Document filename:	**HSCN Obligations Framework – Compliance Addendum**		
Project / Programme	**HSCN**	Project	**HSCN Compliance**
Document Reference			
Project Manager	**Chris Brown**	Status	**Draft**
Owner	**HSCN Compliance Board**	Version	**1.2**
Authors	Paul Evans and Des Ward	Version issue date	**13/07/2017**

HSCN Obligations Framework – Compliance Addendum

Document management

Revision History

Version	Date	Summary of Changes
V0.1	13/06/2016	First draft incorporating the position agreed by Des Ward, Michael Bowyer and Paul Evans
V0.2	30/06/2016	Updated following internal review and review by Innopsis Security Working Group
V0.3	10/07/2016	Updated following internal review and review by Innopsis Security Working Group
V0.4	13/07/2016	Updated following internal review and review by Innopsis Security Working Group
V0.5	30/07/2016	Updated following internal review and review by Innopsis Security Working Group
V0.6	21/10/2016	Updated to NHS Digital template Added compliance process flowchart Added Disaster Recovery Planning as a baseline requirement Issue for review by HSCN Security Sub-board.
V0.7	23/11/2016	Updated with latest Commitment statements
V1.0	10/05/2017	Updated with latest requirements for alignment with BC/DR and Service Management
V1.1	13/06/2017	Updated for re-issue following Service Management and BC/DR requirement alignment
V1.2	13/07/2017	Updated Annex A – now to include Business Continuity control and evidence requirements

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
HSCN Security Sub-Board				

HSCN Service Management

Glossary of Terms

Term / Abbreviation	What it stands for

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. 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.

Contents

1 Introduction

1.1 Status of this paper

This document forms part of the HSCN Supplier Compliance document set. It is approved for issue by the HSCN Compliance Board.

1.2 Purpose of Document

This document sets out requirements for Service Management and Information Assurance that HSCN Suppliers must comply with in order to be able to market and provide HSCN Compliant Services. Together with the HSCN Obligations Framework, the requirements form part of the HSCN Compliance Baseline.

2 Compliance

2.1 Standards

The HSCN Requirements set out in this Compliance Addendum are based on the CAS(T) (CESG Assured Service (Telecommunications)) Security Procedures with additional controls to include aspects of Business Continuity and Disaster Recovery.

Further information on CAS(T) and the Security Procedures can be found at https://www.cesg.gov.uk/articles/policy-and-guidance-documentation-suite-cast.

2.2 Requirements

Annex A sets out the Information Assurance and Service controls set for HSCN.

Controls in Annex A marked as below form the HSCN Minimum Compliance Baseline (MCB). Suppliers must declare compliance with the below

1. Requirements marked as 'critical' in Annex A – these set out the minimum set of controls
2. Requirements marked as 'mandatory' under the following categories in Annex A –
    a. Business continuity planning
    b. Configuration management
    c. Control performance
    d. Incident management
    e. Operations management
    f. Risk assessment
    g. Scope
    h. Supply chain assurance

Suppliers must be compliant with and provide a satisfactory response to each of the controls in the MCB to achieve stage one compliance, then maintain compliance with the MCB at all times whilst delivering HSCN Service.

Further, to ensure a minimum quality of Information Assurance controls are in place, HSCN Suppliers must:

1. Carry out an ITHC scoped in accordance with: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance. (ITHC(s) carried out as part of the CAS(T) certification will suffice as long as the minimum scope of the ITHC is met and the proposed HSCN services are included fully in the ITHC)
2. Provide the results of that ITHC to NHS Digital
3. Agree a remediation plan and statement of residual risk with NHS Digital and implement the remediation plan
4. Provide the statement of residual risk to HSCN consumers (see section below)

2.3 Compliance Scope

The scope of compliance shall be the end-to-end provision of HSCN services. This shall include services provided by sub-contractors and include management / operational systems that support network services

Suppliers must respond to each of the Minimum Control Baseline irrespective of the Assurance level set out in 2.3 below. Suppliers shall also include those services of material subcontractors in responses to the Minimum Control Baseline requirements.

2.4 Scope of ITHC

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

Annex B sets out the minimum scope for the ITHC required for the compliance.

2.5 Assurance

There are three ways in which an HSCN Supplier can demonstrate compliance with the HSCN Minimum Compliance Baseline. In addition to declaring a satisfactory response to each of the controls, each HSCN Supplier must provide assurance to NHS Digital of their conformity with the HSCN Minimum Compliance Baseline for their HSCN services through at least one of the three methods.

These are set out below:

1) **Accredited** - hold and maintain current CAS(T) certification for the services provided, incorporating the HSCN Minimum Compliance baseline controls;
2) **Audited** - hold and maintain current ISO/IEC-27001:2013 certification (for the services provided) for an ISMS that incorporating the HSCN Minimum Compliance baseline controls at the point of becoming an HSCN Supplier and achieve coverage for the remaining CAS(T) requirements marked as 'mandatory' by 1 April 2019;
3) **Asserted** - Self-assert Compliance (for the services provided) with the incorporating the HSCN Minimum Compliance baseline controls at the time of becoming an HSCN Supplier, achieve coverage for the remaining CAS(T) requirements marked as 'mandatory' and achieve either 'accredited' or 'audited' status by 1 April 2019.

2.6 Residual Risk Statement – Assurance to Consumers

In each case, HSCN Suppliers must provide a statement of residual risk available to consumers (both current and future). Residual risks that must be included together with dates for resolution are:

- All un-remediated ITHC findings higher than medium;
- All components that are 'critical' (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);
- 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).

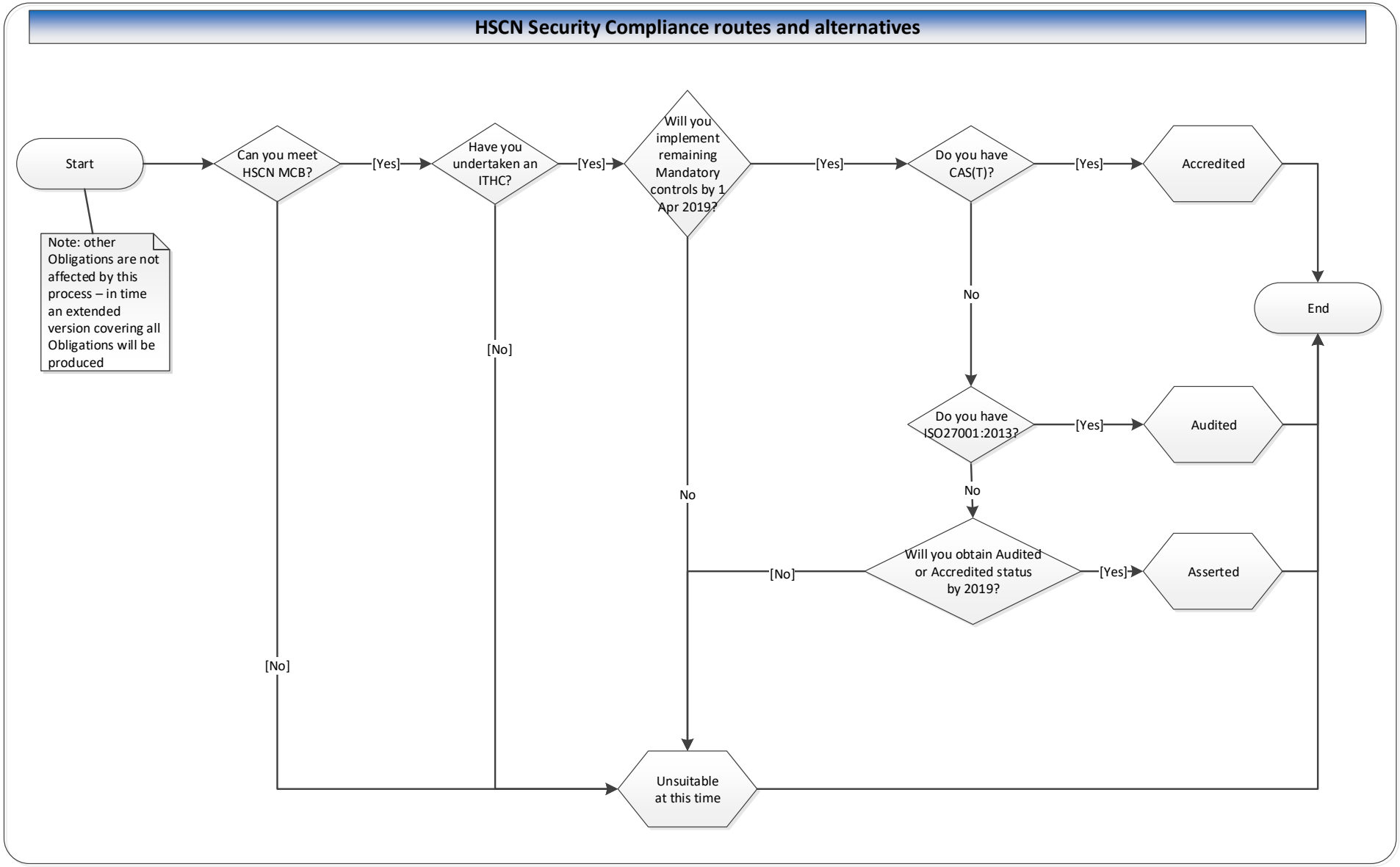

Figure 1 - Compliance Process Flowchart

Annex A

This section sets out the minimum CAS(T) controls for HSCN Supplier compliance. This control set forms part of the HSCN Minimum Compliance Baseline.

Compliance Addendum ANNEX A_

Annex B - ITHC scoping

The purpose of the ITHC as part of the HSCN Compliance process is to provide evidence to NHS Digital (and to your organisation) that across the service proposed for HSCN the risk of unavailability, loss or other compromise of the service through unauthorised access or change are understood by senior management in your organisation and adequately controlled to an acceptable level.

One of the most important aspects in ensuring that an ITHC is comprehensively identifying risks and adequately controlling them is getting the breadth and depth of the scope of the ITHC correct.

The scope of ITHC for HSCN should be based on PSN guidance for ITHC: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance

However, this is generic guidance intended for all aspects of PSN compliance, not solely network infrastructure.

For HSCN, perhaps the most important aspect is that the NHS Digital are assured that the breadth and depth of the ITHC covers the full scope of the services which you proposed to provide as the HSCN service or services, both in breadth and depth of the ITHC.

This includes not just the core network devices (for example, routers, switches, firewall devices, including premise or customer premise equipment where these are supplied and managed by you as part of the HSCN service), but also management infrastructure, such as management networks and services (including email and other information stores) which support the core network service, and end-user devices that are used in administrating and configuring it. The scope of the HSCN service proposed is as stated in your High-Level Design (HLD) submitted as part of your CN-SP submission at stage 1 of the HSCN Compliance application. For subsequent ITHCs, it is important that the scope of the ITHC is updated according to changes to the design of your service or services.

Where the HSCN service is made up of one or more existing services, it is important that the scope covers all variants and segments, and their interconnections. This may be the case where your service is made up of more than one core networks, perhaps through acquisition or regional variation. For stage 1 compliance, NHS Digital recognises that the HSCN service may not have been implemented yet. In this case, it is acceptable to provide an ITHC for an existing service which uses the same or similar components, topology and management layers as the proposed ITHC. However, for all subsequent ITHCs, the ITHC must be carried out on the actual HSCN service. This should include where possible, Customer Premise or Premise Equipment where this equipment is provided and managed as part of your service to the HSCN Consumer.

It is also important to provide representative assurance that the ITHC covers sufficient devices within each segment of the service and device type. For example, a service that comprises 1000 end user management devices, a realistic and representative test would include around 10% of those end user devices. Similarly, 10% of network devices provide a representative number of devices in the service or service segment.

The ITHC should also include authenticated and unauthenticated vulnerability scanning on internal and where appropriate external facing devices and services. Similarly, the ITHC should include an assessment of the configuration of devices that make up the service.

Supporting Systems – ITHC

A good quality ITHC will include in its scope services that support and detail the delivery of the HSCN Service. This includes services that hold information such as customer lists, configuration diagrams, device lists, support and operation personnel details, ITHC scoping and remediation reports. Clearly, this information is of value to a potential attacker of the service and so should be secured accordingly; its loss or compromise could lead to an increased risk to the availability of the service. We provide the following guidance for prospective suppliers about the use of email and cloud services as the repository to hold this information.

Email systems – principles for complia