Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Health Competent Authority
Ùghdarras Iomchaidh Slàinte na h-Alba

NHS SCOTLAND

Network & Information Systems Regulations 2018

2023 Audit Programme

Health Board Guidance

Contact email:
HealthCA@gov.scot

Website:
www.healthca.scot

Version:1.0 Final

Contents

1. Introduction

This paper provides guidance on the procedures to be followed by all NHS Scotland Health Boards to fulfil their responsibilities under the 2023 Audit Programme. Adoption of these procedures will give Health Boards the best possible opportunity to demonstrate progress against the level of compliance with the Network & Information Systems (NIS) Regulations.

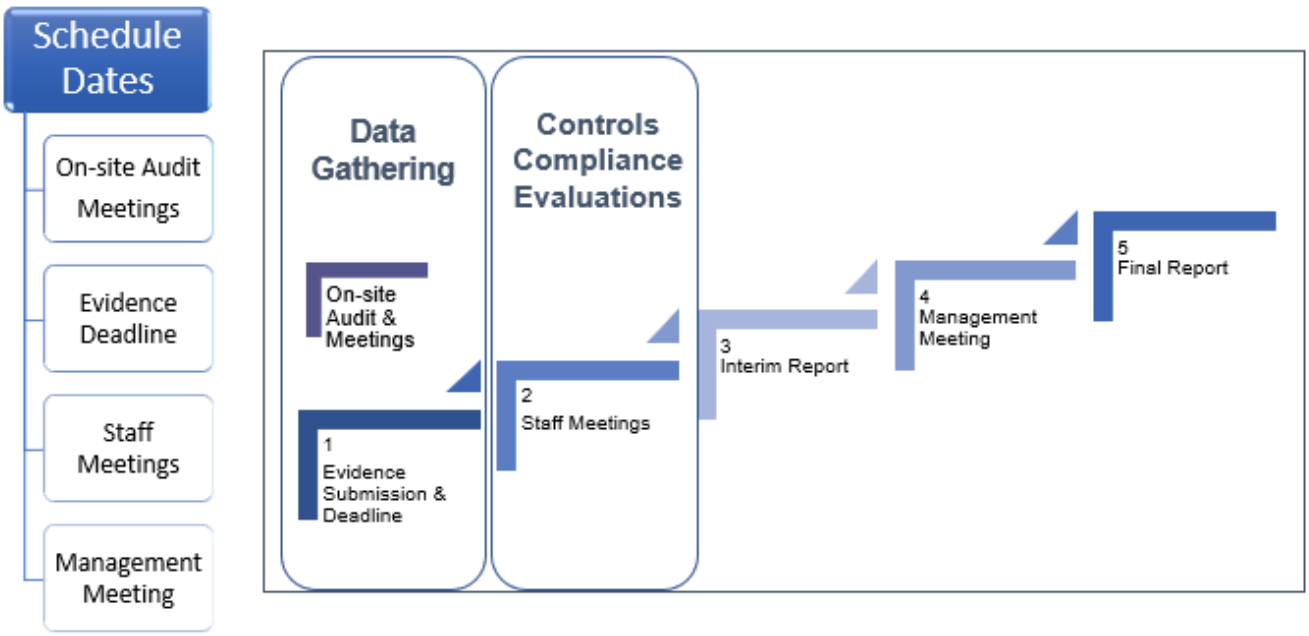
Failure to follow this guidance may result in reject of the submission.

2. Programme Sequence

2.1 Structure

There are several elements to the Audit Programme; guidance for each stage to help Health Boards through the process is detailed below:

- Heath Board Audit date schedule issued to all NHS Scotland Health Boards
- On-site Audit - This will now be carried out separately with observations included in the Interim Report
- Evidence Submission - this may be uploaded anytime but must be completed by the Deadline Date
- Staff Meetings
- Interim Report
- Management Meeting
- Final Report



2.2 Health Board Roles and Responsibilities

To prepare for audits and make arrangements for on-site assessments including:

- Designate a key person contact for the audit (NIS Audit Lead)
- Assign Deputy person should NIS Lead be unavailable
- **EXACTLY** following the procedures as described in this Guidance document

- Completion of the evidence template as instructed
- Issuing/uploading of evidence documentation to the Objective Connect workspace for your Health Board **BEFORE** the Deadline Date
- Arranging for personnel to be available at On-site Audit Meetings, Staff Meetings, Management Meeting as scheduled.
- Arranging for on-site tour of facilities with the auditor

3. On-site Audit

The On-site Audit will take place in one day with dates and timing to be agreed. It shall focus on aspects of the control categories most efficiently addressed by physical examination. As such this inspection complements, but is not a substitute for, the formal documentary evidence to be submitted as part of the audit programme.

The NIS Leads must ensure that staff are available on the planned dates, schedule all calendar appointments (auditor/staff) and on-site tour of facilities.

3.1 Aspects to be addressed

To assist Health Boards in planning, the following aspects will be examined during the On-site Audit. In addition, there will also be the opportunity for Health Boards to provide to the auditor demonstrations or showcase other developments which they feel they wish to highlight.

Facilities/estates

These areas will be examined in a tour around Health Board premises.

- Building entry access control
- Loading / delivery bay access control
- Power resilience – UPS and generator provision
- Connectivity resilience
- Computer/Server/data centre access control
- Internal sensitive areas and associated access control

Technical

- Third party network access control procedures
- Privilege access management procedures/systems

Demonstrations

- This is a free-scope area for any security-related technical or software demonstrations or presentations Health Boards wish to make.

3.2 Attendance

The auditor will wish to meet the following personnel as a minimum and will have individual staff meetings as required:

- Information Security Officer (ISO) or equivalent
- Facilities / Estates manager
- Head of IT/Networks for technical questions

At these site inspections the auditor will meet with any other members of staff the Health Board wishes to present including those listed in the Staff Meetings.

3.3 Supporting Evidence

The outcomes of the On-site Audit shall be incorporated into the Health Board audit assessment; however, it is essential that the board **also** submits documentary and photographic evidence in these areas as this shall form an integral part of the permanent record for the board report.

4. Evidence Submission

4.1 Evidence Template

To facilitate Health Boards in making their evidence submissions an Evidence Template has been produced. This was issued to the NIS Audit Leads at the Health Boards on 16th February 2023 with the Evidence Submission Deadline Dates sent on the 13th March 2023. Figure 4.1 shows an extract. Auditors will review the evidence base submitted against each control before the Staff Meetings.

This template MUST be adopted for all submissions.

The template allows specific evidence to be identified against specific controls of the Revised Public Sector Cyber Resilience Framework (PSCRF) making clear which controls boards wish the evidence to be considered against, thereby ensuring no evidence may be overlooked or missed and highlighting gaps in the Health Board evidence base.

Evidence submissions that do not follow this template will be rejected.

Figure 4.1 Extract from Evidence Template

1. ORGANISATIONAL GOVERNANCE Appropriate organisational structures, policies, and are processes in place to understand, assess and systematically manage security risks to the organisation's network and information systems.			
1.1 Governance Framework: **There is effective organisational security management led at board level and articulated clearly in corresponding policies.**			
TIER	CONTROLS	EVIDENCE SUBMITTED	EXPLANATION/COMMENTARY
TIER 1	1. There is a Board/Senior Management-level commitment to manage the risks arising from the cyber threat.	*Specific FILE NAME(S) which may differ from the document title.*	*Specific pages/paragraphs cited and/or explanation as to why the evidence fulfils the control.*
	2. There are appropriate data protection and information security policies and processes in place to direct the organisation's overall approach to cyber security.		
	3. There are clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services.		

4.2 Cross-Referencing

To ease the burden on Health Boards, the document submission is no longer required to have control cross-references in the file titles/names. Moreover, submissions may be bulk uploaded in a single batch to Objective Connect without the need for segregation into category folders.

However, from experience the Audit Supplier has noted that the file title may differ from the actual document name. It is essential therefore that heath boards ensure the FILE TITLE/NAME submitted **EXACTLY MATCHES** the file title/name cited in the Evidence Template.

Failure to provide the correct FILE TITLE/NAME for documentary evidence may mean this evidence cannot be identified within the documents submitted by the board and therefore will not be assessed.

4.3 Fixed Submission Deadline Date

As noted above the deadline date by which all evidence should be submitted by uploading to the Scottish Health Competent Authority (SHCA) Objective Connect site is included in the programme schedule. **THIS DATE IS FIXED** to ensure the audit programme for all NHS Scotland Health Boards delivers to the schedule.

4.4 What is Evidence?

To demonstrate compliance with control categories a documented evidence base must be developed. The precise nature of evidence varies with individual control requirements; however, boards should adopt the following approach of **Policy-Procedure-Implementation** in developing the evidence base.

- **Policy**
  What is the organisation's policy and approach to this control area?
  This is typically defined in a formal document which may, for example, be a policy, strategy, or corporate plan. Note that software configurations (often termed policies in technical terms) are not the formal policy referred to here but may offer evidence of the implementation of a security policy.

- **Procedure**
  How is this policy implemented?
  What procedures are adopted to fulfil the organisation's defined approach?
  Methods or procedures should be defined in a formal document which could be supported by an operation To-Do list or specification build guide.

- **Implementation**
  Policies and procedures are only effective if they are implemented. The final step is therefore to demonstrate that the defined procedures are actively implemented, for example by configuration screenshots; software dashboards; test and vulnerability reports with prioritised actions; system logs, whichever is most appropriate to the control. Health Boards should clearly state in the evidence template why they believe a piece of evidence supports achievement of the respective control.

4.5 Typical Policy Documents Areas

The content and structure of policy documents varies according to organisational need and style. However, development of the policies shown in Table 4.2 would fulfil several of the framework control specifications. These are specific policy subject areas; Health Boards may wish to combine several of these topics into a document for simplicity.

Table 4.2 Policy Subject Areas

Acceptable Use	Information / Data Management
Access Control	Information Security
Account Management	Media Management (including mobile devices)
Anti-Malware, Vulnerability Management	Password Management
Asset Management (Hardware)	Patch Management
Backup	Penetration Test Protocol
Business Continuity	Physical Security
Clear Desk, Clear Screen Policy	Remote Working
Data Retention And Destruction Policy	Risk Appetite
Disaster Recovery	Risk Management
Encryption / Cryptography	Risk Register
Firewall Management	Secure Build (Hardware)
Hardware Asset Register	Software Asset Register
Incident Management & Response	Software Development
Information Asset Register	Software Management
	Supplier Management

5. Staff Meetings

As mentioned previously in this guidance, key person meetings are also part of the On-site Audit.

These additional individual Staff Meetings have been incorporated into the programme to complement the meetings and discussions held during the On-site Audit.

These meetings will take place by Microsoft Teams and will be held on the date allocated to the Health Board in the schedule. The NIS Leads must ensure that staff are available on the planned dates and arrange calendar appointments with the auditor/staff.

Related further evidence may be submitted immediately after these meetings and ahead of the interim report.

5.1 Attendance

Staff members with the following designations and responsibilities would offer important insights and contributions to the audit outcomes and are suggested attendees.
It is envisaged that each individual meeting will last no longer than one hour unless there are exceptional circumstances.

Essential

- NIS Audit Lead
- Information Security Officer (ISO)
- Senior Information Risk Officer (SIRO)
- Executive Director responsible at board level for information/cyber security

Possible

- HR/OD person responsible for staff induction and training
- Facilities/Estate manager

5.2 Agenda

As the evidence is evaluated the Audit Supplier will compile an agenda to discuss with the board during these individual meetings. This may include weak areas of evidence, areas where evidence was submitted but was not relevant and anything else the auditors identify that they feel requires, or could benefit from, further discussion with staff.

6. Interim Report

Subsequent to the Staff Meeting, the Audit Supplier will issue an Interim Report to the SHCA and Health Boards NIS Audit Leads, which shall provide an assessment of the compliance of the board against each of the controls based upon the evidence submitted and the outcome of the On-site Audit with observations arising from the Staff Meetings. Each control will be assessed against the criteria shown in Table 6.1 and the results presented in the report.

The NIS Audit Leads must share the interim report with the appropriate senior staff in preparation for the Management Meeting.

Table 6.1: Control compliance assessment criteria

Control Assessment	Detail
Achieved	Requirement full addressed, comprehensive policies/procedures with evidence of implementation.
Partially Achieved	Requirement partially addressed, inconsistent policies/procedures; absent or inconclusive evidence of implementation.
Not Achieved	Requirement not addressed, inadequate policies/procedures.

7. Management Meeting

This meeting will offer the opportunity to address the NIS compliance performance outcomes with **senior staff** of the Health Board. It is envisaged that each meeting will last no longer than two hours unless there are exceptional circumstances. Note this is a discussion meeting to discuss the findings of the audit programme. It is NOT opportunity for additional evidence submissions to be made.

The NIS Leads must ensure that staff are available on the planned dates and arrange calendar appointments with the auditor/staff/SHCA.

7.1 Attendance

Health Boards are free to determine which staff they wish to attend this meeting, though it is intended for members of the executive team and board members.

It is suggested that attendees should be selected to reflect the areas of responsibility regarding NIS compliance, risk, and cyber security. The following are examples drawn from experience of staff members who have found such meetings beneficials for their understanding and insight on board performance. Note that not all are required or expected to attend, these are merely suggestions.

- Chief Executive
- Board Chair
- Board members, including non-executives
- SIRO
- Audit and Risk Committee Chair
- Members of the Senior Leadership/Executive Team
- Director of Corporate Services / Chief Operations Officer

The SHCA will aim to attend all Management Meetings as an observing attendee(s).

7.2 Agenda

The agenda items for discussion will vary with individual boards; however, the following items are envisaged as typical topics for discussion throughout the Management Meetings:

- Welcome and Introductions
- Overview of board performance
- Areas for Development
- Aspects of Good Practice
- Questions from Executive Management
- AoB

8. Final Report

Subsequent to the Management Meeting, the Audit Supplier will issue a Final Report to the SHCA. The report shall provide an assessment of the compliance of the board against each of the controls based upon the evidence submitted and the outcome of the on-site audit with observations arising from the Staff Meeting and Management Meeting.

SHCA will issue the Final Report to the Health Boards.