Network & Information Systems Regulations 2018

2022 Review Programme

Health Board Guidance

Revision History:
v. 1.4
20 Jan 2022

Version Control

Document Creation

Author:	Dr Keith Nicholson
Title:	Information & Cyber Security Consultant – Cyber Security Scotland
Contact details:	**email:** knicholson@cybersecurity.scot | **mobile:** 07899 062 965
Date:	11 Jan 2022

Revision History

Version	Date	Changes Summary
1.0	11 Jan 2022	Release document.
1.1	18 Jan 2022	Revised following SHCA review.
1.2	18 Jan 2022	Typo corrected.
1.3	19 Jan 2022	Table format error corrected.
1.4	20 Jan 2022	Typos corrected.

Release Authorisation

Name	Title	Date	Version
Keith Nicholson	Cyber Security Consultant	20 Jan 2022	1.4
George Irvine	Scottish Health Competent Authority, Digital Health & Care, Scottish Government	20 Jan 2022	1.4
Cara Archibald	Scottish Health Competent Authority, Digital Health & Care, Scottish Government	20 Jan 2022	1.4

Distribution

Name	Organisation	Date	Version
Cara Archibald	Scottish Health Competent Authority, Digital Health & Care, Scottish Government	20 Jan 2022	1.4
George Irvine	Scottish Health Competent Authority, Digital Health & Care, Scottish Government	20 Jan 2022	1.4
NIS Leads	All NHS Scotland Health Boards	20 Jan 2022	1.4

Contents

1. Introduction

Following the Final Audit and (with the exception of PHS) a 2021 Progress Review and in accordance with the three-year audit review cycle, a further **Progress Review** shall be undertaken in 2022. The programme schedule is presented in Annex 1.

This paper provides guidance on the procedures to be followed. Adoption of these procedures will give health boards the best possible opportunity to demonstrate progress against the level of compliance with the NIS regulations.

Key Points

- Given this is the second progress review, the only meeting requirement is with the NIS Lead. Others are welcome to attend.
- Unless exceptional circumstances prevail, it is not anticipated any meeting will be longer than four hours with two being more typical if the evidence is well structured and clearly presented.
- The evidence and reporting requirements detailed in Section 2 are consistent and no different from those required for the 2021 review and should therefore be familiar to health boards.
- All the Control Requirements are in-scope for the audit and review programme, regardless of any internal security frameworks boards may have adopted.

2021 Lessons for Consideration

The following points are drawn from examples from the 2021 Review; these are highlighted to encourage boards to adopt good practice to ensure they are recognised for their achievements over the past year.

1. Evidence Base

Health boards that were most successful in making progress from 2020 presented an evidence base in a clear manner with cross-referencing to the recommendations and control requirements. The table shown in Section 2 offers a clear presentation of evidence for the auditors to consider against specific recommendations or controls. Internal spreadsheet documents that require extensive horizontal scrolling do not offer the best clarity of presentation and should be avoided. Note that evidence previously submitted has been deleted and should not therefore be cited without resubmission.

2. Include Controls Evidence

Several boards failed to follow the 2021 guidance and only provided evidence against the recommendations omitting reference to the control requirements. These boards typically under-performed in the compliance analysis, emphasising the importance of addressing controls directly with specific cross-referenced evidence.

3. Poor Cross Referencing

Uploading a series of documents under a Controls Category without refence to a specific control is not an acceptable approach. It is the health board's responsibility to ensure evidence is presented clearly. Auditors cannot make assumptions as to which control or recommendation the documentation is supposed to evidence, as such boards that adopt such an approach risk the evidence being overlooked.

4. Change & Incident Reports

The Change Report, specified below, provides a useful summary of the challenges boards have faced and equally the progress achieved. Some boards failed to submit a Change Report or an Incident Report; such omissions do not reflect well on the board.

5. Late evidence submission

Ideally auditors will review the evidence base submitted before staff discussions; in several instances documentation was submitted too late for this to occur. While resource constraints are recognised, boards should realise that this does not reflect well on the board internal organisation or even commitment to the legislation.

2. Review Procedure

Process

The Review shall focus on relevant changes to the organisation since the 2021 Review. It shall consider two areas of evidence or Key Performance Indicators:

Recommendations: Progress against the management responses and actions to the prioritised recommendations.

Controls: A re-evaluation of the "Partially Achieved" and "Not Achieved" controls and progress on completion of these towards the "Achieved" status.

On the basis of the above the 2022 Review Report will revise the Overall and Control Compliance Analysis and describe a progress Trend Analysis against the controls compliance ratings.

Procedure

1. The NIS Lead to submit a report to detail significant changes since the 2021 Progress Review Report (as detailed below) and evidence of progress precisely cross-referenced to specific control requirements or recommendations.
2. A meeting between the auditor and the NIS Lead to go through the controls and recommendations to discuss progress as noted above.
3. A 2022 Review Report will be produced with revised compliance and progress analysis.

Health Board Actions

Before the Review

1. CONSIDER the following:
   a) **Recommendations:** Review the recommendations previously made and how the progress achieved in addressing these could be evidenced.

   b) **Controls:** Review the "Partially Achieved" and "Not Achieved" controls and how the progress achieved in addressing these could be evidenced.

2. SUBMIT summary documents at least THREE weeks before the review date with details on the following where relevant:
   a) **Incident Report:** Identify any reportable incidents since the audit and measures taken to mitigate any reoccurrence.

   b) **Change Report:** A brief summary of any significant changes in the health board since the audit:
      i. System Changes: Identify any changes to the network, software, hardware, service delivery and associated security implications.
      ii. People Changes: For example to organisation governance, reporting structures, responsibilities, new staff with the implications for NIS compliance.
      iii. Policy Changes: New policies/update to existing previously submitted; including an updated risk register.
      iv. Supplier changes: New service suppliers with details on the security assessments made.

   c) **Evidence Base Summary:** New documentary, screenshot, photographic or video evidence to demonstrate progress since the audit against the Recommendations and Controls. Note that this evidence must be precisely cross-referenced to the relevant recommendation or control for consideration using the response template shown below.

   d) **Action Plan:** To demonstrate the progress that has been achieved and the actions planned with owners and dates to fulfil the recommendations and control requirements.

3. **CONSIDER** whether any additional staff are required to support the NIS Lead to provide or discuss elements of the recommendations and controls evidence base.
4. **AGREE** a schedule with the auditor within the allocated day for the review process and any additional staff to join the discussion.
   Note: additional staff are not a requirement, this is merely offered an option for the NIS Lead.

Review Meeting

The auditor shall discuss with the NIS Lead the progress and developments made on the recommendations and controls since the 2021 Review. These meetings shall typically be undertaken using Teams as before. The intention is to identify and recognise areas of progress. Additional areas of good practice that emerge from the discussions will also be highlighted and recorded.

EVIDENCE BASE SUMMARY TEMPLATE

Prior to the commencement of the Review please complete the following template and submit together with the documentary or visual evidence at least THREE weeks prior to the scheduled date shown in Annex 1.

RECOMMENDATIONS		
Reference Number	Progress Narrative	Supporting evidence submitted.

CONTROLS		
Sub-Category & Control Reference Number (Basic/ Target/Advanced then number)	Progress Narrative	Supporting evidence submitted.

Annex 1: Programme Schedule

		Monday	Tuesday	Wednesday	Thursday	Friday	Sat	Sun	Wk
		27	28	29	30	31	1 New Year's	2	52
Jan		3 Substitute day	4	5	6	7	8	9	1
	2021	10	11	12	13	14	15	16	2
	ANNUAL	17	18	19	20	21	22	23	3
	REPORT	24	25	26	27	28	29	30	4
		31	1	2	3	4	5	6	5
Feb		7	8	9	10	11	12	13	6
		14	15	16	17	18	19	20	7
		21	22	23	24	25	26	27	8
		28	1	2	3	4	5	6	9
Mar		7	8	9	10	11	12	13	10
		14	15	16	17	18	19	20	11
		21	22 FIFE	23 NSS	24	25	26	27	12
		28	29	30	31	1	2	3	13
Apr		4	5	6	7	8	9	10	14
		11	12	13	14	15 Good Friday	16	17	15
		18 Easter Monday	19	20	21	22	23	24	16
		25	26 HIGHLAND	27 SAS	28	29	30	1	17
May		2 Early May B. H.	3	4	5	6	7	8	18
		9	10	11	12	13	14	15	19
		16	17 W. ISLES	18	19	20	21	22	20
		23	24	25	26	27	28	29	21
		30	31 GRAMPIAN	1	2 Spring B. Hol.	3 Platinum Jub.	4	5	22
Jun		6	7 A&A	8 SHETLAND	9	10	11	12	23
		13	14	15	16	17	18	19	24
		20	21	22	23	24	25	26	25
		27	28	29	30	1	2	3	26
Jul		4	5	6	7	8	9	10	27
		11	12 FORTH	13 LOTHIAN	14	15	16	17	28
		18	19	20	21	22	23	24	29
		25	26	27 PHS	28	29	30	31	30
Aug		1	2 D&G	3	4	5	6	7	31
		8	9 TAYSIDE	10 NHS24	11	12	13	14	32
		15	16	17	18	19	20	21	33
		22	23 GG&C	24 BORDERS	25	26	27	28	34
		29 August B. Hol.	30	31	1	2	3	4	35
Sep		5	6	7	8	9	10	11	36
		12	13	14	15	16	17	18	37
		19	20	21	22	23	24	25	38
		26	27	28	29	30	1	2	39
Oct		3	4 LANARK	5 STATE	6	7	8	9	40
		10	11	12	13	14	15	16	41
		17	18	19	20	21	22	23	42
		24	25 ORKNEY	26 GOLDEN JUBILEE	27	28	29	30	43
		31	1	2	3	4	5	6	44
Nov		7	8	9	10	11	12	13	45
		14	15 HIS	16 NES	17	18	19	20	46
		21	22	23	24	25	26	27	47
	2022	28	29	30	1	2	3	4	48
Dec	ANNUAL	5	6	7	8	9	10	11	49
	REPORT	12	13	14	15	16	17	18	50
		19	20	21	22	23	24	25 Christmas	51
		26 Boxing Day	27 Substitute day	28	29	30	31	1 New Year's	52