Network & Information Systems Regulations 2018

2024-25 Progress Review

Health Board Guidance

Contents

Contents 2

1. Introduction 3

2. Review Programme 3

Structure 3
Roles and Responsibilities 3
SHCA 3
Health Boards 4
Cyber Security Scotland 4

3. Evidence Submission 4

Evidence Template 4
Cross-Referencing 5
Fixed Submission Deadline Date 5
What is Evidence? 5
Policy 5
Procedure 6
Implementation 6

4. Staff Meeting 6

Attendance 6
Agenda 6

5. Interim Report 6

6. Management Meeting 7

Attendance 7
Agenda 7

7. Final Report 8

1. Introduction

This paper provides guidance on the procedures to be followed by health boards to fulfil their responsibilities under the 2024-25 NIS Progress Review Programme. Adoption of these procedures will give health boards the best possible opportunity to demonstrate progress against the level of compliance with the NIS regulations.

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

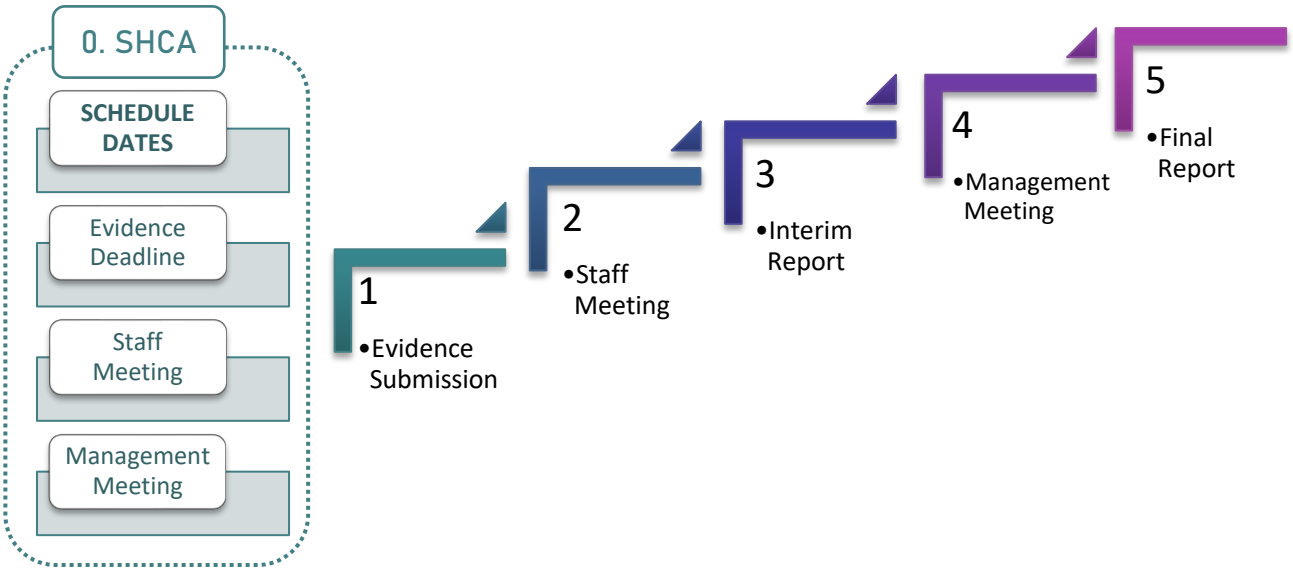
2. Review Programme

This is a **Progress Review** NOT a full audit. Health boards are therefore NOT required to submit evidence to every control; evidence submitted should only be on the controls that are "Not Achieved" or "Partially Achieved."

Structure

There are several elements to the Review Programme; guidance for each stage to help health boards through the process is detailed below:

0. Heath Board Review timetable – issued by the Scottish Health Competent Authority (SHCA) to all NHS Scotland health boards and published on the SHCA website.
1. Evidence Submission - this may be uploaded anytime but must be completed by the Deadline
2. Staff Meeting
3. Interim Report – issued to health boards and SHCA by Cyber Security Scotland
4. Management Meeting
5. Final Report – issued to health board by SHCA



Roles and Responsibilities

SHCA
To liaise, coordinate and agree with health boards the following items:

- Pre-review preparations including issuing of Programme Schedule and Guidance to health boards
- NIS Lead (key person contact)
- Secondary or depute person should NIS Lead be unavailable

- Follow-up with health boards to enforce evidence submission deadline
- Issue of Final Report to NIS Lead

Health Boards
To make arrangements for the progress review including:

- Delegate the NIS Lead as the designated contact for the NIS review
- Assign Deputy person should NIS Lead be unavailable
- Exactly following the procedures as described in the 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 for the Staff Meeting and Management Meeting as scheduled

Cyber Security Scotland
To deliver the reviews in accordance with the tender requirements:

- Review and assess the evidence submitted against each control and provide details of areas they wish to focus on in advance of the staff meetings
- Attend Staff Meeting
- Issue the Interim Report
- Attend a Management Meeting
- Issue the Final Report

3. Evidence Submission

Evidence Template

To facilitate boards in making their evidence submissions an Evidence Template has been produced. This will be issued to health boards with this Guidance document. Figure 3.1 shows an extract. Auditors will review the evidence base submitted against each control before the Staff Meeting.

This template MUST be adopted for all submissions.

The template allows specific evidence to be identified against specific controls making clear which controls boards wish the evidence to be considered against. This is to ensure no evidence is overlooked or missed while highlighting gaps in the health board evidence base.

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

Note: This is a **Progress Review**; Health boards are therefore NOT required to submit evidence to all controls; the focus for the evidence submitted should be on the controls that are "Not Achieved" or "Partially Achieved."

Figure 3.1: Extract from Evidence Template

1. ORGANISATIONAL GOVERNANCE **Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the organisation's network and information systems.**			
TIER	CONTROLS	EVIDENCE SUBMITTED	EXPLANATION/COMMENTARY
1.1 Governance Framework: **There is effective organisational security management led at board level and articulated clearly in corresponding policies.**			
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.		

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. Moreover, submissions may be bulk uploaded in a single batch to Objective Connect without the need for segregation into category folders.

However, from experience we have noted that the file title may differ from the actual document name. It is essential therefore that heath boards ensure the FILE NAME(S) submitted **EXACTLY MATCHES** the file name(s) cited in the Evidence Template.

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

FIXED SUBMISSION DEADLINE DATE

As noted above the deadline date by which all evidence should be submitted by uploading to the SHCA Objective Connect site is included in the review programme schedule issued by SHCA. To ensure the review programme delivers to the 2024-25 schedule it is essential that this fixed date is met

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. Staff Meeting

The Staff Meeting is designed to assist health boards to optimise their compliance assessment. It provides the opportunity for the auditors to discuss aspects of the submission for clarification and to identify gaps in the evidence provided.

ATTENDANCE

The key person required for this meeting is the NIS Lead.

Prior to the meeting Cyber Security Scotland shall issue a **Notification Letter** to the NIS Lead on the areas for discussion. The NIS Lead shall then share this with appropriate senior level colleagues (inc SIRO) within their health board to agree the attendance requirement of any additional staff members specific to those discussion points.

AGENDA

The specific items for discussion will vary with individual boards; however, the meeting is envisaged to follow the following structure:

1. Welcome and Introductions as required
2. Initial feedback from Cyber Security Scotland on the Progress Review outcomes
3. Discussion on clarifications and evidence gaps as identified in the Notification Letter
4. Questions from staff
5. Next Steps

5. Interim Report

Subsequent to the Staff Meeting, Cyber Security Scotland will issue an Interim Report which shall provide an assessment of the compliance of the board against each of the controls based upon the evidence submitted with observations arising from the Staff Meeting. Controls will be assessed against the criteria shown in Table 5.1 and the results presented in the report.

TABLE 5.1: Control compliance assessment criteria.

Control Assessment	Detail
Achieved	Requirement fully 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; no evidence submitted.
Not Applicable	Control does not apply.

The NIS Lead shall then securely share the Interim Report (Official-Sensitive handling) with appropriate senior level colleagues within their health board prior to the Management Meeting.

6. Management Meeting

This meeting will offer the opportunity for auditors to explain to senior staff and board members the NIS compliance performance outcomes of the health board. It is envisaged that each meeting will last no longer than one hour unless there are exceptional circumstances.

Note this is a meeting to explain the findings of the Progress Review. It is NOT opportunity for additional evidence submissions to be made.

ATTENDANCE

Attendance is at the discretion of health boards though as noted, it is primarily intended for members of the executive team and board members. For example, attendees could include

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

Staff from the SHCA may attend the meetings as observers.

AGENDA

The agenda items will vary with individual boards; however, the following structure of the meeting is envisaged:

- Welcome and Introductions
- Overview of the board performance highlighting strengths and areas for development.
- Questions from Executive Management
- Next Steps

It is recognised that some outcomes from the progress report may be disappointing.

Health board staff are therefore reminded that the auditors are following the agreed process. Abusive, threatening and harassment behaviors towards the auditors, or any other party, will not be tolerated.

7. Final Report

Subsequent to the Management Meeting, Cyber Security Scotland will issue a Final Report to the SHCA. The report shall provide an assessment of the compliance of the board based upon the evidence submitted with observations from the Staff Meeting and Management Meeting.

SHCA will issue the Final Report to health boards.