COVID-19 Test Trace, Isolate, Support (TTIS)
Case Management System (CMS)
System Security Policy (SSP)

Document control

Title	CMS - System Security Policy (SSP)
Author	NHS National Services Scotland
Creation date	10th June 2020

Version history

Version	Date	Comments
0.1	10th June 2020	Initial Draft
0.2	12th June 2020	Updated to include reference documents
0.3	26th June 2020	Updated to include recommendations from Security and Architecture Review Board (SARB)
1. 0	22nd July 2020	Added users not within the NHS login mechanisms. Also version moved to version 1.0 as approved by SARB.

Table of contents

1 CMS overview

1.1 Introduction

1.1.1 As part of Covid-19 'Test, Trace, Isolate, Support' (TTIS) a decision has been taken by Public Health Scotland (PHS) to deliver a digital solution for a National Tracing Service. This solution includes the development of the Tracking and Tracing Tool made up of a cloud based case management system (CMS) with integrated telephony.

The case management and telephony systems are existing platforms used within NHS NSS, these tools are cloud based SaaS (Software as a service) namely ServiceNow "Customer Service Management Module" and a new system brought in to aid in the track and trace solution called, 8x8 "Virtual Call Centre (VCC) and Virtual Office (VO)". Both systems are integrated to make up the overall CMS solution.

CMS will facilitate, as part of Covid-19 and beyond, a well-established public health intervention methodology called "contact tracing". Contact tracing will be used to identify the close contacts of those cases who may have had the disease transmitted to them. These close contacts will then be asked to self-isolate so that, if they do develop the disease, there is less risk of transmission to others. The contact tracers will use the CMS to enter contact tracing information for those patients with positive results, they will also view the submitted contacts and their relative priority level to enable targeted phone-based interviews to be arranged.

The SaaS CMS solution is based on the DHI/StormID designed Covid-19 Simple Tracing Tools ('STT')/Negative Notifications Service ('NNS') which both provides a Covid-19 test result service to patients and which has a clinician-facing dashboard / management service for track and trace activities. The solution is driven by the daily lab results data feeds from the Electronic Communication of Surveillance in Scotland ('ECOSS') system which is the established core NHS Scotland service for disseminating laboratory test results.

1.2 Business goals/benefits of the system

1.2.1 The objective of CMS is to remove a significant burden of manual, paper-based contact tracing from NHS Scotland by providing security and a degree of automation in the form of electronic capture of contact information volunteered by patients who have tested positive. CMS will provide a

strategic contact tracing service to aid in the suppression of Covid-19 and beyond.

1.2.2 The initial release of the CMS does not include a patient-facing component whether website or dedicated app, and hence no mechanism for tracking devices or to allow patients to enter contact, setting or symptom information.

1.3 System status and timescales

1.3.1 CMS has been developed by NHS NSS and is live from 22nd June 2020. The core components made up of ServiceNow and 8x8 are described in their own separate SSP's

1.4 System security policy statement

1.4.1 "The system shall employ appropriate security controls and manage risk throughout the life of system to ensure the confidentiality, integrity, availability of data and services is protected." Describe any solution specific objectives, special considerations related to the type of information processed, environment in which system will operate, overview of how it is planned these objectives will be met)

1.4.2 The purpose of the Policy is to protect the information assets from all threats, whether internal or external, deliberate or accidental. The objective of information security is to ensure the security of all assets and continuity of service by identifying and mitigating risk. The system shall employ appropriate security controls and manage risk throughout the life of system to ensure the confidentiality, integrity, availability of data and services is protected.

1.4.3 As CMS gathers information about citizens, the solution includes a definition of ownership that includes the citizen as well as the parties responsible for technical security and management of information. All parties will be informed of their duties in respect of maintaining the privacy and integrity of the information within NHSScotland.

1.4.4 CMS shall be managed by NHS National Services Scotland and will include regular maintenance activities, technical support services, test and release services, service performance targets, incident management, problem triage and resolution, service reporting and escalation.

1.4.5 The core cloud platforms are subjected to annual security penetration test by an independent external accredited security organisation. Identified security threats shall be assessed by the System Owner and System Operator and if required a remediation plan shall be prepared and executed, and re-testing carried out by agreement. This information is provided in ServiceNow and 8X8 specific SSP's

1.5 Privacy impact assessment

1.5.1 A DPIA has been written for this service and can be requested from the NSS the Digital and Security Information Governance team.

1.6 Responsible parties

1.6.1 The following individuals are responsible:

- System owner: NHS National Services Scotland
- System manager/operator: NHS National Services Scotland

  Senior information risk owner (SIRO): Deryck Mitchelson (NSS Digital and Security Director, NHS National Services Scotland).
- Information security officer/Accreditor: Head of Information Security, NHS National Services Scotland.

  Information governance officer: Senior Consultant Information Governance (Information Security and Governance, NSS Digital and Security)

2 System description

2.1 Context

2.1.1 As part of Covid-19 'Test, Trace, Isolate, Support' (TTIS) a decision has been taken by Public Health Scotland (PHS) to deliver a digital solution for a National Tracing Service. This solution includes the development of the Simple Tracing Tool made up of a cloud based case management system (CMS) with integrated telephony.

2.1.2 The principal components and the virology data feeds are all pre-existing technologies and services used within NHS Scotland.

2.2 Operation

2.2.1 The service is hosted as SaaS within the public cloud and operates as follows:

(a) The existing daily export file containing virology lab results is sent by the 'ECOSS' system to an existing digital health platform via the NHS NSS National Integration Hub (NIH) and the National Digital Platform (NDP)

(b) The NIH filters the virology input file to allow only Covid-19 specimen result information and the minimum associated patient data to be forwarded the Lenus platform
(c) Patients are on boarded to the platform through automatic record creation in Lenus when virology results arrive into the platform for any patient who does not already have a record.
(d) The service includes CMS/8X8 contact tracing staff to use. This web application is an extension of ServiceNow Customer Service Management Module, integrated with 8x8 telephony, allowing contact tracing staff to:
    i. View lists of patients with positive results (index cases), filtered by Health Board
    ii. Add telephone (and email address if available) contact information for index cases manually via the dashboard if not already provided automatically from demographics data fed from the Health Board patient management systems
    iii. Add contacts (the people the index case have been in close contact with) manually to each index case, using a quick contact tracing form during a phone interview
    iv. Access an additional list view of the index case records that includes status i.e. when, and whether they have been engaged, and how many contacts have been traced
    v. Select an index case to show their record, including the list of their contacts and settings logged for the case
    vi. Access an additional list view of the contact records across all index cases that allows filtering for the priority tags identified during phone interviews, to help prioritise tracing activity.
    vii. Record the result of a phone-based symptom check on a daily basis for each contact.
    viii. Click on a contact to show and edit their record.
    ix. Convert a contact to a new index case when confirmed via test.

2.3 Hardware

2.3.1 (Architecture, summary of hardware, versions, configuration)

ServiceNow is a cloud based SaaS service. The ServiceNow SSP states the following:
"ServiceNow provides enterprise cloud-based solutions services, via a platform consisting of multi-tiered architecture comprised of over 5,000 web and database servers running the Linux operating system. Data primarily is stored in MySQL databases on the database servers.

These systems are supported by hardware infrastructure comprised of enterprise vendors including Dell, VMware, and Juniper. Network connections are managed using a high availability Juniper SRX Module that provides perimeter filtering. The traffic then passes through a load balancer which load balances the traffic to the application servers."

8x8 Virtual Contact Centre/Virtual Office is a cloud based SaaS service. The 8x8 SSP states the following:

- Server hardware is cloud-based.

2.4 Software

2.4.1 (Server OS/platforms, versions of server and client software, thick or thin client, underlying/enabling technologies where appropriate (such as Java, .NET, php, etc.)

Both ServiceNow and 8X8 which combined offer CMS run as Software as a Service (SaaS) using vendor proprietary software. The software is under control by the vendors and is used globally as a service.

2.5 Interfaces

2.5.1 (List interfaces with other networks/systems/applications/organisations, describe how each communication and interface works e.g. SMTP email, web based access using SSL over HTTP, Internet facing web services based on WSDL, etc. Where possible capture specific technologies and versions of protocols in use)

- Contact tracer/Call Handler endpoint device to access CMS using a supported browser over HTTPS. Azure Active Directory (AAD) and Google Authenticator are used for multi factor authentication (MFA) to authorise the user to the system.
- A local NSS instance of ServiceNow Mid server provides a mechanism for exchanging data with other internal systems. Data is then synchronised with the cloud based ServiceNow platform using a proprietary data synchronisation product (Perspectium).

2.6 Accreditation scope

2.6.1 (Summarise what is in scope and any scope exclusions)

The accreditation scope covers the components that make up CMS. The scope is:

- ServiceNow Case Management Service Module.
- 8X8 Virtual Contact Centre/Virtual Office

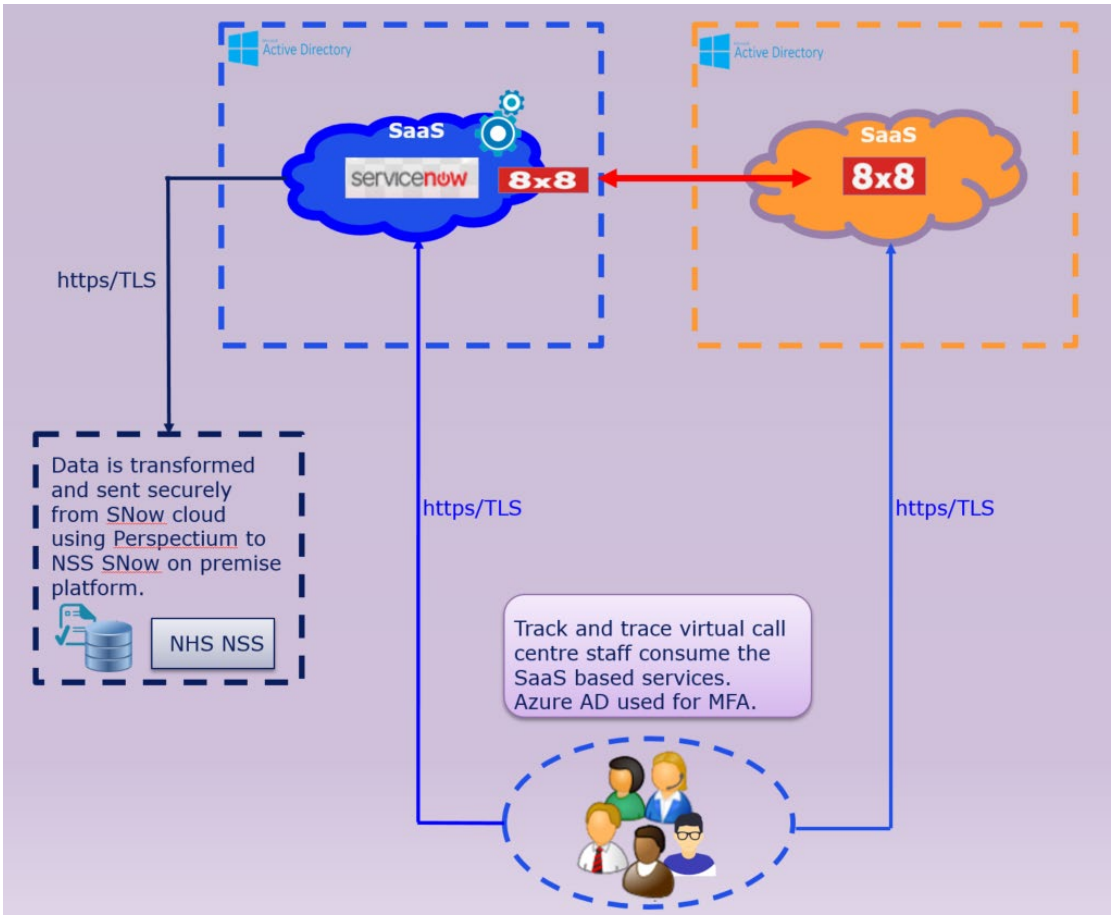
Exclusions include the downstream components where data is consumed.

2.6.2 Figure 1 shows an overview diagram of the system.

2.6.3 All hosting of CMS is within Public Cloud, consuming SaaS. There is a secure synchronisation of data captured as part of contact tracing using TLS between ServiceNow and the NSS network. There is API level connectivity via a ServiceNow mid server, from there the data is sent to the NSS

Corporate Data Warehouse. The diagram in figure 1 shows holistic view of how the CMS service will be consumed. The specific ServiceNow and 8X8 SSP's should be referred to for a lower level look at each individual SaaS.

Figure 1: diagram of proposed architecture



3 Assets and services

3.1 Introduction

3.1.1 At the heart of a risk assessment are assets that are valuable to the business and need to be protected – these assets include:

- **Information assets** e.g. NHS data sets that must be protected from risks such as unauthorised access and loss
- **Physical assets** e.g. mobile devices or data centre equipment that must be protected from threats such as theft and fire damage
- **Services** e.g. clinical applications or infrastructure services like AD and DNS that must be protected from threats such as loss of service

3.1.2 This section captures the assets that are to be protected in the case of this information system.

3.2 Information assets

3.2.1 Table 1 lists the information assets collect by contact tracers/call handlers through interaction with citizens. Contact tracer's/call handlers will be employed by and processing/controlling data for NHS NSS.

ID	Name	Description	NHS sensitivity

A1	Patient personal and system login information	Patient title Patient first name Patient surname Patient date of birth Patient preferred name Patient sex Patient email address Patient residential street address Patient phone number CHI number **Note: In some cases, the point of contact may be a parent/guardian/carer/responsible adult for the patient, so the mobile telephone number or email address may be for that person as a representative of the patient.** Index case: Case status (selection from list) Contacts logged (#) Risk Profile: Key worker description (selection from list) Works with vulnerable people (flag) Been to H&SC setting (flag) Case notes, other risk, occupation or vocation info (free text) *Exposure details:* Contact Setting (selection from list) Date of Contact Age 70+ flag Key worker? Key worker detail Whether pregnant (flag) Medical Condition (flag + comorbidities) Notified (flag) C19 symptoms: (flag) *Public Health England Categorisation:* (selection from A, B, C, D1, D2, E, F, G1, G2)	Red

ID	Name	Description	NHS sensitivity
		Index case setting log: Setting Type (selection from list) Setting Address - Name/Address/ - postcode Phone number Date of contact Location informed (selection y/n) Contacts logged (selection Y/N/In progress/Not required)	
A4	Test results	Health Board Code Laboratory name Laboratory ID Lab results (test result, specimen ID, specimen date, report date) Patient COVID-19 negative test result is available to view within the NNS system.	Green
A5	NSS employee System login details	username and password to authenticate to CMS for data read/write function	Red
A6	System Design	Design documentation listing components that make up the system	Green
A7	Source Code	Application Source Code	Green
A8	Cloud Platform	Public cloud configuration and security settings	Amber

Table 1: information assets

3.2.2 The “NHS sensitivity” is the label applied to the information according to the NHS Scotland traffic light system as set out in Table 2.

Label	Description
Green	This is information which is unlikely to cause distress to individuals, breach confidence or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person’s name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person’s physical or mental state.

Label	Description
Amber	In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular: • any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost. • any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result). • any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).
Red	Most boards also hold some information which is highly sensitive. Particularly: • Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). • Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health. • Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). • Information relating to vulnerable persons' health (e.g. child protection cases) • Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). • Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Table 2: NHS Scotland traffic light sensitivity descriptions

3.3 Physical assets

3.3.1 Table 3 lists the *major* physical assets comprising the system. (If it is a managed service and the supplier owns all the major physical assets this section can be omitted)

CMS is made up of cloud based SaaS. All physical assets exist within a managed public cloud environment.

3.4 Services

3.4.1 Table 3 lists the services provided by the solution.

ID	Name	Description	Max. tolerable downtime
S1	Customer Management System (CMS)	CMS utilises the ServiceNow and 8X8 SaaS public cloud solutions. These solutions are highly available global systems therefore very little downtime envisaged	24 hours

Table 3: Services

4 People

4.1 User groups

4.1.1 Table 3 lists the user groups with access to the system.

ID	Name	Description	Type of access	Number[1]
U1	Participating Health board Clinicians and tracing/call handling staff	Input and process data	User read/write access	200 – 500 (Pilot phase), increasing to 1000+ projected for later releases
U2	Participating Health Board system support teams	Provide system support through diagnostics and repair	System Administrator	1 - 9
Non User Groups				
U3	Supplier Support	Service maintenance and support	Application administrator level access to source code	1 - 9
U4	Admin Support	Infrastructure support for cloud environment	Manage SaaS	< 5

Table 4: User groups

4.2 Other sources of threat

4.2.1 In addition to people-based sources of threat the following people-based sources of threat shall be considered in the risk assessment:

- Environmental threats such as fire, flood
- Technical threats such as technical failure of equipment
- Automated threats such as worms that propagate mostly without human interaction

[1] Approximate number band: 1-9, 10-99, 100-999, etc.

5 Security controls

5.1 Supplier arrangements

5.1.1 What suppliers are involved in provision of any aspect of the solution? (identify all supplier groups including internal/health board teams, and external commercial third parties)

ServiceNow provided via hosted SaaS solution

8x8 provided via hosted SaaS solution

5.1.2 What contracts are in place? Summarise the information security/information governance/data protection contract terms, or other arrangements.

ServiceNow Master Order Agreement:

ServiceNow authorises NSS to access and use the purchased Subscription Service during the Subscription Term (to December 2018). NSS shall not use or otherwise access the Subscription Service in a manner that exceeds our authorised use. NSS are granted rights to the development tool. Restrictions include re-sell, lease, transfer of licence, reverse engineer or decompile.

ServiceNow may remotely review NSSs use of the Subscription Service, and upon ServiceNow's written request, NSS would provide any reasonable assistance, to verify our compliance.

NSS shall retain all of its rights, title, and its intellectual property rights in our Data and Customer Technology.

Neither party may assign its rights or obligations under the MOA, without the prior written consent of the other party. The service will comply with US and foreign export law.

The Data Security Guide describes the following :-

- ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001 and SSAE 16 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "***Standards***") for the information security management system supporting the Subscription Service.

- Physical data centre security – multi zone, onsite guards, biometric controls, CCTV, secure cages

- Industry standard destruction of sensitive materials before disposition of media

- Firewall system, Vulnerability management, virus scanning
- Change control
- General security – Data centre inspections, Personnel security (background checks, drug screening), security awareness training and risk management
- Penetration testing by third party or by the customer

8x8 Agreement:

This is contained within the Proposal for Public Health Scotland document.

5.1.3 Do information security requirements that apply to the named contractor also apply to any subcontractors? Name any sub-contractors.

As Above

5.1.4 Who is responsible for reviewing supplier performance and ensuring conformance with security requirements?

Service Owner

5.1.5 What independent assurance/audits/certifications are applicable to any part of the solution? Describe the scope of any applicable certifications.

ServiceNow certifications

- ISO27001

8X8 certifications

- Cyber Essentials Plus
- ISO 27001:2013
- HM Gov't Authority to Operate
- HIPAA & FISMA
- Cloud Security Alliance
- Privacy Shield

5.2 Access control

5.2.1 How are new users provisioned? How is it ensured that users get the correct permissions?

ServiceNow

NHS users are provided with a login account to ServiceNow using NHS Active Directory groups. Users working on behalf of Health Boards (as an example, Local Authorities) are provisioned with local user accounts, these users invariably do not exist within participating boards active directory therefore local accounts are required. RBAC is employed to make sure authenticated users are assigned the correct role with the appropriate permissions.

8X8

NHS Users are provided with a login account to 8X8 using NHS Active Directory groups. Users working on behalf of Health Boards (as an example, Local Authorities) are provisioned with local user accounts, these users invariably do not exist within participating boards active directory therefore local accounts are required. RBAC is employed to make sure authenticated users are assigned the correct role with the appropriate permissions.

Although both systems are integrated in terms of functionality, authentication to both systems independently is required, this is currently a limitation to providing SSO for CMS that may be addressed in the future.

5.2.2 How do users log onto the solution? Are there different options for different interfaces?

CMS

NHS user's login to a web based portal for ServiceNow/8X8 using either NHS combined with Azure Active Directory Multi Factor Authentication. There are exceptions to this where local authorities working on behalf of a Health Board are working as part of the contact tracing virtual call centre. These users will not be members of the participating Health Board's active directory therefore they will use local accounts for ServiceNow and Google Authenticator for Multi Factor Authentication. For 8x8, these users will login using username and password. This has been accepted as a risk by the programme, see section 6.4.3 table 6 within this document.

5.2.3 How is it ensured that users can only access the information and functions for which they are authorised?

When a user successfully authenticates to CMS, they are allocated access based on their role within the application (RBAC)There is only one route for users to access the system. The access rights to CMS are provisioned and managed at an administrator level.

5.2.4 How are the user accounts managed? For example, who removes accounts of staff that leave the organisation, resets forgotten passwords, updates a user's permissions, changes to permissions, etc?

NHS User accounts/permissions groups/passwords are managed by Active Directory; authentication is managed by AAD (AD Sync with NHS on premise Active Directory) addition of the capability to add or remove clinical users for their own Health Board domain only. For local account users a local administrator for the participating entity will manage accounts based on local policy.

5.2.5 How can users recover their account if they forget their credentials?

Account management and recovery is controlled via Active Directory through normal BAU processes. For local account users a local administrator for the participating entity will manage accounts based on local policy.

5.2.6 How are user credentials, such as passwords, stored within the system?

NHS user's authentication is provided via NHS Active Directory; passwords are managed based on the participating health board local policy. Other user's passwords are stored within ServiceNow and 8x8 and their respective policies state the following, "User passwords are complex, encrypted and stored using a one-way salted hash."

5.2.7 Are any individuals/groups, who are **not** authorised users of the system, able to access any part of the system e.g. the hardware or shared infrastructure components? (For example cleaners or patients that may be able to access physical terminals in shared areas; or users of other applications that may be able to access a shared database or hosting environment)

No.

5.3 Personnel controls

5.3.1 What personnel pre-employment screening checks are applied for personnel involved in provision of the service?

ServiceNow personnel controls

Screening of all personnel is mandatory in all locations regardless of role. ServiceNow performs standard background screening and checks on all prospective employees, permanent or temporary. A specialist 3rd party screening organisation conducts these on behalf of ServiceNow.

The process varies from region to region, subject to local laws and restrictions, and includes 5-year employment verification checks, covering

- Basic criminal disclosure
- Credit inquiry,
- regular drug screening,
- regular security awareness training.

8x8 personnel controls

All 8x8 staff involved with our UK Government contracts have Government security clearance Up to Baseline Personnel Security Standard (BPSS). SC clearance has been obtained for key personnel engaged in our OFFICIAL networks. NPPV clearance is available for staff working unaccompanied at Police or Fire Service sites if required.

5.3.2 How are users made aware of their security responsibilities with respect to the system? (e.g. to keep their password secret, or to report a security breach?)

Tracking and tracing/Call handlers

NHS NSS users of the CMS are already subject to training on information safe handling. The use of the CMS application falls within the scope of their existing briefings and training and includes, clear communication of acceptable use policy, security of information systems and code of compliance.

5.3.3 What training is provided to system administrators or managers on how to properly run the system?

Managers of CMS follow clear procedural guidance set out as part of security awareness training. This training is subject to periodic review and captured as part of the NHS wider Cyber awareness training.

5.3.4 What information security and governance training is provided to users of the system?

NHS employees are subject to security awareness training and information safe handling within the NHS. The CMS application falls within the scope of their existing briefings and training on the secure use of information systems.

5.4 Network security controls

5.4.1 Are the system's network interfaces hardened? For example, have all unnecessary services been disabled and ports closed?

ServiceNow and 8x8 are cloud based SaaS platforms and are subject to a number of security controls, namely, DDoS prevention, annual pen testing, vulnerability scanning, firewalls, Anti-virus. The NSS ServiceNow instanced is hardened further by the implementation of built in High Security Settings The relevant SNow and 8x8 SSP's should be referenced for more details.

5.4.2 How does the solution protect access to network traffic on shared networks?

The solution is deployed within public cloud where it does not have any access to network traffic on shared networks. Solution components that integrate with other systems are protected with both application level and network level security to prevent unauthorised network access to the destination infrastructure.

5.4.3 How is the hosting environment separated/protected from connected networks (e.g. firewall(s), models, config, etc.)?

See answer above

5.4.4 Have all network components been deployed in a hardened configuration, for example all default passwords changed, and unneeded services blocked?

5.4.5 This is a cloud SaaS based service and utilises cloud based security controls.

5.4.6 Is the solution remotely accessible? If so, how is the remote access provided and controlled?

The solution is a public cloud based SaaS MFA is deployed as a security control. Administrator access is via cloud management portal. MFA access is strictly controlled with only those permissions required to carry out infrastructure maintenance being granted with role-based access control and under change control agree by the relevant Change Approval Board.

5.5 Data protection

5.5.1 Who are the data controllers and data processors for this solution?

PHS and NSS are data controllers for the test result data within ECOSS.

Participating Health Boards are also Data Controllers of data relating to patients accessing NHS care within their territorial NHS board geographical areas.

Territorial Health Boards whose testing teams use the service, do so to:

- Input patient contact information (telephone number and email address)
- View patient test results status (positive, negative, and whether a patient has accessed their result)

- Input contact tracing, symptoms and settings information as part of managing the Covid-19 outbreak.

The territorial Boards using this service and providing additional data feeds through Trak are also Data Controllers for the data pertaining to their own patients.

NSS, as a Data Controller will operate the service on behalf of NHSScotland Boards

National Integration Hub (NIH). The NIH receives incoming data feeds from the PHS ECOSS service. This contains patient, HB, and laboratory test result information that is processed and filtered by the NIH for onward transmission of test results to the Lenus platform.

NHS National Education Scotland Digital Service is a Data Processor for the data that transits from the NIH to the Lenus platform via the National Digital Platform (NDP).

This test result data that ingested into the Lenus platform via the National Integration Hub (NIH) and the National Data Platform (NDP).

ServiceNow and 8X8 are data sub-processor for the infrastructure supporting the CMS solution.

5.5.2 Are all information assets held in the system allocated to a responsible owner?

The CMS Data Protection Impact Assessment lists the Data Controllers and Data Processors for the information assets.

The data in the Lenus platform that relates to citizens is owned by the citizens themselves (Assets A1 and A4 where these relate to individuals).

CMS login information (Asset A5) is owned by NSS as the employing Health Board.

System design documentation (Asset A6) is owned by NSS.

Source code (Asset A7) is owned by Cloud SaaS providers

5.5.3 Are any technical controls employed within the solution to protect information assets? For example encryption at rest, de-identification or data obfuscation.

All information assets within the SaaS solutions are encrypted at rest and in transit. More information exists within the ServiceNow and 8x8 SSP's

5.5.4 What controls are in place to ensure secure disposal of hardware and information assets? For example, to prevent unauthorised recovery of data on recycled hard disks, or secure shredding of printed output.

ServiceNow

NIST 800-88 data destruction methods are used when there is a need to retire hard drives or if a server wipe is needed for re-provisioning. ServiceNow also contracts third party vendors for destruction of hard drives to provide certificates of destruction. Detail on the process here

8X8

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

5.5.5 How is data imported/exported from the solution? What controls are employed to protect any data on removable media?

There is no data import/export to/from the SaaS solution.

5.5.6 What information transfers does the solution permit/enable? How are these controlled?

A local NSS instance of ServiceNow provides a mechanism for exchanging data with other internal systems. Data is then synchronised with the cloud based ServiceNow platform using a proprietary data synchronisation product (Perspectium).

5.6 Physical and environmental security

5.6.1 What physical or environmental controls apply at any locations where the solution is hosted?

ServiceNow

All ServiceNow data centres are required to either an ISO 27001 certification or an SSAE 16 attestation. 24x7 onsite security guards, onsite CCTV, multiple security zones with biometric access controls.

8x8

All data centres deployed in the solution employ Physical Access Controls complying with CCM v3.0 and SSAE-16 / ISAE 3402

5.6.2 What physical security controls apply at any locations from where the solution is used/accessed?

Public Cloud providers physical security policy applies to all forms of physical security including:

- multi-zone security
- man-traps
- appropriate perimeter deterrents (fencing, berms, guarded gates)
- on-site guards
- biometric controls
- CCTV
- secure cages
- fire detection and fire suppression systems both localized and throughout the data centre floor.

Participating health boards local physical security policy should apply.

Participating Health Boards computers used by staff are protected by standard security measures governed by local security policy.

5.7 Operational security

5.7.1 Who is responsible for Information Backup controls? Describe the data backup and recovery process.

Platform backup is the responsibility of both ServiceNow and 8X8 as part of the SaaS. With regards recovery, a support ticket would be raised with the service provider to recover the service from backup.

ServiceNow Backups

While Advanced High Availability is the primary means to recover data and restore service in the case of a service disruption, in certain cases it is desirable to use ServiceNow's more traditional data backup and recovery mechanism. This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism.

ServiceNow stores production instances in two geographically separate regional data centres, with sub-production instances hosted in a single data centre. Backups of the two production databases and the single sub-production database are taken every day for all instances throughout the private cloud infrastructure.

The backup cycle consists of four weekly full backups and the past 6 days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database, then it will also be encrypted in the backups.

Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.

For the provision of Disaster Recovery, instant data replication is between Data Centres. This data transaction is secured by encryption.

8X8 Backups

By selecting 8x8's proposed cloud services, you will automatically benefit from the inherent business continuity and disaster recovery that cloud services offer.

Our Architecture is described below and has inherent N+1 resilience throughout. We connect to 26 global tier 1 carriers worldwide and 7 in the UK providing resilience in terms of our PSTN and SIP connectivity.

From a Business continuity perspective our business, core applications and those of our partners are all cloud based and can therefore be accessed from any Internet connected location

At any one time, three database replicas are running—one primary replica and two or more secondary replicas. If the hardware fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is automatically created. So, there are always at minimum two physical, consistent copies of our customers' data in the datacentre. Application servers are also automatically replicated to protect customers of failure of an individual server.

5.7.2 Who is responsible for solution Change Management? Describe the change management process.

ServiceNow

Change Management of the scheme of the system is the responsibility of NSS IT. If there is to be a change performed the appropriate change is required to be raised and authorised within the product itself. In addition to our change management, Service now perform Change management following their fully controlled, authorised and audited change management process.

8x8

8x8 operate Change Management Process in line with ITIL guidelines. 8x8 solutions are tested prior to being brought into service in accordance with pre-agreed test plans, which vary by solution. All planned changes go through a CAB process and risk assessment. Roll back plans are evaluated prior to approval of a change.

The deployment will follow the 8x8 Release and Deployment process, following review and authorisation via the Change Management process

As a SaaS provider we schedule service releases once per quarter. All releases will go through the 8x8 CAB and will be notified to the customer in advance of deployment. Our updates are not service affecting.

5.7.3 What anti-malware controls apply within the solution?

AV scanning is performed by ServiceNow and 8x8 as part of the standard topology of the public could based SaaS.

5.7.4 How are information security incidents (or potential information security incidents) reported, managed and communicated?

With any or potential information security incident, the immediate obligation is to the NSS Adverse Events Management Policy and QPulse. Guidance for Adverse Event Management can be found here.

Case Management System (CMS) is a module built within ServiceNow, in terms of incident management for the SaaS, ServiceNow monitor, analyse and respond to security incidents following their standard operating procedure. Depending on the nature of the incident, ServiceNow security group will escalate and engage response teams necessary to address an incident report to

All events and suspect events that could result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems must be reported immediately.

- Name of person reporting the incident
- The type of data or information involved (be it electronic or physical)
- Whether the loss of the data puts any personal or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of information or equipment affected
- Type and circumstances of the incident

5.7.5 What controls have been employed to ensure continuity of service?

ServiceNow and 8X8 SaaS solutions are globally highly available systems.

5.7.6 Has a business continuity plan and a disaster recovery plan been produced for the solution? Have these plans been tested?

BCDR plans exit for the SaaS solution and is offered as part of the managed service. BCDR tests are ran annually.

5.8 Audit controls

5.8.1 Describe the audit controls employed by the solution. What events are recorded? For how long are audit logs retained? What tools are available to analyse audit logs?

Audit controls employed by the solution

The solution has database audit controls in place which audit database events and queries for the SQL database within the solution. The audit logs are stored in Azure storage.

Audit controls for employees

Internal system audit logs are accessed through the reporting tool that is integrated into the system. All admin events that are performed to and within the SaaS are recorded for accountability reasons, this includes but not exclusive to the following: data uploads, changes to the database, schema changes, user record changes.

Due to the way NSS have setup system access (no default local accounts + ServiceNow have to request access), only NSS admin staff have access to this audit data and do not have to request access from ServiceNow. These

logs are records of what admin changes have been made, login records and high level amendments to any calls raised within NSSs instance. This is configurable and reporting against any fields can be provided.

All user actions are recorded as part of the service of the application.

NSS have configured a policy retention of 7 years + 1 year.

Cloud Log Analytics will provide centralised logging, which can include these records for cloud-based resources.

The system is configured to retain audit logs for at least 6 months.

Cloud Log Analytics will provide centralised logging, which can include these records for both on-premises and cloud-based resources.

5.8.2 Who is responsible for auditing system access?

The SaaS service assures Role based Access Control (RBAC) System access to both ServiceNow and 8x8 is authorised via NSS Active Directory. The NSS Active Directory logging processes and procedures should be consulted for auditing system access. The appropriate level of logging and monitoring is in place adhering to policy.

5.8.3 How are audit logs protected from unauthorised access or modification?

Using in built telemetry as part of the cloud environment, customisable alerting is available across each of these SaaS offerings, this data is stored within the respective cloud environment for 90 days and is accessible to system administrators.

5.9 Solution development, testing and maintenance

5.9.1 Who is responsible for deploying patches and updates?

SaaS is a managed service and the service providers, ServiceNow and 8x8 are responsible for deploying patches and updates. The SaaS offers high availability with no foreseen downtime for patching or update activity.

5.9.2 In what timescales will patches and updates be deployed?

SaaS offers daily vulnerability scanning any vulnerabilities detected are remediated as part of the managed service.

5.9.3 Are any components of the solution **excluded** from the above patching policy?

No.

5.9.4 Describe the patch deployment process.

Patch deployment is offered as part of the managed service. Only approved versions of the SaaS will be available for consumption. ServiceNow and 8x8 are providers of SaaS globally.

5.9.5 What testing controls are in place to understand any potential unintended impacts of updates?

The cloud SaaS providers make Dev, Test and Live platforms available for regulated testing controls.

5.9.6 What agreements are in place to ensure the solution keeps pace with information security developments? For example, migrating onto new information technologies when previous versions become obsolete/unsupported.

The solution is cloud-based SaaS, so security updates are part of the managed service provided by ServiceNow and 8x8.

What security testing has been performed on the solution? What was the outcome of the test? What commitment has been made to ongoing security testing? (this may include things like an IT Health Check on servers, a pen test on external interfaces, vulnerability scans on the servers)

PEN testing is regularly performed on ServiceNow and 8x8 SaaS systems. Tests are performed by a third party on an annual basis, this along with the daily vulnerability scanning helps identify risks and remediation that increase security of the managed service. More information available within he relevant platform SSP.

5.9.7 Is there a separate test and development environment? Is any live data utilised in this environment? How is access to the test and development environment controlled?

There are separate test and development environments. No live data is used in any of the test or development environments.

5.10 Assumptions

5.10.1 What assumptions have been made about security controls that are out of scope of this SSP? For example, assumptions about controls that are believed to be the responsibility of the health boards or suppliers such as end user device security, behaviours or responsibilities, physical/environmental security at operating locations, etc.

It is assumed that:

- the physical and environmental security of the public cloud data centres is the responsibility of the SaaS provider and is out of scope for this SSP
- the security of end user devices used to access the solution are the responsibility of the end user and is out of scope for this SSP

6 Risk analysis and recommendations

This section to be completed in collaboration with the Accreditor/information security practitioner.

6.1 Risk appetite guidance

6.2 A risk appetite provides a guideline for what action should be taken in response to an identified risk.

6.3 The risk appetite of NHS organisations is typically “cautious” and is represented in Table 10 below. This provides an indication of appropriate response to risk.

Extreme	**20-25**	**Unacceptable level of risk exposure that requires immediate corrective action to be taken, and monitoring at Executive and Board level.**
Major	15-19	Unacceptable level of risk which requires measures be put in place to reduce exposure, and monitoring at Executive and Board level,
	10-14	Unacceptable level of risk exposure that requires measures be put in place to reduce exposure and monitoring at Executive level and potentially Board level
Moderate	8 or 9	Acceptable level of risk exposure subject to regular active monitoring measures by senior managers.
Minor or Negligible	1-7	Acceptable level of risk subject to regular passive monitoring measures at local management level.

Table 5: NHS Scotland Risk appetite guideline

6.4 Residual risk statement

6.4.1 No significant residual risk.

6.5 Risk treatment recommendations

6.5.1 Significant residual risks

- No significant residual risks identified within the solution.

6.5.2 Accreditation recommendation

- Information Security and Governance, NSS Digital and Security recommend approval of this SSP.

6.5.3 System Security Policy approved.

7 Annex A – NHS Scotland risk matrices

7.1 Impact/consequence definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Patient Experience	Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care.	Unsatisfactory patient experience/ clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience/ clinical outcome; short term effects – expect recovery <1wk.	Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk.	Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects
Objectives / Project	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives; reputation of the organisation seriously damaged.
Injury (physical and psychological) to patient/visitor/staff.	Adverse event leading to minor injury not requiring first aid.	Minor injury or illness, first aid treatment required.	Agency reportable, e.g. Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity
Complaints / Claims	Locally resolved verbal complaint.	Justified written complaint peripheral to clinical care.	Below excess claim. Justified complaint involving lack of appropriate care.	Claim above excess level. Multiple justified complaints.	Multiple claims or single major claim Complex justified complaint.

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Service / Business Interruption	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service.	Short term disruption to service with minor impact on patient care.	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility. Disruption to facility leading to significant “knock on” effect
Staffing and Competence	Short term low staffing level temporarily reduces service quality (< 1 day). Short term low staffing level (>1 day), where there is no disruption to patient care.	Ongoing low staffing level reduces service quality Minor error due to ineffective training/implementation of training.	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training/implementation of training. Ongoing problems with staffing levels.	Uncertain delivery of key objective/ service due to lack of staff. Major error due to ineffective training/implementation of training.	Non-delivery of key objective/service due to lack of staff. Loss of key staff. Critical error due to ineffectivetraining/ implementation of training.
Financial (including damage / loss / fraud)	Negligible organisational/personal financial loss. (£<1k). (NB. please adjust for context)	Minor organisational/personal financial loss (£1-10k).	Significant organisational/personal financial loss (£10-100k)	Major organisational/personal financial loss (£100k-1m).	Severe organisational/personal financial loss (£>1m).
Inspection / Audit	Small number of recommendations which focus on minor quality improvement issues.	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating. Critical report.	Prosecution. Zero rating. Severely critical report

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Adverse Publicity / Reputation	Rumours, no media coverage. Little effect on staff morale.	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale/public attitudes.	Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation	National media/adverse publicity, less than 3 days. Public confidence in the organisation undermined. Use of services affected.	National/international media/adverse publicity, more than 3 days. MSP/MP concern (Questions in Parliament). Court Enforcement. Public Inquiry/ FAI.

Table 7: Impact/consequence definitions

7.2 Likelihood definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Probability	Rare - can't believe this event would happen – will only happen in exceptional circumstances	Unlikely - not expected to happen but definite potential exists – unlikely to occur.	Possible - may occur occasionally, has happened before on occasions – reasonably chance of occurring	Likely - strong possibility that this could occur – likely to occur	Almost certain - this is expected to occur frequently / in most circumstances – more likely to occur than not

Table 8: Likelihood definitions

7.3 Risk matrix

	Impact				
Likelihood	**Very low (1)**	**Low (2)**	**Medium (3)**	**High (4)**	**Very high (5)**
Very low (1)	Low1	Low 2	Low 3	Medium	Medium
Low (2)	Low	Medium	Medium	Medium	High
Medium (3)	Low	Medium	High	High	High
High (4)	Medium	Medium	High	High	Very High
Very high (5)	Medium	High	High	Very High	Very High

Table 9: Risk evaluation matrix

7.4 NHS Scotland risk appetite statement

7.4.1 NHS Scotland risk appetite is broadly defined as “cautious”: Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward. Further guidance on the acceptance of risk is defined based on residual risk values:

Residual risk value	1-3	4-8	9-19	20+
	Risk acceptable	Risk may be acceptable if all methods for further mitigating or avoiding the risk have been considered	Further reduction of risk strongly recommended	Risk unacceptable

Table 10: Residual risk statement options