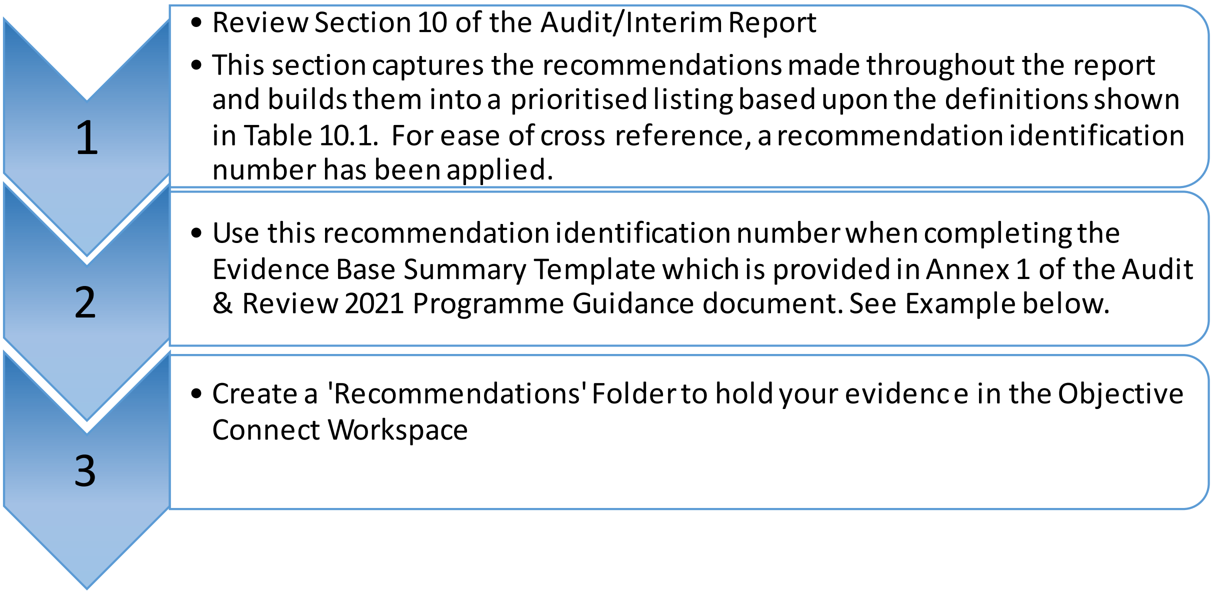
Technical Guidance Note:
Completing the Audit & Review 2021 Programme Evidence Base Summary Template

To ensure your compliance progress is properly evidenced for consideration, Boards are instructed to follow the published audit/review schedule and follow the latest guidance in preparing the evidence for submission.
https://www.healthca.scot/nisr-audit-review-2021-programme-guidance-v-1-4/

Recommendations Procedure



1
- Review Section 10 of the Audit/Interim Report
- This section captures the recommendations made throughout the report and builds them into a prioritised listing based upon the definitions shown in Table 10.1. For ease of cross reference, a recommendation identification number has been applied.

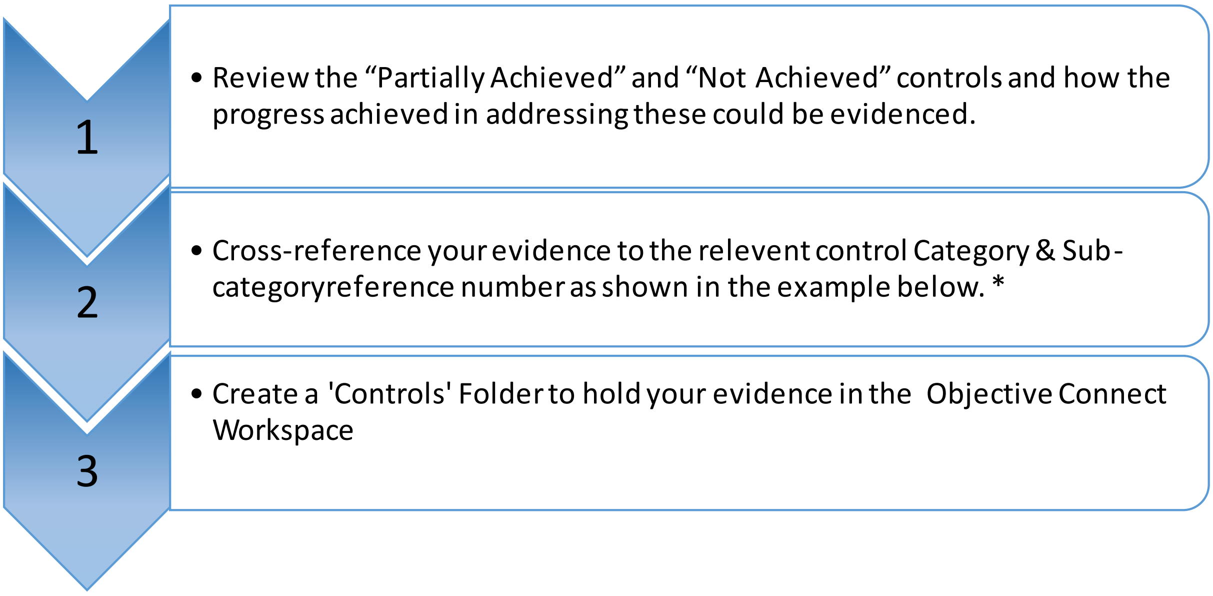
2
- Use this recommendation identification number when completing the Evidence Base Summary Template which is provided in Annex 1 of the Audit & Review 2021 Programme Guidance document. See Example below.

3
- Create a 'Recommendations' Folder to hold your evidence in the Objective Connect Workspace

RECOMMENDATIONS	**Review the recommendations and evidence how progress has been achieved in addressing these.** **EXAMPLE**	
Reference Number	Progress Narrative	Supporting evidence submitted.
1.1.2 The senior management and board members should receive awareness training on cyber risk	Cyber Risk training and development plan has been produced and approved…...	1.1.2 Cyber Risk Training and Development plan 1.1.2 Additional evidence 1.1.2 Additional evidence

Ensure evidence file name makes the cross-reference obvious

Controls Procedure



1

- Review the “Partially Achieved” and “Not Achieved” controls and how the progress achieved in addressing these could be evidenced.

2

- Cross-reference your evidence to the relevent control Category & Sub-categoryreference number as shown in the example below. *

3

- Create a 'Controls' Folder to hold your evidence in the Objective Connect Workspace

* As a guide to the relationship between the ISPF and CRF, Annex 1 of the ISPF shows a mapping of the ISPF controls to the CRF categories. The CRF document shows the Sub-Category & Control Requirement Reference Number.

https://www.gov.scot/publications/cyber-resilience-framework/

CONTROLS	**Review the “Partially Achieved” and “Not Achieved” controls and evidence the progress achieved in addressing these.** **EXAMPLE**	
Sub-Category & Control Requirement Reference Number	Progress Narrative	Supporting evidence submitted.
1.1 Target 5: There is a culture of awareness and education about cyber security across the organisation.	Use of NCSC exercise in a box. ELearning package in production for all staff	1.1 Simulated Phishing Campaign 1.1 Online Safety package 1.1 Covid scams poster 1.1 ………..

Ensure evidence file name makes the cross-reference obvious

Background

The Scottish Health Competent Authority (CA) is required by Article 15 of the NIS Regulations 2018 to conduct formal assessments and audits of health boards to obtain compliance assurance. To achieve this, a standardised methodology for both undertaking and reporting the audit has been developed to ensure transparency and consistency across health boards and between auditors.

The NIS Regulations compliance audit is intended to provide an independent, objective evaluation to aid improvement of a health board's operations and compliance. It is undertaken in a systematic and structured approach to evaluate the effectiveness of risk management, cyber security controls and governance processes as required by the regulations.

The categories and controls defined by the NHSS Information Security Policy Framework: 2018 were adopted as the basis for the NIS Audit and Review Programme. To harmonise with Local Authority Care Services security assessments and to ensure consistency across public bodies, the audit was structured in a manner consistent with the Public Sector Cyber Resilience Framework. This also had the additional benefit of enabling health boards to utilise the Scottish Government's self-assessment tool if they wish.

Correspondence from the Scottish Health Competent Authority of the 1st March 2019 outlined our intention to move fully towards the use of the 'Cyber Resilience Framework'

Amalgamation of the Information Security Policy Framework and the Scottish Public Sector Cyber Resilience Framework.

From 2022 onwards NHSS Information Security Policy Framework: 2018 shall no longer be in use and the Scottish Government Cyber Resilience Framework which applies to all public bodies in Scotland, including health boards and Local Authorities shall be wholly adopted as the framework to which NIS compliance audits shall be conducted against. This has the benefit of a uniform set of criteria for cyber security across all public bodies and for health will have the added benefit of better enabling the integration of health and care between the NHS and Local Authorities in a manner consistent with the Digital Health and Care Strategy.

Current NIS Audits and Reviews shall be performed using the ISPF controls, but to aid the familiarisation and migration of health boards to the CRF, the findings shall be reported under the categories of the CRF.

As a guide to the relationship between the ISPF and CRF, Annex 1 shows a mapping of the ISPF controls to the CRF categories.

You can access the ISPF here: https://www.healthca.scot/

You can access the CRF here: https://www.gov.scot/publications/cyber-resilience-framework/