|  |  |  |  |
|---|---|---|---|
| Document filename: | **HSCN Compliance Operating Model** |  |  |
| Directorate / Programme | **HSCN** | Project | **Marketplace Creation** |
| Document Reference |  |  |  |
| Project Manager | **Chris Brown** | Status | **Final** |
| Owner | Chris Brown | Version | **1.5** |
| Author | Chris Brown | Version issue date | **11/12/2017** |

# HSCN Compliance Operating Model

# Document Management

## Revision History

| Version | Date | Summary of Changes |
|---|---|---|
| 0.1 | 21/07/2016 | First informal draft for comment |
| 0.2 | 02/08/2016 | To Nick Schlanker for review |
| 0.3 | 05/08/2016 | Draft for HSCIC comments |
| 0.4 | 09/09/2016 | Updated following v3.0 of Obligations Framework |
| 0.5 | 25/10/2016 | Restructured and re-written as Obligations Framework progresses |
| 0.6 | 31/10/2016 | Heavy Edit from Project Manager and rearticulating of process flows pending soft deployment of first of type process and preceding programme team and legal review |
| 0.7 | 03/11/2016 | Uplift post DLA Legal review, addition of appendix section, addition of references to Obligations Framework Op-Cert conditions and addition of Supplier commitment requirements. |
| 0.8 | 04/11/2016 | Uplift post HSCN Commercial and DLA Piper Legal reviews |
| 0.9 | 10/11/2016 | Uplift post Head of Transformation, HSCN Commercial and DLA Piper Legal reviews (round 2) |
| 0.10 | 21/11/2016 | Uplift following DLA comments on version 0.9 and revised (and Industry agreed) CAS(T) compliance position |
| 0.11 | 23/11/2016 | Uplift following input from HSCN Commercial and Innopsis |
| 0.12 | 23/11/2016 | Final tidying by John Matthews |
| 1.0 | 05/12/2016 | Final baselined version following Innopsis Directors review |
| 1.1 | 27/03/2017 | Uplift to provide additional specificity to process |
| 1.2 | 16/05/2017 | Uplift to provide additional specificity to process |
| 1.3 | 13/06/2017 | Uplift to incorporate additional clarity on application tiers and Service Management requirements |
| 1.4 | 16/07/2017 | Uplift of changes |
| 1.5 | 11/12/2017 | Uplifted to incorporate the version 4.3 of the Obligations Framework and version 1.1 of the Service Management Addendum |

### Reviewers

This document must be reviewed by the following people:

| Reviewer name | Title / Responsibility | Date |
|---|---|---|
| Nick Schlanker | Head of Solution Design | Up to version 1: 05/12/2016 |
| Kate Gill | Technical Architect | Up to version 1: 05/12/2016 |
| Ian Cooke | Head of Service Management | Up to version 1.3: 13/06/2017 |
| Paul Evans | Security and Connection Agreement Lead | Up to version 1.3: 13/06/2017 |
| John Matthews | Commercial Lead | Up to version 1: 05/12/2016 |
| Paul Gilliatt | Programme Head | Up to version 1: 05/12/2016 |
| Hazel Randall | Legal Lead | All versions |
| Des Ward | Industry representative – Compliance and IG | Up to version 1.3: 13/06/2017 |

### Approved by

This document must be approved by the following people:

| Name | Signature | Title | Date | Version |
|---|---|---|---|---|
| Paul Gilliatt - Programme | | | | |
| John Matthews - Commercial | | | | |
| Hazel Randall – Legal | | | | |
| DLA Piper – Legal (external) | | | | |
| Des Ward – Industry rep | | | | |

**Document Control:**

The controlled copy of this document is maintained in the HSCIC Sharepoint site. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

# Glossary of Terms

| **Term** | **Definition of Term** |
|---|---|
| Authoritative Technology Services | Provides the support for Domain Name Service and Network Time Protocol to be consumed by other HSCN components and applications that transit HSCN. |
| CAS(T) standards | NCSC Security Standards for telecommunications service providers |
| Compliance or<br>HSCN Compliance or<br>HSCN Compliant | A status as detailed in this document and as updated by the HSCN Authority from time to time throughout the Term and notified to the Supplier |
| Consumer or<br>HSCN Consumer | Means the recipient of HSCN Connectivity Services. |
| CN-SP | An organisation that is supplying or is approved to supply HSCN Connectivity Services having achieved the appropriate HSCN Compliance |
| CN-SP Deed | A deed in the form of the template contained in https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers as executed between the HSCN Authority and a CN-SP |
| HSCN Assurance Mark | Means the HSCN trade mark, short particulars of which are set out in Schedule 4 of the CN-SP Deed |
| HSCN Connectivity Services | Any service which is offered by a CN-SP to provide access to and / or routing over the HSCN |
| HSCN Obligations Framework | The obligations as available at https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers which may be updated from time-to-time by the HSCN Authority |
| ISO/IEC standards | International Management Standards |
| PSN | The Public Services Network |
| Supplier | A supplier (or prospective supplier) of HSCN services |
| The HSCN CN-SP Service Management Requirement Addendum | Means the latest version of the "HSCN CN-SP Service Management Requirement Addendum" as available at https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers |

# Contents

# 1 Introduction

## 1.1 The purpose of this document

This document describes the end state for the Compliance process for HSCN (referred to as "HSCN Compliance"). It details the Processes, Organisation, People, Information, and Technology required to achieve and maintain Compliance.

## 1.2 Key Principles

As stated in obligation OPCERT.1 of the HSCN Obligations Framework, in order for a Supplier to sell HSCN Connectivity Services they must hold **HSCN Compliance** status. HSCN Compliance status confirms that the Supplier adheres to the standards and policies that are set out in the **HSCN Obligations Framework**. The HSCN Compliance process described in this document sets out how HSCN Compliance status is tested and awarded.

The Compliance model adheres to the following set of core principles – the model is:

- Clear as to what is being audited for Compliance, for how long and by whom;
- Recognises equivalent certifications that could be validated as contributing to HSCN Compliance – this includes a set of 'foundation' certifications including PSN, CAS(T) Security and ISO/IEC;
- Reuses existing processes and resources where appropriate;
- Minimises cost and time whilst being sufficiently robust to act as a useful control and assurance mechanism;
- Outlines a process for withdrawal of Compliance and impact; and
- Assists Suppliers with published support.

The HSCN Obligations Framework adheres to the following set of core principles:

- The HSCN Programme will aim to maximise Supplier participation in the HSCN Marketplace (including small, medium and large Suppliers);
- Minimise upfront investment costs for end users and Suppliers; and
- Take a default position to align to and reuse existing standards commonly adhered to already (such as ISO and PSN) and minimise unique requirements – hence the use of 'equivalent' certifications.

Please note – there are a set of specific HSCN Obligations that relate directly to Compliance, these are OPCERT 1 to 5:

- OPCERT.1: Minimum Compliance
- OPCERT.2: Supplier Assessment
- OPCERT.3: Obligation Evidence
- OPCERT.4: Compliance Decision
- OPCERT.5: Renewal Cycle

Please refer to the HSCN Obligations Framework in Appendix 1 for more information.

## 1.3 Key Objectives

The principles detailed in paragraph 1.2 can be combined into the following objectives for the HSCN Compliance process.

The Process will:

- Document clear business and technical scope of service;
- Reuse existing standards and equivalent certifications;
- Minimise cost and time to Suppliers in terms of the application process;
- Minimise cost and time to the HSCN Authority in terms of the auditing process both pre Supplier provision of services and products and also during operational assessment once live;
- Minimise upfront investment where possible;
- Provide robust assessment and assurance of service to Consumers; and
- Provide consistent service to Suppliers independent of the size of the Supplier business – therefore barriers to entry will be minimised where possible.

## 1.4 Key Compliance stages

The Compliance model is made up of 3 core stages:

- **Stage 1 (Pre-market):** Obligations which must be reviewed and met before the Supplier can market/sell HSCN-badged services.

- **Stage 2 (Pre-live):** The relevant obligations which must be met before a Supplier can begin supplying services to Consumers, and connect to the HSCN Authority stood up services – such as the Peering Exchange Network, HSCN Data Security Centre and the Authoritative Technology Services, this stage is part of the wider on-boarding process run by the Service Co-ordination function operated by the HSCN Authority (please refer to the HSCN Solution Overview Version 2.0).

  **Please note:** Once the supplier commences delivery of Services they will be subject to a 3 month probation check where the Authority will run a set of checks to ensure that the supplier is operating in adherence to the Obligations.

- **Stage 3 (Post-live):** Obligations which can only be proven by Supplier performance once the Supplier is delivering HSCN services.

  As part of Stage 3 Compliance, there will be regular and an annual assessment of Supplier performance and adherence to the HSCN Obligations Framework and HSCN's core network analysis and Service Co-ordinator capabilities will be brought in to play to achieve this.

  If a Supplier is found to be non-compliant with any obligation the HSCN Authority can invoke a number of remedies, the ultimate of which would be to revoke Compliance – this process is detailed later in this document. This process would be governed by the conditions set out in the CN-SP Deed and would require formal HSCN Senior Responsible Owner (SRO) approval.

In addition to the HSCN Obligations Framework being used as a basis for Compliance, the Compliance process is supported by two further key governing mechanisms:

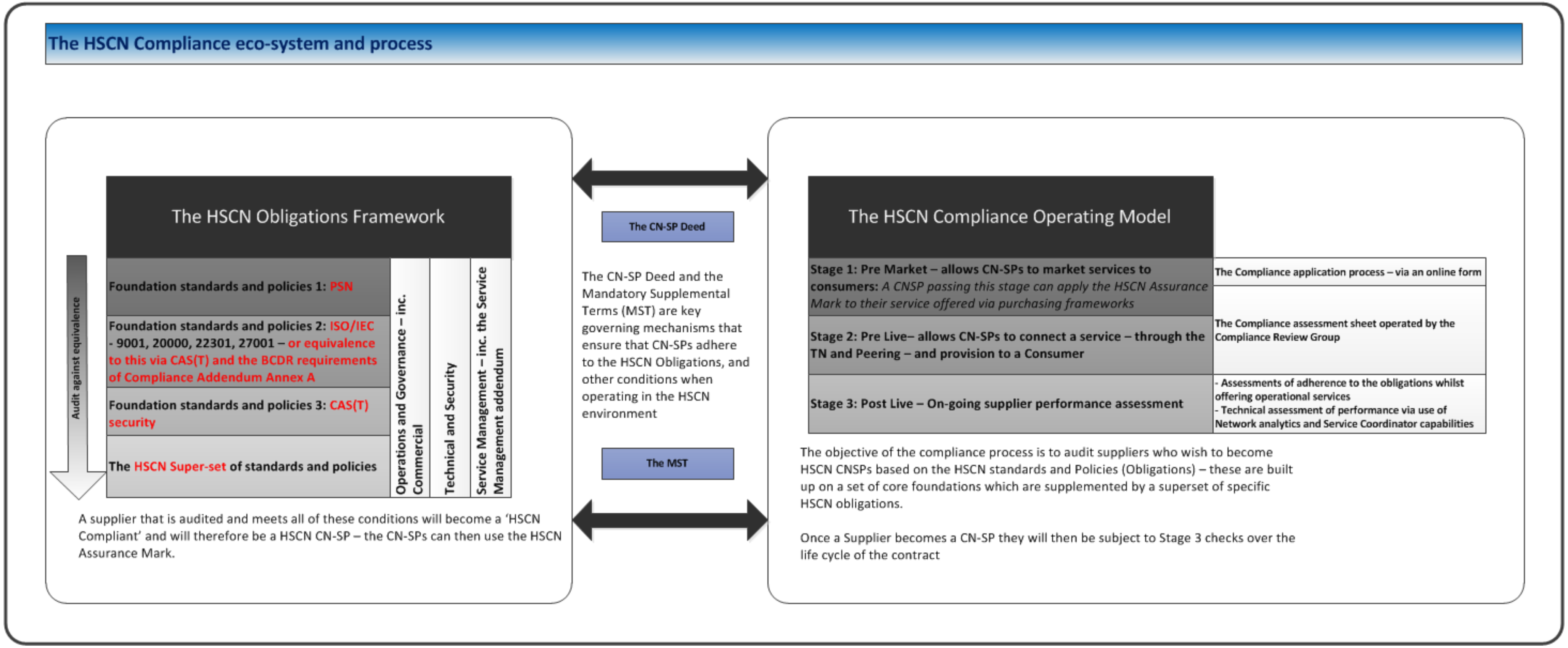
1. The **CN-SP Deed**: The deed, which is signed as part of Stage 1, ensures that the Supplier will adhere to the obligations set by HSCN and that the Supplier will co-operate with other Suppliers operating in the disaggregated HSCN eco-system. It is a legally binding document between the HSCN Authority and each CN-SP. The deed is therefore the key legal mechanism that supports the Compliance process, and, the HSCN Obligations Framework itself.

2. The **Mandatory Supplemental Terms (MST)**: A set of HSCN terms and conditions that also support Compliance and the HSCN Obligations Framework. The MST must be included in the CN-SP/Consumer contract.

   The Supplier's attention is drawn to Clause 5.0 (in particular 5.2) of the CN-SP Deed which may require the Supplier to agree to additional Security Risk Assessments (to be defined between the HSCN Authority and the Supplier).

Figure 1 (overleaf) explains diagrammatically how all of these components work together.

**Figure 1** – High level overview of the Compliance Process and the HSCN Obligations Framework interface



The HSCN Compliance eco-system and process

The HSCN Obligations Framework

Foundation standards and policies 1: PSN

Foundation standards and policies 2: ISO/IEC - 9001, 20000, 22301, 27001 – or equivalence to this via CAS(T) and the BCDR requirements of Compliance Addendum Annex A

Foundation standards and policies 3: CAS(T) security

The HSCN Super-set of standards and policies

Operations and Governance – inc. Commercial
Technical and Security
Service Management – inc. the Service Management addendum

A supplier that is audited and meets all of these conditions will become a 'HSCN Compliant' and will therefore be a HSCN CN-SP – the CN-SPs can then use the HSCN Assurance Mark.

The CN-SP Deed and the Mandatory Supplemental Terms (MST) are key governing mechanisms that ensure that CN-SPs adhere to the HSCN Obligations, and other conditions when operating in the HSCN environment

The HSCN Compliance Operating Model

| | |
|---|---|
| **Stage 1: Pre Market – allows CN-SPs to market services to consumers:** *A CNSP passing this stage can apply the HSCN Assurance Mark to their service offered via purchasing frameworks* | The Compliance application process – via an online form |
| **Stage 2: Pre Live– allows CN-SPs to connect a service – through the TN and Peering – and provision to a Consumer** | The Compliance assessment sheet operated by the Compliance Review Group |
| **Stage 3: Post Live – On-going supplier performance assessment** | - Assessments of adherence to the obligations whilst offering operational services<br>- Technical assessment of performance via use of Network analytics and Service Coordinator capabilities |

The objective of the compliance process is to audit suppliers who wish to become HSCN CNSPs based on the HSCN standards and Policies (Obligations) – these are built up on a set of core foundations which are supplemented by a superset of specific HSCN obligations.

Once a Supplier becomes a CN-SP they will then be subject to Stage 3 checks over the life cycle of the contract

# 2 Overview and governance

## 2.1 A detailed level walk-through of the HSCN Compliance process

This walk-through will explain, how the process will work over the three key stages.

**Pre stage 1**

- HSCN will sign-post Suppliers to a section of the HSCN website which accommodates information covering the HSCN Obligations Framework and this document – a HSCN Compliance Stage 1 application form will also reside in this location.
- HSCN will advise that any Supplier who holds an interest in applying to become a CN-SP downloads the HSCN Obligations Framework, the CN-SP Deed and the Mandatory Supplemental Terms and runs these through their internal governance to assess whether, or not, applying to become a CN-SP is likely to be achievable for them.
- If the Supplier upon conducting an internal review process decides that Compliance is likely to be achievable then they will complete the HSCN Compliance Stage 1 application form which will ask a set of key questions about the Supplier and also existing certification that they hold, covering PSN, ISO/IEC standards and CAS(T).

**Stage 1**

1. **Summary description and purpose**

- The first stage of Compliance that, once confirmed, allows a Supplier to market/sell HSCN-badged services and therefore, become a CN-SP.
- The Supplier will begin the process by completing the HSCN Compliance application form that will be available on the HSCN website – here:

  https://www.digital.nhs.uk/health-social-care-network/Suppliers/compliance-stage1-form

2. **Information required, or pre requisites**

- The Supplier will be asked to complete an application form. This form will incorporate a set of questions covering:
  - The Company – including the Company number, details of leadership, the D-U-N-S number, details of the country of registration; and
  - Certification that is held (or the Supplier 'may' hold) across PSN, ISO/IEC and CAS(T). In addition, the Supplier will be asked to declare a formal commitment that they will adhere to the HSCN Obligations Framework and the CN-SP Deed, and will seek no amendments to the published documentation prior to signature.
- In addition to the questions, there is a set of obligations (from the **HSCN Obligations Framework**) that any Supplier applying for Stage 1 will need to adhere to. Each obligation will require (1) a short response whether this be a declaration that the applicant will adhere to the Obligation or a response based upon their solution, (2) a response to meet the requirement of the evidence cell in the spreadsheet (column D) which will state the type of response that is required.
- Following on from the Obligations Framework response we will require a High Level Design document that covers the solutions based thinking (including network architecture) of the solution that the applicant is proposing. Each Obligation that is

responded to must then be clearly referenced in to the High Level Design Document. Therefore a synopsis response will be required to the spreadsheet based Obligation and this must then be referenced to a High Level Design document section/page number.

- The Supplier will be asked to provide a findings report from their IT HealthCheck (ITHC) – this must meet the requirements set out in the official government guidance on ITHCs. This guidance can be found here:

  https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance

  In addition to the findings report the applicant must also provide the accompanying Remediation Action Plan which will detail how all open issues are to be resolved, and when.

  The Stage 1 obligations are cited in the HSCN Obligations Framework in Appendix 1 – column D ('Evidence required for HSCN Compliance').

### 3. Assessment approach that will be employed, or tools

#### Approach

- The HSCN Authority Programme team (incorporating the Compliance Review Group) will run a set of checks based on the questions asked and the declarations provided. This will include checks on certificates held through PSN, Data Standards Online, and checks with independent CAS(T) assessors.
- Evidence should be submitted either as a written response (which HSCN can then check against) or an attachment referenced from the relevant obligation.
  **Note:** The ITHC will require a specific written response in accordance with the standard HM Government guidance linked to above.

#### Tools

- The Compliance Review Group (CRG) administrator will utilise a spreadsheet model that is based on the HSCN Obligations Framework – Equivalent certification held is filtered to enable the CRG to determine a super-set of specific obligations that require assessment.

### 4. Compliance, or failure notification method

#### Confirming Stage 1 Compliance (a 'pass')

- If the Supplier passes Stage 1 checks then they will achieve CN-SP status – in order for this to be formally confirmed the Supplier will be required to sign the CN-SP Deed at this stage.
- Upon receipt of the signed CN-SP Deed, HSCN will write to the Supplier and will provide the HSCN Assurance Mark for marketing purposes.
- In addition we will cite their compliant status in the list of compliant Suppliers on our website.

#### If the Supplier fails this stage

- If a Stage 1 application fails the Supplier will be advised of this and the reasons for failure in writing. In such an instance the Supplier will be able to re-submit an application as long as the requirements cited in the reason for the initial failure are rectified.

5. **Maintenance required once this stage has been confirmed**

- Once a Supplier passes through Stage 1 and becomes a CN-SP it will be legally obliged (due to signing the CN-SP Deed) to maintain its status based on all certifications assessed and obligations adhered to – the Stage 3 Compliance checks (which will incorporate a yearly re-assessment of Compliance) will ensure that the HSCN Authority will police adherence robustly.

### Stage 1 - Further information

### Declaration of commitment to adhere to the HSCN Obligations Framework and CN-SP Deed

It is at this stage where we will ask (in the application form) for the applicant to specifically declare a **commitment** that they will adhere to the conditions of the HSCN Obligations Framework and they will formally commit to undertake activities that are key for the service(s) being delivered. This ensures both the HSCN Authority, and indeed, HSCN Consumers whom the Supplier may wish to market services to post Stage 1 that the HSCN Assurance Mark is issued with auditable evidence that the Supplier has stated explicitly that they will fully comply to the HSCN Obligations in the event of challenge or non-conformance when HSCN Connectivity Services are operational, or prior to operational go live status.

### The application form

The contents of the application form, and the outcomes of our assessment will also be held by the HSCN Authority in a data and information management repository (initially a SharePoint solution) – in the future 'steady state' this data will be held in the HSCN Management System (HMS).

The key information required for Stage 1, and asked for on the application form, will include:

- Company name;
- Country of Registration[1];
- Name of the company officer signing the CN-SP Deed;
- Name of the company officer accountable for completing the Compliance application process and a nominated point of contact for the HSCN Authority whilst the assessment process is being undertaken;
- Companies House number and also a D-U-N-S number;
- ISO certification claimed – declared;
- ISO certification numbers;
- CAS(T) (or ISO 27001) certification claimed and proof – or, formal sign-up to the limited time Transition period (please refer to section 2.4) if only 'critical' conditions can be met at this time;
- PSN Compliance claimed and proof;
- The 'commitment' statement box check; and

[1] If a Company is not registered and or operating from the UK then the HSCN Authority reserves the right to request further information around the company structure

- A statement declaring that ITHC findings will be provided to HSCN for review - and, if necessary, any remediation actions required will have taken place prior to provisioning any service, and the outcomes of this will be available to HSCN consumers.

Evidence should be submitted either as a written response (which the HSCN Authority can then check against) or an attachment referenced from the relevant obligation. These artefacts will then be assessed by HSCN staff with the relevant experience/skills.

If a Stage 1 application fails the Supplier will be advised of this and the reasons for failure in writing. The Supplier will be able to re-submit an application as long as the requirements cited in the reason for the initial failure are rectified.

The application form questions for Stage 1 are presented in this application form:

https://www.digital.nhs.uk/health-social-care-network/Suppliers/compliance-stage1-form

## Stage 2

### 1. Summary description and purpose

- The second stage of Compliance that, once confirmed, allows a Supplier (now the CN-SP) to provision a permanent live connection between their network and the HSCN Authority stood up services – such as the Peering Exchange Network,  HSCN Data Security Centre and the Authoritative Technology Services - and a service to a HSCN Consumer.
- Stage 2 therefore engages at the on-boarding stage and can begin once the core HSCN capabilities, such as the HSCN Authority stood up services, are deployed and ready to be connected to.
- Stage 2 Compliance will ensure that the CN-SP is able to connect to the HSCN without putting the network at risk and that the Supplier has the processes in place to support the collaborative approach in the multiple Supplier eco-system, such as working together to solve incidents.
- It is at this stage, when the Supplier is close to provisioning HSCN Connectivity Services (note – the core HSCN capabilities such as HSCN Authority stood up services – such as the Peering Exchange Network,  HSCN Data Security Centre and the Authoritative Technology Services must be in place at this point),  where an additional assessment will be carried out by the Compliance Review Group covering the Supplier's technical, security and service management capabilities. This stage will cover the key 'pre go-live' checks.

### 2. Information required, or pre requisites

- The Supplier will need to present the following types of evidence at Stage 2:

  - A written response (if specifically required) to the Obligations if required in the HSCN Obligations Framework 'Evidence required for HSCN Compliance' section – **this will include uplifting the Stage 1 High Level Design in to a Detailed Design document**.

  - The Supplier shall meet the requirements of the HSCN CN-SP Service Management Requirement Addendum (via a detailed Service Management design) providing specific responses to this which the Authority can assess (again the specifics on what is required in the response are articulated in the Obligations Framework evidence column D) - the Authority may also request that the supplier runs service rehearsals or service acceptances tests that are to be witness-able by the Authority. Please draw this in to a specific detailed design which is sectioned out by the process areas listed in the obligations framework.

- For Technical/Security and Operations/Governance the Supplier will provide design documentation as stipulated in the HSCN Obligations Framework advising where content related to a specific obligation sits.
- The Authority will provide guidance on how the Supplier should connect to HSCN infrastructure components such as the Peering Exchange, ANM and NAS. This will also include a specification of the types of tests that will need to be run and the Supplier will be asked to provide a test plan to cover their approach to testing.

- The specific evidence required is cited in the HSCN Obligations Framework embedded in Appendix 1:

    - A statement of residual risk;
    - Operational processes and procedures (or null return if applicable);
    - Test plans and results – based on Peering Exchange testing;
    - Sample Quality of Service utilisation report; and
    - For the Service Management assessment, all Suppliers will be required to provide Service Desk contact details and network monitoring tool accounts.

### 3. Assessment approach that will be employed, or tools

#### Approach

- The assessment approach at this stage will involve the HSCN Authority CRG subject matter experts across the full sphere of technical, security, service management, commercial and legal running an assessment based upon artefacts provided by the Supplier.
- Artefacts should be submitted as a written response (which the HSCN Authority can then check against). The artefacts will likely be existing Supplier design documents and the HSCN Authority will ask the Supplier to point to specific sections of their documentation which covers the requirements of specific obligations (referring to the HSCN Obligations Framework ‘Evidence required for HSCN Compliance’ section).

#### Tools

- The HSCN Authority CRG administrator will utilise a bespoke spreadsheet model that is based on the HSCN Obligations Framework – this will support the CRG in checking off obligations that have been confirmed as being met based upon the assessment of Supplier presented artefacts.

### 4. Compliance, or failure notification method

#### Confirming Stage 2 Compliance (a ‘pass’)

- If the Supplier passes Stage 2 assessment then they will be allowed to connect to the HSCN via the Peering Exchange;
- The HSCN Authority will write to the Supplier to advise them of their confirmed status; and
- In addition we will cite their compliant status in our list of compliant Suppliers on our website.

**If the Supplier fails this stage**

- If a Stage 2 application fails, the Supplier will be advised of this and the reasons for failure in writing. In such an instance the Supplier will be able to re-submit an application as long as the requirements cited in the reason for the initial failure are rectified.

### 5. Maintenance required once this stage has been confirmed

- Once a Supplier passes through Stage 2 and is permitted to connect to HSCN and physically provision services to Consumers they will be legally obliged (due to signing the CN-SP Deed) to maintain the statuses based on all certifications assessed and obligations adhered to – the Stage 3 Compliance checks (which will incorporate a yearly re-assessment of Compliance) will ensure that HSCN will police adherence robustly.

## Stage 3

Stage 3 Compliance focusses on the assessment of the on-going adherence to the HSCN Obligations Framework – Stage 3 can only be conducted when CN-SPs are supplying live HSCN Connectivity Services as it is solely reliant upon live performance.

Although the CN-SPs will be monitored throughout their contract tenures as a matter of course they will be formally assessed once per year, as outlined below.

Those obligations that require a regular data feed will be used to generate a dashboard that will show service status to the HSCN Authority. Performance against quantitative (measureable) obligations will be monitored by the Service Co-ordinator and Network Analytics Service. Any significant issues will be picked up by the HSCN Authority for actioning.

In the event that either monitoring or a HSCN Consumer complaint raises a significant issue with performance, or adherence to the HSCN Obligations Framework, the HSCN Authority will, with the Service Co-ordinator and Network Analytics capability, work to determine a root cause of the issue. Then, supported by the CN-SP Deed, the HSCN Authority will work to implement a resolution with the CN-SP to ensure the issue is concluded satisfactorily.

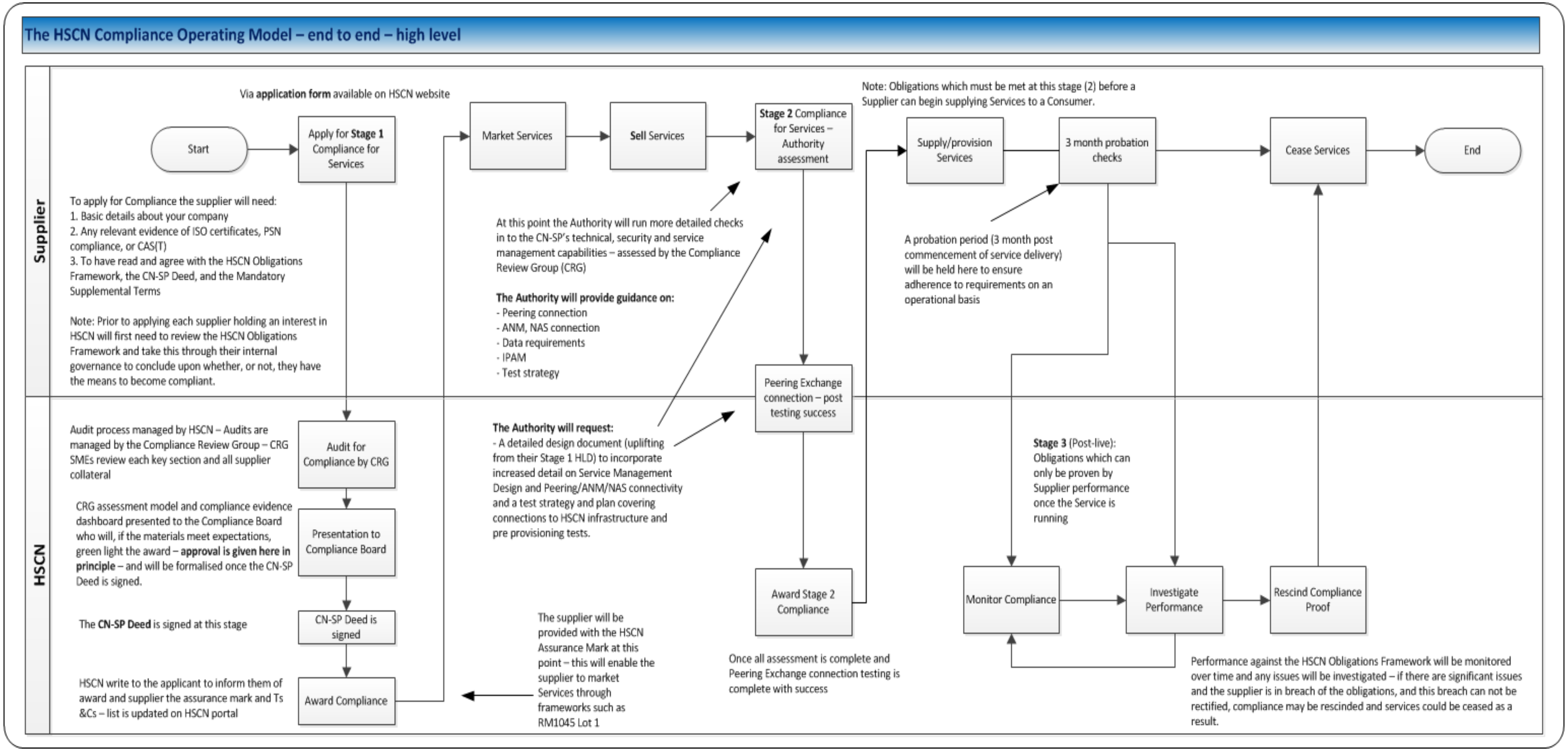
Figure 2 presents the key stages, and the logic that supports these stages.

### Monitoring types

- **Ongoing monitoring:** The HSCN Authority will carry out operational monitoring on an on-going basis to ensure that the service(s) are being delivered in a manner appropriate to the requirements of the HSCN Obligations. Any issues will be captured by the HSCN Service Coordinator and managed via the HSCN Authority – it is the HSCN Authority that will inform the CN-SP that is in non-compliance and manage the issue through to remedy with the CN-SP; and

- **Once per year assessment:** A specific assessment into Supplier conformance to the HSCN Obligations will be carried out once per year on, or as close as possible to, the anniversary date of a CN-SP achieving Stage 1 HSCN Compliance. Again, the HSCN Authority will be responsible for communicating any issues to the CN-SP and managing these through to remedy.

**Figure 2**: the three stages Compliance process – logic flow


The HSCN Compliance Operating Model – end to end – high level
Supplier
HSCN
Start
Apply for **Stage 1** Compliance for Services
Market Services
**Sell** Services
**Stage 2** Compliance for Services – Authority assessment
Supply/provision Services
3 month probation checks
Cease Services
End
Peering Exchange connection – post testing success
Audit for Compliance by CRG
Presentation to Compliance Board
CN-SP Deed is signed
Award Compliance
Award Stage 2 Compliance
Monitor Compliance
Investigate Performance
Rescind Compliance Proof

Via **application form** available on HSCN website

To apply for Compliance the supplier will need:
1. Basic details about your company
2. Any relevant evidence of ISO certificates, PSN compliance, or CAS(T)
3. To have read and agree with the HSCN Obligations Framework, the CN-SP Deed, and the Mandatory Supplemental Terms

Note: Prior to applying each supplier holding an interest in HSCN will first need to review the HSCN Obligations Framework and take this through their internal governance to conclude upon whether, or not, they have the means to become compliant.

At this point the Authority will run more detailed checks in to the CN-SP's technical, security and service management capabilities – assessed by the Compliance Review Group (CRG)

**The Authority will provide guidance on:**
- Peering connection
- ANM, NAS connection
- Data requirements
- IPAM
- Test strategy

Note: Obligations which must be met at this stage (2) before a Supplier can begin supplying Services to a Consumer.

A probation period (3 month post commencement of service delivery) will be held here to ensure adherence to requirements on an operational basis

Audit process managed by HSCN – Audits are managed by the Compliance Review Group – CRG SMEs review each key section and all supplier collateral

CRG assessment model and compliance evidence dashboard presented to the Compliance Board who will, if the materials meet expectations, green light the award – **approval is given here in principle** – and will be formalised once the CN-SP Deed is signed.

The **CN-SP Deed** is signed at this stage

HSCN write to the applicant to inform them of award and supplier the assurance mark and Ts &Cs – list is updated on HSCN portal

**The Authority will request:**
- A detailed design document (uplifting from their Stage 1 HLD) to incorporate increased detail on Service Management Design and Peering/ANM/NAS connectivity and a test strategy and plan covering connections to HSCN infrastructure and pre provisioning tests.

The supplier will be provided with the HSCN Assurance Mark at this point – this will enable the supplier to market Services through frameworks such as RM1045 Lot 1

Once all assessment is complete and Peering Exchange connection testing is complete with success

**Stage 3** (Post-live): Obligations which can only be proven by Supplier performance once the Service is running

Performance against the HSCN Obligations Framework will be monitored over time and any issues will be investigated – if there are significant issues and the supplier is in breach of the obligations, and this breach can not be rectified, compliance may be rescinded and services could be ceased as a result.

## 2.2 Proof of Compliance

There will be two methods of identifying the Suppliers who have achieved HSCN Compliance:

- A list of compliant Suppliers on the HSCN website; and
- Use of the HSCN Assurance Mark which will be granted subject to specific T&Cs; and

Once the Supplier has achieved Stage 1 Compliance they will be provided with the HSCN Assurance Mark to promote their HSCN service offerings.

Note: HSCN Compliance will not automatically enable a supplier to qualify for any Framework such as those operated by the Crown Commercial Service. The Supplier shall be solely responsible for any such applications in accordance with the relevant procurement regulations.

**Issuing the HSCN Assurance Mark – Business Rules**

- The HSCN Assurance Mark will be issued once the Supplier passes Stage 1 compliance and has signed the CN-SP Deed to become a CN-SP;
- The HSCN Assurance Mark will be issued to the Supplier via secure NHS Mail as a JPEG file once the CN-SP Deed has been signed; and
- Terms and Conditions covering the use of the HSCN Assurance Mark will be attached to this issue email – this will include legal conditions and guidance covering how the HSCN Assurance Mark should be incorporated in to documents/web pages.

Note: If a Supplier is deemed to be non-compliant to the HSCN Obligations Framework or the CN-SP Deed, the HSCN Authority can after complying with the process described in the CN-SP Deed require that the HSCN Assurance Mark is removed from Supplier materials – please refer to section 2.3 for more information on the Rejection/Revocation of HSCN Compliance status.

## 2.3 Non-Compliance

**Rejection of HSCN Compliance status**

If, based on the Compliance assessment at either Stages 1 or 2 (therefore pre go-live), it is found that a Supplier is not meeting, or adhering, to an obligation, the HSCN Authority will notify the Supplier with specific information covering the item(s) that need to be rectified prior to Compliance being awarded – the Supplier may then take remedial action for reassessment.

**Revocation of HSCN Compliance status**

Where the Supplier holds HSCN Compliance status and is found to be non-compliant with one or more of the HSCN Obligations, the HSCN Authority may use any of the remedies described in the CN-SP Deed.

**Mandatory Exclusions**

Where the Supplier would be excluded from participation in a procurement procedure pursuant to one of the grounds for mandatory exclusion contained in section 57 of the Public Contracts Regulations 2015, the HSCN Authority shall take this into account regarding that Supplier's HSCN Compliance status, and:

- where the Supplier is in the process of applying for HSCN Compliance status, such status will be rejected; or
- where the Supplier holds HSCN Compliance status, such status will be revoked.

## 2.4 Security and Service Management Compliance through CAS (T) Assurance

The primary security obligation for HSCN is equivalence to the CAS(T) certification. The HSCN Information Assurance Requirements for HSCN Suppliers are based on the CAS(T) (CESG Assured Service (Telecommunications)) requirements. CAS(T) does also cover some key Service Management, Business Continuity and Disaster Recovery requirements – which have been augmented to ensure that specific HSCN security and service management requirements are incorporated prior to award of **stage one** compliance.

These controls are taken from ISO/IEC-27001:2013 (ISO27001) and were identified in consultation with the Industry, CESG (now the National Cyber Security Centre) and the HSCN Programme Security Sub-Board and the NHS Digital Service Management function as being an appropriate control set against the risk of compromise leading to loss of availability of HSCN services.

Further information on CAS(T) can be found at:

https://www.cesg.gov.uk/articles/policy-and-guidance-documentation-suite-cast

The scope of Compliance shall be the end-to-end provision of HSCN services.

The CAS(T) Annex A (which can be found in Appendix 3) sets out the minimum scope for controls required for HSCN Compliance.

If as part of that scope of service, the HSCN Supplier is providing services that are already CAS(T) certified, assurance is met by the existing certificate. Further assurance will, however, be required for those parts of the service that are not covered by existing certification.

**Security and Service Management compliance requirements**

Annex A sets out the minimum scope for information and service assurance required for the HSCN Security Compliance.

The minimum baseline set of compliance requirements to become an HSCN Supplier are the following:

- Requirements marked as **HSCN Minimum Compliance Baseline** in Annex A – these set out the minimum set of security, business continuity and service management controls;
- Requirements marked as **HSCN Minimum Compliance Baseline** under the Business Continuity Planning, Configuration management, Control performance, Governance, Incident management, Operations management, Risk assessment, Scope and Supply chain assurance categories in Annex A – these complete the HSCN baseline for compliance; and
- Carry out an ITHC scoped in accordance with guidance in Annex B – ITHC scoping.

This ITHC ensures a minimum quality of security controls in place, and provides information to HSCN Consumers about the quality of a HSCN Supplier's security controls with regard to HSCN services. An ITHC carried out as part of the CAS(T) certification will suffice as long as the minimum scope is met, and that the CAS(T) certification covers the proposed HSCN services.

## Assurance of Security Compliance

There are three ways in which a HSCN Supplier can demonstrate Compliance with the minimum security requirements. Each HSCN Supplier must provide assurance for the HSCN services through at least one of the three methods set out below:

1) **Accredited** - hold and maintain full (thus meeting all controls currently) current CAS(T) certification for the services provided – to the level required for the HSCN Minimum Compliance Baseline – as per the MCB filter in Annex A of the Compliance Addendum. A plan articulating how the remaining requirements marked as 'Mandatory' will be audited must be created for stage 1 application and available for HSCN Authority review (on request);
2) **Audited** - hold and maintain current ISO/IEC-27001:2013 certification (for the services provided) for an ISMS that includes the HSCN Minimum Compliance Baseline requirements at the point of becoming an HSCN Supplier (i.e. prior to Stage 1 application) and achieve coverage for the remaining CAS(T) requirements marked as 'Mandatory' by 1st April 2019 at the latest. A plan articulating how the remaining requirements marked as 'Mandatory' will be implemented must be created for stage 1 application and available for HSCN Authority review (on request). For this tier – **all 'Critical' and 'Mandatory' controls required by HSCN for the minimum compliance baseline** need to be implemented and evidenced prior to stage 1 application – as per the MCB filter in Annex A of the Compliance Addendum. ISMS certification audits must be conducted by a UKAS-accredited auditor and attaining Accredited Status by 1st April 2019 at the latest; and
3) **Asserted** - Self-assert compliance (for the services provided) with the CAS(T) 'Critical' and 'Mandatory' requirements for the HSCN Minimum Compliance Baseline at the point of becoming an HSCN Supplier (i.e. prior to Stage 1 application) and achieve coverage for the remaining CAS(T) requirements marked as 'Mandatory' by 1st April 2019 at the latest. Must also attain Accredited status by 1st April 2019 (or if asked to by the HSCN authority). A plan articulating how the remaining requirements marked as 'Mandatory' will be implemented must be created for stage 1 application and available for HSCN Authority review (on request). For this tier – **all 'Critical' and 'Mandatory' controls required by HSCN for the minimum compliance baseline** need to be implemented and evidenced prior to stage 1 application.

The HSCN Minimum Compliance Baseline controls are outlined in **Annex A of the Compliance Addendum.**

In each case, HSCN Suppliers must make available a statement of residual risk available to Consumers (current and future) and the HSCN Authority on request. Residual risks that must be included are:

- All un-remediated ITHC findings higher than medium;
- All components that are part of the MCB (as defined within the CAS(T) security procedures referenced above) to the delivery of the services that are not assured to the correct level of availability under CAS(T); and
- All components of the services that are under the Consumer's management or out of the providers' control (i.e. wires only circuits and radio from the mast in terms of mobile respectively).

**Please note:** As part of the Compliance process HSCN will require that CAS(T) certification and ISO27001:2013 certification is provided by an independent provider.

### How will HSCN manage cases where applicants do not hold full Compliance at the point of application?

A staged approach has been agreed, which is summarised in figure 3 below, using the Declaration and Certification options for verification. The staged approach provides for the following statuses in relation to security Compliance **- Asserted**, **Audited** and **Accredited** as identified above. This approach will be known as the ‘Transition period for formal assurance of Compliance’- this will be referred to as the ‘Transition period’.

Compliance with HSCN requirements for information and service assurance remains part of the overall Compliance process, while having its own transitionary approach to full Compliance. Achieving Asserted status will satisfy the HSCN minimum compliance baseline, but CAS(T) certification from a UKAS auditor must be achieved by 1 April 2019 and to attain Accredited Status.

In order to ensure full visibility of any Supplier’s progress (a Supplier that is subject to the transition period), the HSCN Authority will set a number of checks against each Supplier over the Transition period. This will ensure that the HSCN Authority is kept fully appraised of progress made toward full Compliance and is able to act early if it seems likely that full Compliance will not be met within the Transition period. The HSCN Authority will have the right, under the terms of the CN-SP Deed, to revoke Compliance and stop a Supplier from selling any further services should they fail to achieve compliance required from the Audited or Accredited tier within the defined transition period or retain existing Audited or Accredited certification.

### The CAS(T) Transition period – what must a Supplier do?

Suppliers will be able to achieve HSCN compliance during the Transition period without full (Accredited) CAS(T) certification but must:

- Be (and remain) compliant with the HSCN minimum compliance baseline from the outset;
- Provide an assurance that this baseline is implemented from the outset – therefore they must have an independent member of the CHECK scheme carry out an IT Health Check before selling services (and annually thereafter), and make a copy of the residual risk report available to the HSCN Authority (and potential customers). The ITHC that will be required for Stage 1 is a key assurance for PSN Suppliers and is necessary for CAS(T) compliance. Please refer to Annex B of the Compliance Addendum for more information on how to conduct an ITHC;
- Achieve formal CAS(T) accredited certification within 2 years of achieving Stage 1 compliance or by 1 April 2019 (as a firm deadline) if Stage 1 compliance is achieved after 1 April 2017;
- Obtain CAS(T) accredited certification from an independent assurance body that is recognised by NCSC (for CAS(T)); and
- Retain compliance and the Supplier will not be able to obtain interim HSCN Compliance on the basis of a lapsed formal certification (**Note:** Suppliers, holding PSN compliance, or certification with ISO/IEC-20000:2011 or ISO/IEC-22301:2012 cannot downgrade their compliance and take advantage of the transition period – that’s not what its intended for).

### Risk Mitigation

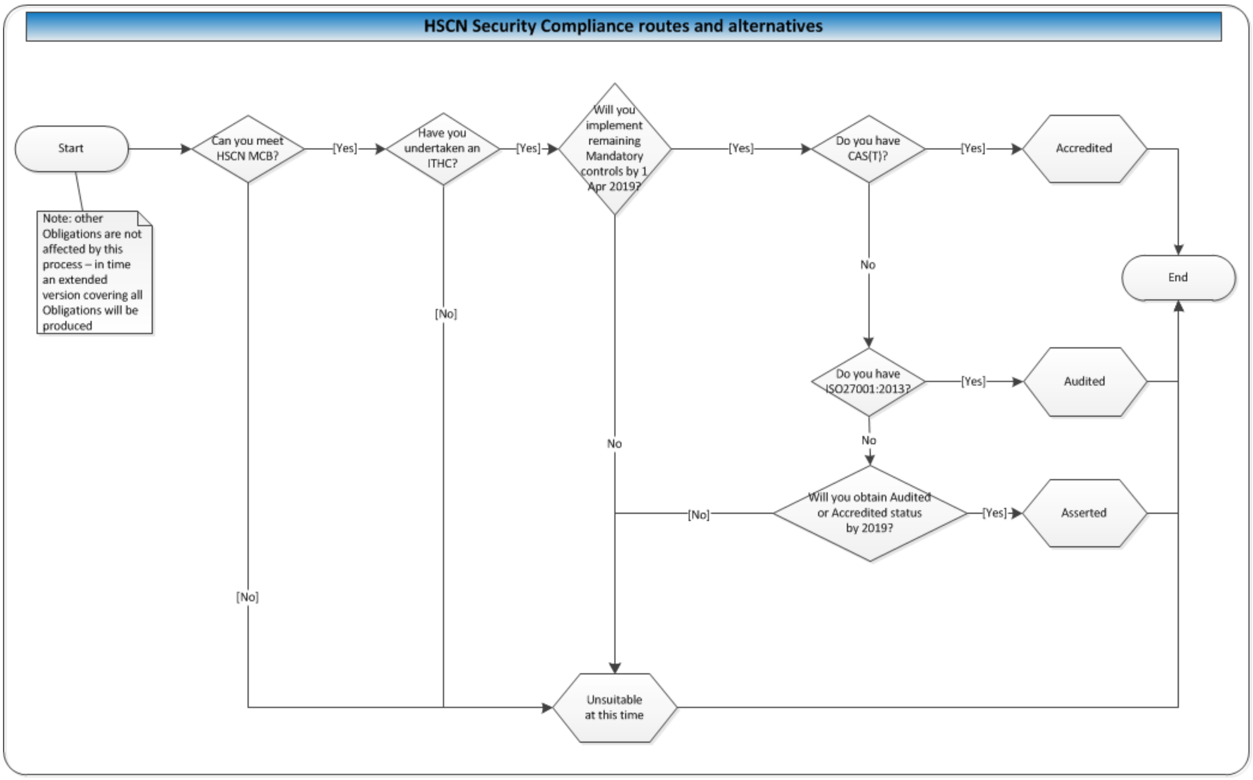
To further mitigate risks associated with non-independently verified Suppliers HSCN apply some conditional measures on Suppliers during the transition period. HSCN has incorporated wording in to the CN-SP Deed that:

- Makes provision for the HSCN Authority to require any Supplier (irrespective of current assurance level) to conduct a risk assessment, based on market share and taking into account geography and care settings of customers. This risk assessment shall review the risk to the availability of the HSCN service, including impact levels of all assets providing the service and be based on an agreed risk methodology. The output of that risk assessment must include any additional security controls and / or levels of assurance required, and must be satisfactory to the HSCN Authority (acting reasonably) based on the risk to availability of the HSCN and impact levels of all providing services; and
- If the Supplier fails to comply or reach agreement with the HSCN Authority, then the ultimate sanction available to the HSCN Authority is to suspend the Supplier from selling HSCN services. This means the HSCN Authority monitoring the number and type of connections that each Supplier has sold against agreed criteria of what constitutes an acceptable market share to the HSCN Authority / DH for Suppliers with no independent assurance of the implementation of the security controls.

### Maintenance of CAS(T) compliance

Suppliers that are already CAS(T) certified will not be allowed a Transition period and must retain (and maintain) their CAS(T) certification (compliant with the HSCN minimum compliance baseline) from the point that they apply for HSCN Compliance.

**Figure 3:** Security Compliance routes and alternatives


HSCN Security Compliance routes and alternatives
Start
Can you meet HSCN MCB?
[Yes]
Have you undertaken an ITHC?
[Yes]
Will you implement remaining Mandatory controls by 1 Apr 2019?
[Yes]
Do you have CAS(T)?
[Yes]
Accredited
End
Note: other Obligations are not affected by this process – in time an extended version covering all Obligations will be produced
[No]
No
Do you have ISO27001:2013?
[Yes]
Audited
No
No
[No]
Will you obtain Audited or Accredited status by 2019?
[Yes]
Asserted
[No]
Unsuitable at this time

The full **CAS(T) control list** (CAS(T) Annex) can be found in Appendix 3.

This annex lists the security controls, categories, criticality of the control, sets out additional guidance and also provides a mapping (if appropriate) to other existing ISO/IEC controls.

Please note the ‘criticality’ column outlines a status for each control in terms of the HSCN requirement to have the control and, at what point.

Suppliers must be compliant with the critical and mandatory conditions in the Governance category of the Annex as a minimum at the point of Stage 1 application.

Ultimately, in order to become a HSCN CN-SP the Supplier needs to be compliant with the HSCN minimum compliance baseline at the stage one compliance application, all the controls set out in the CAS(T) annex by 1 April 2019 and be able to demonstrate compliance through independent assurance (CAS-(T) or ISO27001)).

## 2.5 Governance

Ownership for the Compliance business system will sit in the HSCN Authority which will be responsible for sourcing the required skills.  Prior to this the HSCN Programme will manage the process to bring the first wave of CN-SPs in to the HSCN.

Changes to the Compliance process and HSCN Obligations Framework will be managed through the Change Control Process (a separate piece of collateral), which encourages collaboration between industry and the HSCN Authority.

The HSCN Authority will continue to work collaboratively with Innopsis and other industry bodies which may become appropriate, to develop and maintain the Compliance process to meet the needs of both the HSCN Authority and the commercial needs of the Suppliers.

# 3 The Compliance Review Group

The Compliance Review Group (CRG) will be responsible for  running the Compliance assessment process. The Group will be made up of subject matter experts from within the HSCN Authority and will incorporate expertise in:

- **Technical/networking**
  With expert knowledge of: Technical architecture, Network design,
- **Network security**
  With expert knowledge of: Technical architecture, Network design, Security design and CAS(T), International quality standards
- **Service Management**
  With expert knowledge of: ITIL standard processes and applications, International quality standards
- **Commercial and Governance**
  With expert knowledge of: The overall commercial framework supporting HSCN and specialist legal and contracting expertise
- **Finance**
  With expert knowledge of: Management accounting and the financial model that supports the commercial construct
- **Legal**
  With expert knowledge of: An HCSN Authority legal expert will undertake this role supported, where required, by an external legal firm.

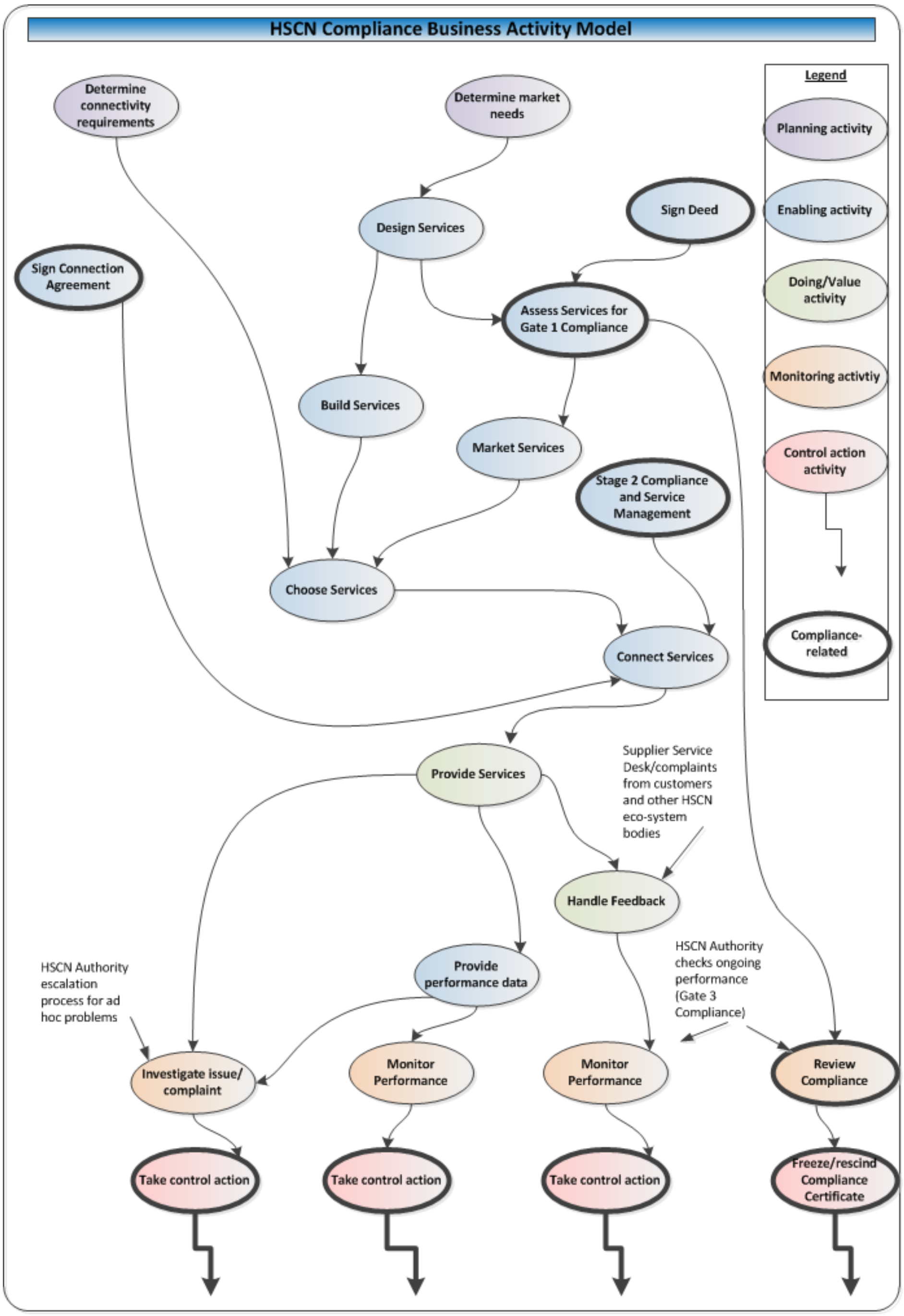
The CRG will be supported by a small administration team.

The group will not be operational on a full-time basis, rather, the group will be called at the request of the lead compliance assessor as and when technical expertise is required.

# 4 Business Activity Model

This view shows the logical dependencies between activities, and assigns no responsibility for those activities. It is used to sequence work through the process by showing pre-requisite activities, and to ensure completeness – that no necessary activity is omitted from consideration.

**Figure 4:** The Compliance Business Activity Model


HSCN Compliance Business Activity Model
Determine connectivity requirements
Determine market needs
Design Services
Sign Deed
Sign Connection Agreement
Assess Services for Gate 1 Compliance
Build Services
Market Services
Stage 2 Compliance and Service Management
Choose Services
Connect Services
Provide Services
Supplier Service Desk/complaints from customers and other HSCN eco-system bodies
Handle Feedback
HSCN Authority checks ongoing performance (Gate 3 Compliance)
HSCN Authority escalation process for ad hoc problems
Provide performance data
Investigate issue/ complaint
Monitor Performance
Monitor Performance
Review Compliance
Take control action
Take control action
Take control action
Freeze/rescind Compliance Certificate
Legend
Planning activity
Enabling activity
Doing/Value activity
Monitoring activtiy
Control action activity
Compliance-related

# Appendix section

## Appendix item 1: The HSCN Obligations Framework

The HSCN Obligations Framework (version 4.3) is embedded here:

HSCN Obligations
Framework version 4.

## Appendix item 2: The HSCN CN-SP Service Management Requirement Addendum

To support the HSCN Obligations Framework Service Management section.

The HSCN CN-SP Service Management Requirement Addendum (version 1.1) is embedded here:

HSCN Service
Management Addenc

## Appendix item 3: The Compliance Addendum and Annex A

This Addendum and Annex lists the security controls (CAS-T), Service Management and BC/DR controls, criticality of the control, and also sets out additional guidance and provides a mapping (if appropriate) to other existing ISO/IEC controls.

Please note the **Minimum Compliance Baseline** column outlines a status for each control in terms of the HSCN requirement to have the control and, at what point.

Suppliers must be compliant with the Critical and Mandatory conditions in the Governance category of the Annex as a minimum at the point of Stage 1 application.

Ultimately, in order to become a CN-SP the Supplier needs to be compliant with all the controls set out in the CAS(T) Annex by 1 April 2019 and be able to demonstrate compliance through independent assurance (CAS-(T) or ISO27001:2013)).

The Addendum and Annex document is embedded here:

HSCN Obligations
Framework Complianc

# Appendix item 4: Security Compliance: Commitment tiers in detail

This appendix contains the principles associated with the 3 core tiers of commitment – the requirements on the supplying organisation in terms of what the supplier needs to **have/hold**, and what they will need to **do** to meet the requirements of each tier.

## Asserted tier

I commit that our organisation **has**:

- ensured that the scope of the services proposed for HSCN compliance meets the definitions laid out in the 'Scope' category of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- ensured that the scope of the services proposed for HSCN compliance has been risk assessed according to the 'Risk Assessment' category of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- identified where compliance with the technical, security and service management sections of the obligations framework is evidenced within supporting documentation supplied (i.e. High Level Designs, contracts and service management documentation)
- implemented the Critical controls of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- implemented the Mandatory controls within the 'Business Continuity Planning', 'Configuration management', 'Control performance', 'Governance', 'Incident management', 'Operations management' and 'Supply chain assurance' categories of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- created a plan of how all remaining Mandatory controls in Annex A will be implemented (to the level specified within column D – "CAS(T) additional guidance") prior to the 1st April 2019
- ensured an IT Health Check (ITHC) is conducted by an organisation delivering CHECK, CREST or Tiger security testing services for the scope of service provided as per the government ITHC guidance (https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance)**, incorporating the additional requirements within A.18.2.3 from Annex A and ITHC scoping guidance within Annex B of the HSCN Supplier Compliance Addendum** and renewed prior to the anniversary of compliance
- provided a residual risk statement (or null return) covering:
    - all unremediated ITHC findings higher than medium
    - all components that are critical to the delivery of services that are not assured to the correct level of availability under Chapter Five of the CAS(T) security procedures
    - all components of services out of the providers' control
    - and send it on request to customers, potential customers and the Authority

I commit that our organisation **will**:

- communicate the intended date for implementation of all mandatory controls (to the level specified within column D – “CAS(T) additional guidance”) to the HSCN authority
- maintain the plan to achieve the intended level of compliance
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority
- ensure that all additional/amended services shall be delivered to the level of assurance committed to, on the date committed
- keep our key contacts updated, and review them at least annually
- ensure that the ITHC is conducted on the scope of the service prior to the expiry date
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority

## Audited tier

I commit that our organisation **has**:

- ensured that the scope of the services proposed for HSCN compliance meets the definitions laid out in the ‘Scope’ category of Annex A, to the level specified within column D – “CAS(T) additional guidance”
- ensured that the scope of the services proposed for HSCN compliance has been risk assessed according to the ‘Risk Assessment’ category of Annex A, to the level specified within column D – “CAS(T) additional guidance”
- identified where compliance with the technical, security and service management sections of the obligations framework is evidenced within supporting documentation supplied (i.e. High Level Designs, contracts and service management documentation)
- ensured that the ISMS has adopted the mandatory requirements from the scoping, risk assessment and risk treatment categories within Annex A, to the level specified within column D – “CAS(T) additional guidance”
- implemented the Critical controls of Annex A, to the level specified within column D – “CAS(T) additional guidance”
- implemented the Mandatory controls within the ‘Business Continuity Planning’, ‘Configuration management’, ‘Control performance’, ‘Governance’, ‘Incident management’, ‘Operations management’ and ‘Supply chain assurance’ categories of Annex A, to the level specified within column D – “CAS(T) additional guidance”
- created a plan of how all remaining Mandatory controls in Annex A will be implemented (to the level specified within column D – “CAS(T) additional guidance”) prior to the 1st April 2019
- ensured an IT Health Check (ITHC) is conducted by an organisation delivering CHECK, CREST or Tiger security testing services for the scope of service provided as per the government ITHC guidance (https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance)**, incorporating the additional requirements within A.18.2.3 from Annex A and ITHC scoping guidance within Annex B of the HSCN Supplier Compliance Addendum** and renewed prior to the anniversary of compliance
- provided a residual risk statement (or null return) covering:

.

- all unremediated ITHC findings higher than medium
- all components that are critical to the delivery of services that are not assured to the correct level of availability under Chapter Five of the CAS(T) security procedures
- all components of services out of the providers' control
- and send it on request to customers, potential customers and the Authority.

I commit that our organisation **will**:

- communicate the intended date for implementation of all mandatory controls (to the level specified within column D – "CAS(T) additional guidance") to the HSCN authority
- maintain the plan to achieve the intended level of compliance
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority
- ensure that all additional/amended services shall be delivered to the level of assurance committed to, on the date committed
- keep our key contacts updated, and review them at least annually
- ensure that the ITHC is conducted on the scope of the service prior to the expiry date
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority

## Accredited tier

I commit that our organisation **has**:

- ensured that the scope of the services proposed for HSCN compliance meets the definitions laid out in the 'Scope' category of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- ensured that the scope of the services proposed for HSCN compliance has been risk assessed according to the 'Risk Assessment' category of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- identified where compliance with the technical, security and service management sections of the obligations framework is evidenced within supporting documentation supplied (i.e. High Level Designs, contracts and service management documentation)
- obtained a valid CESG Assured Services (Telecommunications) certification from a CAS auditing company
- implemented the Mandatory controls within the 'Business Continuity Planning', 'Configuration management', 'Control performance', 'Governance', 'Incident management', 'Operations management' and 'Supply chain assurance' categories of Annex A, to the level specified within column D – "CAS(T) additional guidance"
- created a plan of how all remaining Mandatory controls in Annex A will be audited (to the level specified within column D – "CAS(T) additional guidance") prior to the 1st April 2019
- ensured an IT Health Check (ITHC) is conducted by an organisation delivering CHECK, CREST or Tiger security testing services for the scope of service provided as per the government ITHC guidance (**https://www.gov.uk/government/publications/ithealthcheckithcsupportingguidance), incorporating the additional requirements within A.18.2.3 from Annex A**

**and ITHC scoping guidance within Annex B of the HSCN Supplier Compliance Addendum** and renewed prior to the anniversary of compliance

- provided a residual risk statement (or null return) covering:
    - all unremediated ITHC findings higher than medium
    - all components that are critical to the delivery of services that are not assured to the correct level of availability under Chapter Five of the CAS(T) security procedures
    - all components of services out of the providers' control
    - and send it on request to customers, potential customers and the Authority

I commit that our organisation **will**:

- communicate the intended date for implementation of all mandatory controls (to the level specified within column D – “CAS(T) additional guidance”) to the HSCN authority
- maintain the plan to audit the controls
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority
- ensure that all additional/amended services shall be delivered to the level of assurance committed to, on the date committed
- keep our key contacts updated, and review them at least annually
- ensure that the ITHC is conducted on the scope of the service prior to the expiry date
- ensure that any changes to the assurance tier of the service shall be notified to the HSCN authority.