		(1)	
Regional FHIR aggregator			X	
Regional PIX encounter register		X		
Regional subscription REST hook		X		
Consumer subscription REST hook	X	(2)		
Regional messaging service		X		
Consumer messaging service	X			
Regional registry services		X	X	X
YHCR system software				X

(1) Most data providers will only interact with the regional FHIR aggregator, but some may choose to allow privileged consumers direct access. In these cases, the provider chooses to allow connections from nominated consumers. It is the responsibility of the provider to ensure that the trusted certificate correctly identifies the consumer.

(2) Most subscription consumers will only accept subscription results from the regional subscription broker, but some may choose to allow privileged providers to delivery subscription results directly. In these cases, the consumer chooses to allow connections from nominated providers. It is the responsibility of the consumer to ensure that the trusted certificate correctly identifies the provider.

Note that the certificate identifies the organisations which holds not their role in the YHCR. The YHCR regional services will determine the role from the YHCR membership registry. Most other participants will only interact with the YHCR regional infrastructure and will only explicitly trust the certificates of the YHCR itself. If it wishes to have a direct relationship with other participants, then it will also explicitly trust the certificates of those organisations on a case by case basis as in notes (1) and (2) above.

All certificates will be issued to YHCR domain name. All connections must be mutually authenticated to ensure that connection addresses correspond to the domain name and IP address. Note that this implies that connections for a data consumer must be presented to the YHCR from a single IP address with implication that proxy software may be needed to abstract the YHCR from the addresses of individual clients.

Certificates are issued for use with TLS 1.2 and TLS 1.3.

2.1.3 The YHCR Domain

The YHCR will control the domain yhcr.nhs.uk and will operate a domain name server. Address records will be set up for all participating organisations' network endpoints.

The integrity of DNS records is key to the security of the YHCR. A system administrator with the ability to both sign certificates and to manage DNS entries could open up unauthorised access to the YHCR. It is strongly recommended that operators of the YHCR segregate duties for:

- managing the participant registry;
- signing certificates;
- managing DNS entries.

2.1.4 YHCR Exclusive Port Usage

Ports used by all participants for YHCR services will be used exclusively for YHCR services. Connections will only be possible over a protocol secured with an appropriate YHCR certificate.

2.1.5 Validating Identity of Participants in YHCR

The security of the private public networks relies wholly on the correct identification of certificate holders. The certificate signing process must ensure that identity of the certificate holder is proven. Certificate signing should be software controlled has follow the following process:

1. A certificate signing request (CSR) is sent by participating organisation to a YHCR email address.
2. The CSR is associated with an organisation registered in the membership registry.
3. Details of the CSR are validated against entries in the membership registry.
4. The senior officer is emailed to verify the authenticity of the request.
5. The response determines whether the CSR is processed.
6. A signed certificate is registered in the membership registry.

The process must prevent multiple certificates being issued to the same participant for the same purpose but must allow replacement of expired certificates in advance of the expiry date.

Revocation of certificates will also be software controlled.

The root CA private key must be maintained securely with highly restricted access privileges.

2.2 Assuring Compliance

The onboarding process (detailed in design papers 020 and 021) will validate through a mix a self-assessment and testing that that the conditions for membership of the YHCR are complied with. Continuous assessment will provide ongoing assurance that key aspects of the security regime continue to be complied with.

Automated compliance monitoring software will periodically probe network endpoints of the YHCR services, data provider services and data consumer services to ensure that:

- an unsecure connection is not possible;
- a connection is not possible using an expired certificate or certificate not signed by the YHCR;
- a FHIR request is not accepted without a bearer token;
- a FHIR request is not accepted if the bearer token is expired or not signed by the YHCR;
- IAM does not authorise a request for an unsigned claim;
- IAM does not authorise a request for a claim signed by an expired certificate or certificate not signed by the YHCR;
- audit records are created by the YHCR FHIR aggregator;
- audit records are created by data providers [(2)];
- subscriptions can only be revoked by the consumer that created the subscription [(1)];
- asynchronous result sets can only be collected by the consumer that placed the search [(1)];
- a subscription delivery channel must be pre-registered in the membership registry [(1)];
- access for the purpose of direct care only allows access to patient identifiable data for the patient in context [(1)];
- access for the purpose of indirect care or analytics requires the consent of the patient [(1)];
- access for the purpose of administration does not permit access to patient identifiable data[1)].

(1) Mitigations for threats identified in section 3.
(2) Audit capabilities are tested by issuing a FHIR search and then requesting the corresponding audit record.

It is recommended that responsibility for operating automated compliance monitoring software is segregated from responsibility for maintaining other YHCR regional infrastructure.

2.3 Auditing of Access

Design paper 009 – “Auditing” details the approach to secure, tamper-proof, logging access to the YHCR and auditing YHCR usage.

2.4 Denial of Service, Malware, and Breach Protection

Regional components of the YHCR will be hosted in the public cloud. The hosting organisation will be contracted to provide measures for protecting against a threat of attack and will be asked to provide and regularly update evidence of steps taken.

Participants in the YHCR, including the organisation responsible for its operation, will be require to:

- configure firewalls to mitigate the threat of denial of service attacks;
- comply with NHS Digital’s guidance on malware protection;

- deploy modern breach detection tools.

2.4.1 Containment

A participant to the YHCR which is subject to an attack must:

a) Inform the organisation operating the YHCR of the attack (the process is detailed in the YHCR Operations Guide).
b) Shutdown firewalls or routers which permit access to YHCR regional services or allow access from the YHCR into local service.
c) Only re-establish connection when the attack has been cleared.

2.4.2 Reporting and Root Cause Analysis

An analysis of the cause of any breach, whether as a result in the weakness the domain of responsibility or outside will be promptly performed by the organisation responsible for operating the YHCR. The breach and root cause analysis will be reported to the YHCR Board and NHS Digital.

2.5 Firewall Configuration

Regional firewalls are configured to allow access to services only to organisations registered in the membership registry. Firewall configuration files are periodically, automatically, reconciled to the membership registry. Specifically, an internet connection is not possible from any of the components which comprise regional infrastructure.

2.6 Vulnerability Assessments

The YHCR team will undertake periodic vulnerability assessments the results of which will be provided to the YHCR Management Board. Actions arising will be tracked.

The YHCR team will included cyber-security experts who monitor emerging threats and belong to networks which give early visibility of new malware and attacks

2.7 Patch Management

Patches to system software will be assessed and applied within 72 hours of the patch being publicly available. A log will be maintained of any patches not applied and the reason for the decision

3 Data Protection

The security risks of data loss, corruption, and unauthorised access can be interpreted differently in the domain of responsibility, where the YHCR acts mainly as a data conduit with relatively low levels of data persistence, from the domain of interest where data providers are custodians of long lasting data, and data consumers expose data to end users with the potential for misuse.

3.1 Data in Motion

The YHCR acts a conduit for data in the following circumstances:

- a FHIR operation is executed by a data consumer and serviced by the YHCR with data sourced from data providers;
- a subscription result is sent from a data provider and distributed by the YHCR to data consumers;
- a data consumer issues an asynchronous search, the YHCR acts a proxy for the data consumer in collating and releasing search results;
- a reliable message is sent from one participant to another and the YHCR acts as an intermediary in message delivery.

In all cases data is held only transitorily in the YHCR. But data is persisted, albeit only for a short period of time, in the following situations:

- Data passing between components in the YHCR is persisted as messages. Persistence allows troubled software to be recovered without data loss and provides means for problem diagnosis. Message content is purged regularly.
- Subscription data and messages for delivery to a consumer are lodged in a queue. The queue allows attempts to deliver the data to fail and be retried. The queue is emptied when data is delivered.
- Asynchronous search results are collected from data providers and cached in the YHCR for collection by the data consumer. The cache is cleared when they are collected.

Persistence is a mitigation against data loss but is the source of certain threats which leads to the risk of unauthorised access.

The following risks, threats and mitigations are noted:

Risk	Threat	Mitigation
A FHIR result from a data provider is lost in the YHCR and not returned to a consumer.	A software error causes a result set to be lost.	Automated regression testing.
		Rigorous software deployment process.
	A consumer connection times-out before results are assembled and delivered from the YHCR.	The data consumer will be aware of the timeout and is able to respond accordingly.
Subscription results are not relayed to the consumer registering the subscription.	A software error causes a subscription result to be lost	Automated regression testing.
		Rigorous software deployment process.
	A system administrator corrupts data relating consumer subscriptions to provider subscriptions.	Segregated access control restricts access to live operational data to privileged individuals.

Risk	Threat	Mitigation
		A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted. Automated integrity checking software automatically revalidates relationships between consumer and provider subscriptions.
	An external entity modifies data relating consumer subscriptions and provider subscriptions or revokes a subscription.	Subscription data cannot be modified through an API other than the FHIR API which permits the subscription to be revoked. Boundary protection measures ensure that access is only available via the published API. A subscription can only be revoked by the consumer that created the subscription and this is ensured by automated compliance monitoring. The revoking consumer is identified by the X509 certificate used to gain access to the API.
	Subscription results are not delivered to a data consumer because of a consumer-side system outage.	Subscription result delivery operates on a queue. Queues are persisted. Delivery is reattempted ad-infinitum if delivery fails. Results are only removed from the queue on successful delivery or if removed by a system administrator. Segregated access control restricts access to queue management functionality to privileged individuals. A log is maintained for the reason for of all system administrator intervention. Audit logs are maintained of items deleted from queues. Audit logs are

Risk	Threat	Mitigation
		forensically processed, and abnormal activities alerted.
Asynchronous results sourced from a data provider are lost in transit.	A software error causes a result set to be lost.	Automated regression testing.
		Rigorous software deployment process.
	A system administrator corrupts the result set cache.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted.
	An external entity corrupts the result set cache.	Asynchronous result sets are only accessible via the asynchronous data collection REST service. Boundary protection measures ensure that access is only available via the published API. An asynchronous result set can only be collected by the consumer that placed the asynchronous search request and this is ensured by automated compliance monitoring. The consumer is identified by the X509 certificate used to gain access to the API.
Asynchronous results are not collected by the FHIR aggregator from the data provider.	A software error causes the existence of a source for an asynchronous result set to be lost.	Automated regression testing.
		Rigorous software deployment process.
	A system administrator corrupts the data relating the consumer search to searches placed with data providers.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted. Automated integrity checking software automatically revalidates

Risk	Threat	Mitigation
		relationships between consumer and provider searches.
	An external entity corrupts the data relating the consumer search to searches placed with data providers.	This data is not accessible via an API. Boundary protection measures ensure that access is only available via published APIs.
	An outage at the data provider means that search results are not collected.	Search result collection operations are queued. Queues are persisted. Delivery is reattempted ad-infinitum if delivery fails. Results are only removed from the queue on successful delivery or if removed by a system administrator. Segregated access control restricts access to queue management functionality to privileged individuals. A log is maintained for the reason for of all system administrator intervention. Audit logs are maintained of items deleted from queues. Audit logs are forensically processed, and abnormal activities alerted.
Message data is lost in transit.	The YHCR Regional Messaging Intermediary loses a message through software error or system administrator action.	Design 006 establishes the principle of a reliable messaging infrastructure that guarantees delivery from source to target,
A FHIR result from a data provider, a subscription result, an asynchronous result set or a message is corrupted in transit.	A software error causes the existence of a source for an asynchronous result set to be lost.	Automated regression testing.
		Rigorous software deployment process.
		FHIR resources in transit through the FHIR Aggregator can be optionally validated against the YHCR FHIR profiles. Validation will be performed on a sample basis.
	A system administrator corrupts data in transit.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are

Risk	Threat	Mitigation
		forensically processed, and abnormal activities alerted.
	An external entity corrupts data in transit.	This data is not accessible via an API. Boundary protection measures ensure that access is only available via published APIs.
Subscription results are distributed to the wrong consumer endpoint leading to unauthorised access to data.	The data consumer provides an invalid distribution channel in the subscription request.	The YHCR validates the endpoint against the one registered for the consumer in the membership registry. Automated integrity checking software automatically validates this restriction.
	The distribution channel endpoint is wrongly recorded in the membership registry.	Requires collusion between the data consumer and the YHCR operations team. Endpoints must be secured by a YHCR signed certificate. This is testing through the automatic integrity testing tool. The certificate signing process involves authorisation from a senior officer at the data consumer.
	A system administrator modifies the subscription distribution channel.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted. The endpoint must be one secured by a YHCR signed certificate. The certificate signing process ensures that the endpoint is registered to a known participant in the YHCR.
An asynchronous result set is picked up by an unauthorised recipient.	An external entity invokes the asynchronous data collection REST service.	An asynchronous result set can only be collected by the consumer that placed the asynchronous search request and this is ensured by automated compliance monitoring.

Risk	Threat	Mitigation
		The consumer is identified by the X509 certificate used to gain access to the API.
	A system administrator modifies the source of an asynchronous search request thus allowing unauthorised collection.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted. The recipient must be registered in the membership registry and have gone through the certificate signing process.
A message is distributed to an unauthorised recent.	The message source provides an invalid destination endpoint in the message header.	The YHCR *MessageHeader* profile obsoletes the destination endpoint URL, instead this is derived from the recipient organisation. The recipient must be registered in the membership registry and have gone through the certificate signing process. Messages will only be delivered to endpoints secured by a correct YHCR signed certificate.
	A system administrator modifies the destination organisation in a message header.	Segregated access control restricts access to live operational data to privileged individuals. A log is maintained for the reason for of all system administrator modified data. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted. The recipient must be registered in the membership registry and have gone through the certificate signing process.
Unauthorised access is gained to transient persisted data.	A system administrator accesses transient data and releases it to a third party.	Transient data is stored in encrypted databases.

Risk	Threat	Mitigation
		System software which allows access to transient data can only be accessed from nominated computers and IP addresses. A firewall limits access from administrator computers to YHCR infrastructure and have no external storage connections. Segregated access control restricts access to live operational data to privileged individuals. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted.
	An external entity accesses transient data.	This data is not accessible via an API. Boundary protection measures ensure that access is only available via published APIs.

3.2 Data at Rest

The YHCR persists data centrally as follows:

- master data which allows a unified representation of patients, practitioners, organisations, and locations to be presented across the region;
- the membership registry;
- configuration data for YHCR components;
- audit data;
- policies and records of consent;
- patient identifiable data.

This last category is a catch all for clinical records which are held centrally for any reason. Some of the reasons may be:

- the data has been derived by an algorithm which is hosted regionally, for example, a frailty index;
- responsibility for managing the data is shared between clinicians and administrators working at different care settings and central storage is convenient for the application, for example, an end-of-life care plan.

Centrally persisted data is held mainly in the regional FHIR Store (design paper 018), the exceptions being the membership registry and component configuration data. API based read only access is provided to the membership registry. Configuration data is only accessible to operators through a file system or dedicated management portals.

Generally, data in the regional FHIR Store can be accessed through the FHIR Aggregator by any data consumer authorised to assume an appropriate regional role. Access rights are defined by design paper 005 - "Identity and Access Management" and these derived for data consumer's reason for access and the regional role they perform. Access rights may be modified by policies operated by data provider or regional consent enforcement (design paper 008 – "Data Access and Consent Management").

Access rights which are enforced regionally can be summarised as follows:

Reason for Access	Regional Role	Scope of Access	Regional Consent Enforcement
Direct care (Emergency)	Clinical Professional	Patient identifiable data (1) is only accessible for the patient in context.	(2)
	Social Care Professional		
	System or Robot		
	Citizen	Patient identifiable data (1) is only accessible for the patient in context. Data is presented by data providers in a manner suitable for non-care professional consumption.	(2)
	Authorised Carer		
Direct care (Non- Emergency)	Clinical Professional	Patient identifiable data (1) is only accessible for the patient in context.	(2)
	Social Care Professional		
	System or Robot		
	Citizen	Patient identifiable data (1) is only accessible for the patient in context. Data is presented by data providers in a manner suitable for non-care professional consumption.	(2)
	Authorised Carer		
Indirect care with the consent of the patient.	Clinical Professional	Patient identifiable data (1) is only accessible for the patient in context.	yes
	Social Care Professional		
	System or Robot		
Indirect care not in the context of a patient.	Clinical Professional	Access is permitted to all data including cross patient searches.	yes
	Social Care Professional		
	System or Robot		
Analytics with access restricted to pseudonymised data.	System or Robot	Access is permitted to all data including cross patient searches.	yes
Administration	Administrator	Any data held in the regional FHIR store other than *AuditEvents*. No rights to data held at data providers.	no
	Auditor	Access to centrally and locally held *AuditEvents*	no

(1) The definition of patient identifiable data is provided by design paper 005 – "Identity and Access Management"

(2) Consent is not required for the purpose of direct care except in special situations such as when data is controlled by the patient themselves or is not relevant to direct care. These situations are managed by nominating particular data sources as requiring consent/

The above access rights apply to reading data. Individuals may also have rights to create and update data in the regional FHIR Store and to post resources to local data providers. The following rules apply to creating and modifying data:

- Only a citizen may create or revoke a *Consent* resource. The subject of the resource must be the citizen themselves. The resource is managed through the regional FHIR Store API.
- A data subscribe may create or revoke a *Subscription* resource. The resource is created in the context of the data consumers access (reason for access and role) and access rules applied to subscription results in this context. The resource is managed through the regional FHIR Store API.
- Patient identifiable resources may only be managed in the regional FHIR Store by a person with a regional persona and with an appropriate regional role (design paper 006 – "Identity and Access Management"). Regional role definitions include rules which restrict management activities to specified data points. A regional role can only be assigned to a regional identity by a system administrator.
- Data required for the operation of the YHCR including master Patient, Organisation, Practitioner, Location and Linkage resources cannot be managed through the FHIR API and requires a system administrator to make changes.
- Resources posted to a local data provider will be accepted or rejected based on the claim made by the data consumer in accessing the YHCR and embedded in the bearer-token (design paper 006 – "Identity and Access Management").

The following risks to data at rest are noted:

Risk	Threat	Mitigation
Consent records do not reflect citizen wishes resulting in unauthorised disclosure of data.	A system administrator modified or deletes a Consent resource or Policy definition.	Data at rest is encrypted and can only be modified through a user interface. Segregated access control restricts access to the FHIR Store to privileged individuals. All management activities are logged. Audit logs are forensically processed. Management of Consent or Policy resources is an abnormal activity that would be flagged for investigation.
	A citizen misconstrues the intent of consent or misunderstands policy wording.	Policies are lodged in the regional FHIR Store which provides a single source of policy wording which is reused regionally. Policy wording is reviewed and approved through a formal process. Data consumers presenting policies and capture consent are accredited centrally. Only accredited consumers are registered with the YHCR and have access to YHCR data.
	A mismatch between policy wording and data rules cause the policy to be incorrectly applied.	Policy rules are treated as code and follows the same process for testing, sign-off and migration to live operation.

Risk	Threat	Mitigation
A consumer accesses data not permitted by their reason for access or role.	A misclassification by the FHIR Aggregator of resources causes patient identifiable data to be released for a patient other than the one in the current context.	Automated compliance monitoring assures correct classification of resources.
	A software error resulting in the misinterpretation of reason for access or role by the FHIR Aggregator allows access to protected data.	Automated compliance monitoring assures correct interpretation of the reason for access and role.
A YHCR user has inappropriate access to regionally held clinical data.	A regional role was wrongly allocated to a regional persona.	Segregated access control restricts access to the regional personas to privileged individuals. A supervisor reviews newly assigned roles. Reports of user roles are regularly distributed to data consumers.
	The role is incorrectly defined and incorrectly permits access to data points.	Role definitions are treated as code and follows the same process for testing, sign-off and migration to live operation.
	A system administrator accesses clinical data and releases it to a third party.	Clinical data is stored in encrypted databases. System software which allows access to the FHIR store can only be accessed from nominated computers and IP addresses. A firewall limits access from administrator computers to YHCR infrastructure and have no external storage connections. Segregated access control restricts access to live operational data to privileged individuals. Audit logs are maintained of access to operational data. Audit logs are forensically processed, and abnormal activities alerted.
Data is disclosed data to a third party not connected to the YHCR.	A YHCR database administrator copies data and the media falls into the hands of a third party.	The network of the organisation managing the YHCR connects to regional components from a single IP address. Only devices provided by the YHCR may connect to this network. Device management is enforced through a directory service.

Risk	Threat	Mitigation
		The storage of YHCR devices is encrypted and connection to external storage is not possible. An internet connection is not possible from the network of the organisation managing the YHCR. YHCR staff are trained in security awareness.
	An end user at a data consumer copies data and the media falls into the hands of a third party.	The threat is within the domain of interest and is not directly controllable by the YHCR. Data consumers are accredited when onboarded to the YHCR. The onboarding process involves a assessment of local security measures. The YHCR monitors for unusual activity at a data consumer which includes bulk access to data.

4 Business Continuity

Design paper 021 – "Non-Functional Requirements for Regional Infrastructure" details how regional components will be operated using cloud services with the objective of providing a highly available environment.

This section offers a precis of design paper 021 to support completion of the CAF assessment for Objectives B and D.

4.1 Cloud Hosting

All regional components will be hosted in the public cloud as services or software running on virtualised infrastructure. The cloud environment will provide for redundancy of in key network components and services (firewalls, load balancing devices, routers, storage as a service, DNS, directory services).

4.2 Network Resiliency

Services will be multi-homed: occupying more than one IP addresses with different backbone network provider servicing each IP address.

4.3 Scalability and High Availability

All regional components other than storage are stateless and parallel components will be run on multiple nodes in an active-active configuration. Load-balancing devices will distribute transactions between nodes. The failure of any one node does not lead to a loss of service. Nodes can also be pulled from live operation for maintenance without loss of service. Nodes will be distributed across physical data centres reducing the potential for catastrophic loss.

Databases will be mirrored across physical centres in an active passive configuration. Loss of an active service will result in automatic failover to a passive node.

High volume data which is persisted centrally (the regional FHIR store) be sharded by logical identifier so allowing data to be distributed across servers, enabling the solution to be scaled horizontally, and reducing the business impact of a failed shard.

4.4 Backup and Recovery

The cloud operator will manage snapshotting of virtualised environment and backup of storage as a service.

Database journals and logs will be persisted in cloud storage as a service enabling current database state to be recovered from a machine snapshot.

Recovery of data from backup is scripted and scripts are tested regularly.

4.5 Disaster Recovery

Cloud services will be distributed across physical data centres. Recovery of individual components and recovery of a whole service will be scripted and rehearsed regularly. The component- based architecture of the YHCR facilitates segregation of functionality between autonomous services and minimises the risk of a complete outage.

5 YHCR Administration and Operations

5.1 Source Control and Release Management

Source code for all YHCR components will be maintained in a public source code repository. The master branch for all components will contain the code deployed to live operations. The repository will be branched for projects and releases. A project is controlled by an individual developer where s a release branch comprises the pull requests (a group of changes) from one or more projects and is intended as a candidate for migration to live operation. A release manager will determine which candidate changes will comprise a release and will be responsible for merging pull requests from projects with the release branch and, on go-live, merging the release branch with the master branch.

Developers have commit rights only to project branches. Only active developers have commit rights. An onboarding/offboarding process will ensure that rights are managed.

Developers build and test on their own private environment. The YHCR offers centralised environments for:

- integration testing where targeted testing of a release will occur;
- staging where high-volume, automated regression testing will occur;
- live operations;
- onboarding, an identical environment to live which operates on synthetic data.

Only the release manager will have rights to deploy code in these environments. The release cycle will promote a release from integration testing through staging and then to live/onboarding. The release cycle will run weekly

5.2 Administration, Support and Operations People and Roles

The YHCR team will perform the following functions:

- onboarding of YHCR participants;
- development of bug fixes and new functionality;
- support and problem investigation;
- security assessment and breach detection;
- housekeeping including backups and patching of system software.

There is sufficiemt duplication of function in the team to avoid dependency on any one individual.

Roles definitions are orientated around these functions and are designed to segregate duties where there is a security implication. Segregation includes:

- developers not have access to the configuration of components in hosted environments;
- staff onboarding new participants do not have access to software used in the generation of security certificates or to firewall configuration;
- database administrators to not have access to audit data or system logs;
- support staff have read only access to configuration, message traces and persisted data;
- system administrators do not have access to data;

- administrators of DNS and network directory service have no access to any of the regional components or infrastructure on which they operate.

YHCR management processes are documented and all staff will follow an induction programme which requires their confirmation that they have read and understood appropriate material.

The YHCR operations team reports to the YHCR board. Compliance with security procedures and processes and an assessment of risk is presented to the board on a quarterly basis.

Cyber-security training is provided to all members of the Operations team. The appropriateness and currency of the training is regularly reviewed alongside emerging threats.

5.3 Network and Device Security

The network of the organisation operating the YHCR connects to regional components from a single IP address. A virtual private network (VPN) connects components hosted in the public cloud with the physical network of the operator. The VPN is secured using a certificate issued by the YHCR. A directory service centralises management of users and devices which may connect to the network. Only devices registered with the directory service may connect to the network.

Two form-factor authentication is required to access a device and to the management console of regional components.

All devices are supplied by the YHCR. No user of a device has administrative privileges and only software installed by a network administrator is permitted.

The storage of YHCR devices is encrypted and connection to external storage is not possible, except from nominated devices which are physically secured and to which only privileged system administrators have login rights. Transfer of data and programme code from these devices onto and off the network are logged.

Malware protection software is installed on all devices and this regularly updated.

An internet connection is not possible from the network or devices connecting to it. Interaction with the source code repository for the purpose of preparing a code release is undertaken from an off-network device. Code and data is transferred onto the network by the mechanism described above.

5.4 Maintenance of Security Policies and Procedures

A security assessment is performed for all code changes made to regional components. A material change in service triggers a full review of operating policies and procedures. The results of the review are communicated to the YHCR board.

5.5 Service Monitoring

5.5.1 Service Abuse Detection

Design paper 009 – "Auditing" sets out the technical requirements for indexing audit data which enables usage of the YHCR to be monitored and suspicious patterns of use to be identified. The design paper sets out some initial use cases but the sophistication of these is expected to evolve over time.

5.5.2 Boundary Protection Monitoring

The YHCR regional components will be hosted in the public cloud. Cloud provider tooling for monitoring attempted breaches of security will be employed.

5.5.3 Service Availability Monitoring

Real-time monitoring software will facilitate visualisation of the operational status and performance of components of the YHCR. Aspects of the service which are monitored will include:

- current availability of all YHCR services;
- spot and historic transaction rates for YHCR services;
- time of last authentication by data consumer;
- number of non-expired bearer tokens issued by data consumer;
- authorization failure rates by data consumer;
- time of last transaction executed with a data provider;
- transaction execution rates by data provider and data consumer;
- average transaction latency by data provider and data consumer;
- transaction failure rates by data provider and data consumer.

Alerts for measurements which fall outside of normal bounds are sent to alert staff.

Appendix 1 – NIS Objective B: Proportionate security measures are in place to protect essential services and systems from cyber-attack.

CAF Guidance for Objective B1: Service Protection, Policies and Processes

B1a - Policy and process development					
You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Your service protection policies and processes are absent or incomplete.	This document	Your service protection policies and processes document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.	This document and in particular .YHCR Administration and Operations	You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these policies and processes and key performance indicators are reported to your executive management.	This document and in particular .YHCR Administration and Operations
Service protection policies and processes are not applied universally or consistently.	YHCR Administration and Operations	You review and update service protection policies and processes in response to major cyber security incidents.	Reporting and Root Cause Analysis	Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies.	This document
People often or routinely circumvent service protection policies and processes to achieve business objectives.	YHCR Administration and Operations			Essential service protection policies and processes that rely on user behaviour are practical, appropriate and achievable.	Administration, Support and Operations People and Roles

Your organisation's security governance and risk management approach has no bearing on your service protection policies and processes.	This document			You review and update service protection policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.	Reporting and Root Cause Analysis Vulnerability Assessments YHCR Administration and Operations
System security is totally reliant on users' careful and consistent application of manual security processes.	This document			Any changes to the essential service or the threat it faces triggers a review of service protection polices.	Maintenance of Security Policies and Procedures
Service protection policies and processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.	Maintenance of Security Policies and Procedures			Your systems are designed so that they remain secure even when user security policies and processes are not always followed.	Boundary Protection Data Protection
Service protection policies and processes are not readily available to staff, too detailed to remember, or too hard to understand.	Source Control and Release Management Administration, Support and Operations People and Roles				
B1b - Policy and process implementation					
You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

Service protection policies and processes are ignored or only partially followed.	Operational Evidence required. YHCR Administration and Operations	Most of your service protection policies and processes are followed and their application is monitored.	Operational Evidence required. YHCR Administration and Operations	All your service protection policies and processes are followed, their correct application and security effectiveness is evaluated.	Operational Evidence required. YHCR Administration and Operations
The reliance on your service protection policies and processes is not well understood.	Operational Evidence required. YHCR Administration and Operations	Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness	Administration, Support and Operations People and Roles	Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.	Administration, Support and Operations People and Roles
Staff are unaware of their responsibilities under your service protection policies and processes.	Administration, Support and Operations People and Roles	All staff are aware of their responsibilities under your service protection policies and processes.	Administration, Support and Operations People and Roles	Your service protection policies and processes are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.	Administration, Support and Operations People and Roles
You do not attempt to detect breaches of service protection policies and processes.	Service Monitoring	All breaches of service protection policies and processes with the potential to disrupt the essential service are fully investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address	Reporting and Root Cause Analysis	Appropriate action is taken to address all breaches of service protection policies and processes with potential to disrupt the essential service including aggregated breaches.	Containment
Service protection policies and processes lack integration with other organisational policies and processes	YHCR Administration and Operations				

Your service protection policies and processes are not well communicated across your organisation.	Administration, Support and Operations People and Roles				

CAF Guidance for Objective B2: Identify and Control Access

B2a - Identity verification, authentication and authorisation					
You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential service					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Authorised users with access to networks or information systems on which your essential service depends cannot be individually identified.	A Secure Public Network Administration, Support and Operations People and Roles	All authorised users with access to networks or information systems on which your essential service depends are individually identified and authenticated.	A Secure Public Network Administration, Support and Operations People and Roles	Only authorised and individually authenticated users can physically access and logically connect to your networks or information systems on which your essential service depends.	A Secure Public Network Administration, Support and Operations People and Roles
Unauthorised individuals or devices can access your networks or information systems on which your essential service depends.	A Secure Public Network Network and Device Security	User access to essential service networks and information systems is limited to the minimum necessary	A Secure Public Network Network and Device Security	User access to all your networks and information systems supporting the essential service is limited to the minimum necessary	A Secure Public Network Network and Device Security
User access is not limited to the minimum necessary.	A Secure Public Network Network and Device Security	You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to sensitive systems such as	A Secure Public Network Network and Device Security	You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to all systems that operate or support your essential service.	A Secure Public Network Network and Device Security

		operational technology.			
		You individually authenticate and authorise all remote user access to all your networks and information systems that support your essential service.	A Secure Public Network Network and Device Security	You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote user access to all your networks and information systems that support your essential service.	A Secure Public Network Network and Device Security
		The list of users with access to essential service networks and systems is reviewed on a regular basis at least annually.	Administration, Support and Operations People and Roles	The list of users with access to networks and systems supporting and delivering the essential service is reviewed on a regular basis, at least every six months.	Administration, Support and Operations People and Roles
B2b - Device management					
You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Users can connect to your essential service's networks using devices that are not corporately managed.	Network and Device Security	Only corporately owned and managed devices can access your essential service's networks and information systems.	Network and Device Security	Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.	Network and Device Security

Privileged users can perform administrative functions from devices that are not corporately managed.	Network and Device Security	All privileged access occurs from corporately management devices dedicated to management functions.	Network and Device Security	You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems, or you only allow third-party devices or networks dedicated to supporting your systems to connect.	Network and Device Security
You have not gained assurance in the security of any third-party devices or networks connected to your systems.	Network and Device Security	You have sought to understand the security properties of third-party devices and networks before they can be connected to your systems. You have taken appropriate steps to mitigate any risks identified.	Network and Device Security	You perform certificate based device identity management and only allow known devices to access essential services.	Network and Device Security
Physically connecting a device to your network gives that device access to your essential service without device or user authentication	Network and Device Security	The act of connecting to a network port or cable does not grant access to any systems.	Network and Device Security	You perform regular scans to detect unknown devices and investigate any findings	Network and Device Security
		You are able to detect unknown devices being connected to your network, and investigate such incidents	Network and Device Security		
B2c - Privileged user management					
You closely manage privileged user access to networks and information systems supporting the essential service.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

The identities of the individuals with privileged access to your essential service systems (infrastructure, platforms, software, configuration, etc) are not known or not managed.	Administration, Support and Operations People and Roles	Privileged user access requires additional validation, but this does not use a strong form of authentication (e.g. two-factor, hardware authentication or additional real-time security monitoring).	Administration, Support and Operations People and Roles Network and Device Security	Privileged user access to your essential service systems is carried out from dedicated separate accounts that are closely monitored and managed	Administration, Support and Operations People and Roles Network and Device Security
Privileged user access to your essential service systems is via weak authentication mechanisms. (e.g. only simple passwords.)	Network and Device Security	The identities of the individuals with privileged access to your essential service systems (infrastructure, platforms, software, configuration, etc) are known and managed. This includes third parties.	Network and Device Security	The issuing of temporary, time-bound rights for privileged user access and external third-party support access is either in place or you are migrating to an access control solution that supports this functionality.	Network and Device Security
The list of privileged users has not been reviewed recently. (e.g. within the last 12 months.)	Administration, Support and Operations People and Roles	Activity by privileged users is routinely reviewed and validated. (e.g. at least annually)..	Administration, Support and Operations People and Roles	Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.	Administration, Support and Operations People and Roles
Privileged user access is granted on a system-wide basis rather than by role or function.	Administration, Support and Operations People and Roles	Privileged users are only granted specific privileged permissions which are essential to their business role or function	Administration, Support and Operations People and Roles	All privileged user access to your networks and information systems requires strong authentication, such as two-factor, hardware authentication, or additional real-time security monitoring.	Administration, Support and Operations People and Roles
Privilege user access to your essential services is via generic, shared or default name accounts.	Administration, Support and Operations People and Roles			All Privileged user activity is routinely reviewed, validated andrecorded for offline analysis and investigation.	Administration, Support and Operations People and Roles

Where there are "always on" terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted.	Network and Device Security				
There is no logical separation between roles that an individual may have and hence the actions they perform. (e.g. access to corporate email and privilege user actions.)	Administration, Support and Operations People and Roles				
B2d - Identity and Access Management (IdAM					
You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential service.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Greater rights are granted to users than necessary.	Administration, Support and Operations People and Roles	You follow a robust procedure to verify each user and issue the minimum required access rights.	Administration, Support and Operations People and Roles	Your procedure to verify each user and issue the minimum required access rights is robust and regularly audited.	Administration, Support and Operations People and Roles
User rights are granted without validation of their identity and requirement for access.	Administration, Support and Operations People and Roles	You regularly review access rights and those no longer needed are revoked.	Administration, Support and Operations People and Roles	User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually.	Administration, Support and Operations People and Roles

User rights are not reviewed when they move jobs	Administration, Support and Operations People and Roles	User permissions are reviewed when people change roles via your joiners, leavers and movers process.	Administration, Support and Operations People and Roles	All user access is logged and monitored.	Data Protection Service Abuse Detection
User rights remain active when people leave your organisation.	Administration, Support and Operations People and Roles	All user access is logged and monitored	Data Protection	You regularly review access logs and correlate this data with other access records and expected activity.	Data Protection
				Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated.	Denial of Service, Malware, and Breach Protection Boundary Protection Monitoring

CAF Guidance for Objective B3: Data Security

B3a - Understanding data					
You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing or accessing data important to the delivery of essential services.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
You have incomplete knowledge of what data is used by and produced in the delivery of the essential service.	Data Protection	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker.	Data Protection	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker.	Data Protection

You have not identified the important data on which your essential service relies.	Data Protection	You have identified and catalogued who has access to the data important to the delivery of the essential service.	Data Protection	You have identified and catalogued who has access to the data important to the delivery of the essential service.	Data Protection
You have not identified who has access to data important to the delivery of the essential service.	Data Protection	You periodically review location, transmission, quantity and quality of data important to the delivery of the essential service.	Data Protection Service Abuse Detection	You maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service.	Data Protection
You have not clearly articulated the impact of data compromise or inaccessibility.	Data Protection	You have identified all mobile devices and media that hold data important to the delivery of the essential service.	Network and Device Security	You take steps to remove or minimise unnecessary copies or unneeded historic data.	Data Protection
		You understand and document the impact on your essential service of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data.	This document	You have identified all mobile devices and media that may hold data important to the delivery of the essential service.	Network and Device Security
		You occasionally validate these documented impact statements.	Maintenance of Security Policies and Procedures	You maintain a current understanding of the data links used to transmit data that is important to your essential service.	A Secure Public Network Data in Motion
				You understand the context, limitations and dependencies of your important data.	Data Protection

				You understand and document the impact on your essential service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.	Data Protection
				You validate these documented impact statements regularly, at least annually.	Data Protection
B3b - Data In Transit					
You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
You do not know what all your data links are, or which carry data important to the delivery of the essential service.	A Secure Public Network Data in Motion	You have identified and protected (effectively and proportionately) all the data links that carry data important to the delivery of your essential service.	A Secure Public Network Data in Motion	You have identified and protected (effectively and proportionately) all the data links that carry data important to the delivery of your essential service.	A Secure Public Network Data in Motion
Data important to the delivery of the essential service travels without technical protection over non-trusted or openly	A Secure Public Network	You apply appropriate technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.	A Secure Public Network	You apply appropriate physical or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the	A Secure Public Network

accessible carriers.				robustness of the protection applied.	
Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.	Network Resiliency			Suitable alternative transmission paths are available where there is a significant risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).	Network Resiliency
B3c - Stored data					
You have protected stored data important to the delivery of the essential service					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
You have no, or limited, knowledge of where data important to the delivery of the essential service is stored.	Data Protection	All copies of data important to the delivery of your essential service are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.	Data Protection	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.	Data Protection
You have not protected vulnerable stored data important to the delivery of the essential service in a suitable way.	Data Protection	You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.	Data Protection	You have applied suitable physical or technical means to protect this important stored data from unauthorised access,	Data Protection

				modification or deletion.	
Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	Denial of Service, Malware, and Breach Protection	If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.	YHCR as a Certificate Authority	If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.	YHCR as a Certificate Authority
		You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	Denial of Service, Malware, and Breach Protection	You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	Denial of Service, Malware, and Breach Protection
				Necessary historic or archive data is suitably secured in storage.	Data Protection
B3d - Mobile data					
You have protected data important to the delivery of the essential service on mobile devices					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

You don't know which mobile devices may hold data important to the delivery of the essential service.	Network and Device Security	You know which mobile devices hold data important to the delivery of the essential service.	Network and Device Security	Mobile devices that hold data that is important to the delivery of the essential service are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.	Network and Device Security
You allow data important to the delivery of the essential service to be stored on devices not managed by your organisation, or to at least equivalent standard.	Network and Device Security	Data important to the delivery of the essential service is only stored on mobile devices with at least equivalent security standard to your organisation.	Network and Device Security	Your organisation can remotely wipe all mobile devices holding data important to the delivery of essential service.	Network and Device Security
Data on mobile devices is not technically secured, or only some is secured.	Network and Device Security	Data on mobile devices is technically secured.	Network and Device Security	You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.	Network and Device Security
B3e - Media / equipment sanitisation					
You appropriately sanitise data from the service, media or equipment					
Not Achieved- At least one of the following statements is true		Achieved - All the following Statements are true			
Statement	Evidence of Compliance	Statement	Evidence of Compliance		

Some or all devices, equipment or removable media that hold data important to the delivery of the essential service are disposed of without sanitisation of that data.	Network and Device Security	You catalogue and track all devices that contain data important to the delivery of the essential service (whether a specific storage device or one with integral storage).	Network and Device Security		
		All data important to the delivery of the essential service is sanitised from all devices, equipment, or removable media before disposal.	Network and Device Security		

CAF Guidance for Objective B4: System Security

B4a - Secure by Design					
You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Systems essential to the operation of the essential service are not appropriately segregated from other systems.	Network and Device Security	You employ appropriate expertise to design network and information systems.	Network and Device Security	You employ appropriate expertise to design network and information systems.	Network and Device Security

Internet access is available from operational systems.	Firewall Configuration Network and Device Security	You design strong boundary defences where your networks and information systems interface with other organisations or the world at large.	A Secure Public Network	Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone.	Network and Device Security A Secure Public Network
Data flows between the essential service's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic.	Data in Motion	You design simple data flows between your networks and information systems and any external interface to enable effective monitoring.	Data in Motion	The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring.	Data in Motion
Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential service.	Network and Device Security A Secure Public Network	You design to make network and information system recovery simple.	Network and Device Security A Secure Public Network	The networks and information systems supporting your essential service are designed to be easy to recover.	Network and Device Security A Secure Public Network
		All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	Data in Motion	Content-based attacks are mitigated for all inputs to operational systems that effect the essential service (e.g. via transformation and inspection)	Data in Motion Service Abuse Detection
B4b -Secure configuration					
You securely configure the network and information systems that support the delivery of essential services.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

You haven't identified the assets that need to be carefully configured to maintain the security of the essential service.	A Secure Public Network	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential service.	A Secure Public Network	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice)the assets that need to be carefully configured to maintain the security of the essential service.	A Secure Public Network Patch Management
Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential service.	Network and Device Security	Secure platform and device builds are used across the estate.	Network and Device Security	All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.	Source Control and Release Management
Configuration details are not recorded or lack enough information to be able to rebuild the system or device.	Source Control and Release Management	Consistent, secure and minimal system and device configurations are applied across the same types of environment.	Source Control and Release Management	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented	Source Control and Release Management
The recording of security changes or adjustments that effect your essential service is lacking or inconsistent	Maintenance of Security Policies and Procedures	Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service are approved and documented.	Maintenance of Security Policies and Procedures	You regularly review and validate that your network and information systems have the expected, secured settings and configuration.	Maintenance of Security Policies and Procedures
		You verify software before installation is permitted.	Source Control and Release Management	Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.	Source Control and Release Management Network and Device Security

				If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.	N/a
B4c - Secure management					
You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Essential service networks and systems are administered or maintained using non-dedicated devices.	Network and Device Security	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices.	Network and Device Security	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.	Network and Device Security
You do not have good or current technical documentation of your networks and information systems.	Network and Device Security	Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.	Network and Device Security	You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.	Network and Device Security

		You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Denial of Service, Malware, and Breach Protection	You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Denial of Service, Malware, and Breach Protection
B4d - Vulnerability management					
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
You do not understand the exposure of your essential service to publicly-known vulnerabilities.	Vulnerability Assessments	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities	Vulnerability Assessments	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities.	Vulnerability Assessments
You do not mitigate externally-exposed vulnerabilities promptly.	Patch Management	Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and externally-exposed vulnerabilities are mitigated (eg by patching) promptly.	Patch Management	Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and mitigated (eg by patching) promptly	Patch Management

There are no means to check data or software imports for malware.	Denial of Service, Malware, and Breach Protection	Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.	Denial of Service, Malware, and Breach Protection	You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service and verify this understanding with third-party testing.	Vulnerability Assessments
You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential service.	Vulnerability Assessments	You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology		You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service	
You have not suitably mitigated systems or software that is no longer supported	N/a	You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service.	Vulnerability Assessments		
You are not pursuing replacement for unsupported systems or software.	N/a				

CAF Guidance for Objective B5: Resilient Networks and Systems

B5a - Resilience preparation					
You are prepared to restore your essential service following disruption. .					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

You have limited understanding of all the elements that are required to restore the essential service.	Source Control and Release Management	You know all networks, information systems and underlying technologies that are necessary to restore the essential service and understand their interdependence.	The YHCR Membership Registry	You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g. manual fail-over, table-top exercises, or red-teaming.	
You have not completed business continuity and/or disaster recovery plans for your essential service's networks, information systems and their dependencies.	Disaster Recovery	You know the order in which systems need to be recovered to efficiently and effectively restore the essential service	Disaster Recovery	You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware	Vulnerability Assessments
You have not fully assessed the practical implementation of your disaster recovery plans					
B5b - Design for resilience					
You design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Operational networks and systems are not appropriately segregated.	Network and Device Security	Operational systems for your essential service are logically separated from your business systems, e.g. they reside on the same network as the rest of the organisation, but within a DMZ.	Network and Device Security	Your essential service's operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not	Network and Device Security

		Internet access is not available from operational systems.		accessible from operational systems.	
Internet services, such as browsing and email, are accessible from essential service operational systems.	Network and Device Security	Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated	Network and Device Security	You have identified and mitigated all resource limitations, e.g. bandwidth limitations and single network paths.	Network and Device Security
You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential service.	Business Continuity			You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential service depends upon are replicated inanother location, important network connectivity has alternative physical paths and service providers.)	Cloud Hosting
				You review and update assessments of dependencies, resource and geographical limitations and mitigation's when necessary.	Cloud Hosting
B5c - Backups					
You have protected stored data important to the delivery of the essential service					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

Backup coverage is incomplete in coverage and would be inadequate to restore your essential service.	Backup and Recovery	You have appropriately secured backups (including data, configuration information, software, equipment, processes and key roles or knowledge). These backups will be accessible to recover from an extreme event.	Backup and Recovery	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.	Backup and Recovery
Backups are not frequent enough for your essential service to be restored within a suitable time-frame.	Backup and Recovery	You routinely test backups to ensure that the backup process functions correctly and the backups are usable	Backup and Recovery	Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service	Administration, Support and Operations People and Roles
				Backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Backup and Recovery

CAF Guidance for Objective B6: Staff Awareness and Training

B6a - Cyber security culture					
You develop and pursue a positive cyber security culture.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance

People in your organisation don't understand what they contribute to the cyber security of the essential service.	Administration, Support and Operations People and Roles	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation.	Administration, Support and Operations People and Roles	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.	Administration, Support and Operations People and Roles
People in your organisation don't know how to raise a concern about cyber security.	Administration, Support and Operations People and Roles	All people in your organisation understand the contribution they make to the essential service's cyber security.	Administration, Support and Operations People and Roles	People in your organisation raising potential cyber security incidents and issues are treated positively.	Administration, Support and Operations People and Roles
People believe that reporting issues may get them into trouble.	Administration, Support and Operations People and Roles	All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	Administration, Support and Operations People and Roles	Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.	Administration, Support and Operations People and Roles
Your organisation's approach to cyber security is perceived by staff as getting in the way of them delivering the essential service	Administration, Support and Operations People and Roles			Your management is seen to be committed to and actively involved in cyber security.	Administration, Support and Operations People and Roles
				Your organisation communicates openly about cyber security, with any concern being taken seriously.	

				People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise	Administration, Support and Operations People and Roles
B6b - Cyber security training					
The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
There are teams who operate and support your essential service that lack any cyber security training.	Administration, Support and Operations People and Roles	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles.	Administration, Support and Operations People and Roles	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths.	Administration, Support and Operations People and Roles
Cyber security training is restricted to specific roles in your organisation.	Administration, Support and Operations People and Roles	You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively	Administration, Support and Operations People and Roles	Each individuals' cyber security training is tracked and refreshed at suitable intervals.	Administration, Support and Operations People and Roles
Cyber security training records for your organisation are lacking or incomplete	Administration, Support and Operations People and Roles	Cyber security information is easily available.	Administration, Support and Operations People and Roles	You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective.	Administration, Support and Operations People and Roles

				You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.	Administration, Support and Operations People and Roles

Appendix 2 – NIS Objective C: Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

CAF Guidance for Objective C1: Security Monitoring

C1a - Monitoring Coverage					
The data sources that you include in your monitoring allow for timely identification of security events which might affect the delivery of your essential service					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Data relating to the security and operation of your essential services is not collected.	Service Monitoring	Data relating to the security and operation of some areas of your essential services is collected.	Service Monitoring	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect your essential service. (e.g. presence of malware, malicious emails, user policy violations).	Service Monitoring
You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential services, such as know malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).	Service Monitoring	You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures.	Service Monitoring	Your monitoring data provides enough detail to reliably detect security incidents that could affect your essential service.	Service Monitoring
You are not able to audit the activities of users in relation to your essential service.	Auditing of Access	Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.	Auditing of Access	You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures.	Auditing of Access Boundary Protection Monitoring Network and Device Security

You do not capture any traffic crossing your network boundary including as a minimum IP connections	Auditing of Access Boundary Protection Monitoring Network and Device Security	You monitor traffic crossing your network boundary (including IP address connections as a minimum)	Auditing of Access Boundary Protection Monitoring Network and Device Security	Extensive monitoring of user activity in relation to essential services enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Auditing of Access Boundary Protection Monitoring Network and Device Security
				You have extensive monitoring coverage that includes host-based monitoring and network gateways.	Auditing of Access Boundary Protection Monitoring Network and Device Security
				All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability	
C1b - Securing Logs					
Logging data should be held securely and read access to it should be granted only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.	Auditing of Access	Only authorised staff can view logging data for investigations.	Auditing of Access	The integrity of logging data is protected, or any modification is detected and attributed.	Auditing of Access

There is no controlled list of who can view and query logging information.	Auditing of Access	Privileged users can view logging information.	Auditing of Access	The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it.	Auditing of Access
There is no monitoring of the access to logging data.	Auditing of Access	There is some monitoring of access to logging data. (e.g. copying, deleting or modification, or even viewing.)	Auditing of Access	Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.	Auditing of Access
There is no policy for accessing logging data.	Auditing of Access			Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.	Auditing of Access
Logging is not synchronised, using an accurate common time source.	Auditing of Access			Access to logging data is limited to those with business need and no others.	Auditing of Access
				All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.	Auditing of Access
				Legitimate reasons for accessing logging data are given in use policies.	Administration, Support and Operations People and Roles
C1c - Monitoring Coverage					

Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.	Denial of Service, Malware, and Breach Protection	Alerts from third party security software are investigated, and action taken.	Denial of Service, Malware, and Breach Protection	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	Service Monitoring
Logs are distributed across devices with no easy way to access them other than manual login or physical action.	Auditing of Access	Some logging datasets can be easily queried with search tools to aid investigations.	Auditing of Access	A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts.	Auditing of Access Service Abuse Detection
The resolution of alerts to a network asset or system is not performed.	Service Availability Monitoring	The resolution of alerts to a network asset or system is performed regularly.	Service Availability Monitoring	Alerts can be easily resolved to network assets using knowledge of networks and systems	Service Availability Monitoring
Security alerts relating to essential services are not prioritised.	Service Availability Monitoring	Security alerts relating to some essential services are prioritised.	Service Availability Monitoring	Security alerts relating to all essential services are prioritised and this information is used to support incident management.	Service Availability Monitoring
Logs are reviewed infrequently	Service Monitoring	Logs are reviewed at regular intervals.	Service Monitoring	Logs are reviewed almost continuously, in real time.	Service Monitoring

				Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	Service Availability Monitoring
C1d - Identifying security incident					
You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
Your organisation has no sources of threat intelligence.	Vulnerability Assessments	Your organisation uses some threat intelligence services, but you don't choose providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms).	Vulnerability Assessments	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare).	Vulnerability Assessments
You do not apply updates in a timely way, after receiving them. (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)).	Patch Management	You receive updates for all your signature based protective technologies (e.g. AV, IDS).	Patch Management	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	Patch Management

You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.	Patch Management	You apply some updates, signatures and IoCs in a timely way.	Patch Management	You receive signature updates for all your protective technologies (e.g. AV, IDS).	Patch Management
You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	Vulnerability Assessments	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	Vulnerability Assessments	You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).	Vulnerability Assessments
C1e - Monitoring tools and skillst					
Monitoring staff skills, tools and roles, including any that are out-sourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protec					
Not Achieved- At least one of the following statements is true		Partially Achieved- All of the following statements are true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance	Statement	Evidence of Compliance
There are no staff who perform a monitoring function.	Service Monitoring	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.	Service Monitoring	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.	Service Monitoring
Monitoring staff do not have the correct specialist skills.	Service Monitoring	Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	Service Monitoring	Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.	Service Monitoring

Monitoring staff are not capable of reporting against governance requirements. Monitoring staff lack the skills to successfully perform any part of the defined workflow.	Service Monitoring	Monitoring staff are capable of following most of the required workflows.	Service Monitoring	Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.	Service Monitoring
Monitoring tools are only able to make use of a fraction of logging data being collected.	Service Monitoring	Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.	Service Monitoring	Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	Service Monitoring
Monitoring tools cannot be configured to make use of new logging streams, as they come online.	Service Monitoring	Your monitoring tools work with most logging data, with some configuration.	Service Monitoring	Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.	Service Monitoring
Monitoring staff have a lack of awareness of the essential services the organisation provides, what assets relate to those services and hence the importance of the logging data and security events.	Service Monitoring	Monitoring staff are aware of some essential services and can manage alerts relating to them	Service Monitoring	Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	Service Monitoring
				Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.	Service Monitoring

CAF Guidance for Objective C2: Proactive Security Event Discovery

C2a - System abnormalities for attack detection			
You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.			
Not Achieved- At least one of the following statements is true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	This document and other designs	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity. (e.g. You fully understand which systems should and should not communicate and when.)	This document and other designs
You have no established understanding of what abnormalities to look for that might signify malicious activities	This document and other designs	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	This document and other designs Service Monitoring
		The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services.	Service Monitoring
		The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.	Service Monitoring
C2b - Proactive attack discovery			

You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.			
Not Achieved- At least one of the following statements is true		Achieved - All the following Statements are true	
Statement	Evidence of Compliance	Statement	Evidence of Compliance
You do not routinely search for system abnormalities indicative of malicious activity.	Service Monitoring	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting your essential service, generating alerts based on the results of such searches.	Service Monitoring
		You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.	Service Monitoring

Appendix 3 – Maturity Matrix

Section	Narrative	Consultative	Draft	Normative
1 Introduction 1.1 Purpose of this Document	X			
1.2 About the NIS Directive	X			
1.3 Relationship Between this Document and the CAF	X			
1.4 Domain of Responsibility and Domain of Interest		X		
1.5 Relationship of this Document with Other Standards	X			
1.6 Intended Users of the This Document	X			
2 Boundary Protection 2.1 A Secure Public Network 2.1.1 The YHCR Membership Registry		X		
2.1.2 YHCR as a Certificate Authority			X	
2.1.3 The YHCR Domain			X	
2.1.4 YHCR Exclusive Port Usage			X	
2.1.5 Validating Identity of Participants in YHCR			X	
2.2 Assuring Compliance		X		
2.3 Auditing of Access	X			
2.4 Denial of Service, Malware, and Breach Protection 2.4.1 Containment			X	
2.4.2 Reporting and Root Cause Analysis			X	
2.5 Firewall Configuration			X	
2.6 Vulnerability Assessments			X	
2.7 Patch Management			X	
3 Data Protection 3.1 Data at Motion		X		
3.2 Data at Rest		X		
4 Business Continuity 4.1 Cloud Hosting			X	
4.2 Network Resiliency			X	
4.3 Scalability and High Availability			X	
4.4 Backup and Recovery			X	
4.5 Disaster Recovery			X	
5 YHCR Administration and Operations			X	

5.1 Source Control and Release Management				
5.2 Administration, Support and Operations People and Roles			X	
5.3 Network and Device Security			X	
5.4 Maintenance of Security Policies and Procedures			X	
5.5 Service Monitoring 5.5.1 Service Abuse Detection		X		
5.5.2 Boundary Protection Monitoring			X	
5.5.3 Service Availability Monitoring		X		