HSCN Compliance – Interim Network and Telco security regime overview
Publish date: 18th October 2019

In response to the announcement by the National Cyber Security Centre in September 2019 that the CAS(T) regime will be ceased there is a requirement for HSCN Compliance to set a interim network and telco security regime whilst we await the implementation of a replacement regime which is likely to be implemented by the end of 2020.

Therefore, this interim regime is expected to be in place until c. 31st December 2020.

The NCSC will not be revoking existing CAS(T) certificates as they will continue to be recognised as demonstrating a high level of cyber security obtained by industry. However, there will be insufficient time for any new evaluations or recertification processes that have yet to be started to be completed prior to the scheme closure – therefore the interim HSCN regime will be adopted with immediate effect.

The Interim regime - requirements

For those suppliers who already hold full CAS(T) accreditation (with a certificate that is in-date) there is no change to our requirement – however please refer to points (2) and (3) below as these requirements will continue to stand as additional attributes to CAS(T) – for all suppliers irrespective of their CAS(T) position.

For those suppliers who either currently hold a CAS(T) certificate which is about to expire, or who are currently in the HSCN Compliance application process, the obligation is as follows:

As per the existing HSCN Compliance requirement all suppliers must:

1. Hold an ISO27001:2013 certificate based on an audit of their network connectivity service Information Security Management System (ISMS) by a UKAS affiliated auditor. The scope of the audit must be agreed with HSCN Compliance prior to audit.
   As part of this pre audit scope NHS Digital and the supplier must come to an agreement that statement of applicability fully corresponds to the attributes of the service that needs to be audited and it must meet the requirements of the HSCN Minimum Compliance Baseline (MCB)*
2. Provide a yearly IT Health Check. This needs to include the scope that HSCN will review prior to audit, outcomes report that we can correlate back to the scope and associated remediation action plan. This documentation will be audited by HSCN Compliance (including the NHS Digital Data Security Centre).
3. Provide a detailed response to the HSCN Business Continuity and Disaster Recovery (BC/DR) controls annex - this documentation will be audited by HSCN Compliance (including the NHS Digital Business Continuity cell).

*The audit is to be carried out on an ISMS that includes all the requirements of the MCB, and these are part of any audit terms of reference (ToR) that the UKAS auditor uses when auditing the ISMS clauses or HSCN Compliance Addendum Annex A controls.

These requirements are in line with the existing HSCN AUDITED compliance tier (agreed by all CPs involved in the CN-SP compliance consultation and deeds of undertaking) which is outlined in the HSCN Compliance Operating Model (found here: https://digital.nhs.uk/services/health-and-social-care-network/hscn-suppliers).

The audited statement is still intact and reads:

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.

If you have any questions or queries on this statement, please contact compliance.hscn@nhs.net.