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

Audit Programme: Structure & Reporting

Guidance

Version 1.7
19 May 2022

Contact email:
HealthCA@gov.scot

Website:
www.healthca.scot/

Revision History:
v. 1.6 Release

Contents

1. Introduction

Purpose

This paper provides guidance on how to conduct and report the findings of a NIS Regulations audit.

Rational

This guidance is provided to ensure consistency in methodology, structure and reporting, to remove variability in outlook and approach between auditors and provide clarity to health boards on the requirements and priority of the audit recommendations.

Background

The Scottish Health Competent Authority (SHCA) is required by Article 15 of the NIS Regulations 2018[1] 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[2] as required by the regulations.

Requirements

The Article 10[1] of the NIS regulations defines the security duties of health boards as an operator of essential services (OES):

> **10.**—(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.
> (2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.
> (3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.
> (4) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2).

Outcomes

Where operators do not comply with the NIS regulations, the Health CA has the power to take regulatory action including:

- Issuing an Information Notice to request information;
- Issuing an Enforcement Notice to require action to address failings; and
- Issuing a Penalty Notice levying a financial penalty not exceeding £17 million.

Action taken will be proportionate and only applied where it is clear that adequate security measures were not in place. The Health CA would assess the level of compliance and work with the individual

[1] Statutory Instruments, 2018 No. 506, Electronic Communications. The Network and Information Systems Regulations 2018, April 2018, 36pp. http://www.legislation.gov.uk/id/uksi/2018/506
[2] This mirrors the definition of internal audit by the Chartered Institute of Internal Auditors. https://www.iia.org.uk/resources/ippf/ (accessed 5/2/2019)

health board to ensure risks are mitigated whilst also considering what additional measures might be required to be implemented by the health board.

Penalties

The UK government intends to introduce a maximum financial penalty of £17 million for all contraventions under the NIS Regulations.

Under the NIS Regulations a health board has the right to ask an independent reviewer to review any penalty decision.

Compliance Dates

As notified[3] health boards were legally required to be compliant with the NIS Regulations from **10th May 2018**.

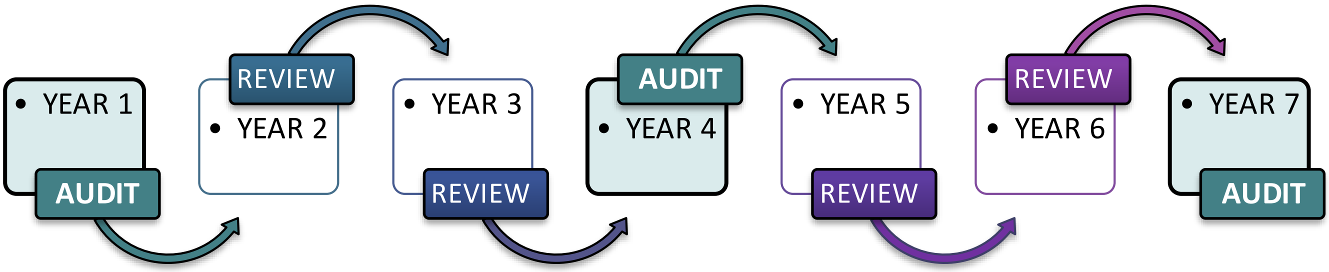
Health boards may wish to undertake a Gap Analysis on their existing systems and security in order to assess what improvements are needed. A copy of the Gap Analysis and proposed Action Plan should be submitted to the Scottish Health Competent Authority.

Audits vs Reviews

In 2019 the Scottish Health Competent Authority commissioned audits of all health boards. Thereafter, audits shall be conducted typically every third year unless incident reports merit a more frequent audit programme.

In intervening years, compliance Reviews shall be commissioned instead of audits (Figure 1.1). These will focus on progress on: recommendations from audits; risk mitigation development outcomes arising from incidents and the management of security requirements since the introduction of new regulations, best practice guidance or technology changes.

FIGURE 1.1: Audit – Review programme cycle.



To ensure health boards are not subject to multiple security-related audits from differing organisations within a single year, the CA shall liaise with Audit Scotland and individual health boards to place the NIS Audits within a health board's "audit universe" three-year programme.

[3] Scottish Government. EU Security of Network and Information Systems (NIS Directive), Letter to Chief Executives of NHSS Boards from Huggins, Geoff, 8 May 2018, 2pp.
Swinney, John, Yousaf, Humza. Network and Information Systems Regulations (NISR), Letter to Chief Executives of NHSS Boards, 31 May 2022, 5pp.

2. Audit Programme: Structure & Procedure

The audit programme end-to-end is a seven-stage exercise, the first five of which are conducted before the formal assessment commences. Each will be described in turn. Note that the Review stage is post-audit and subject to a separate guidance paper[4].

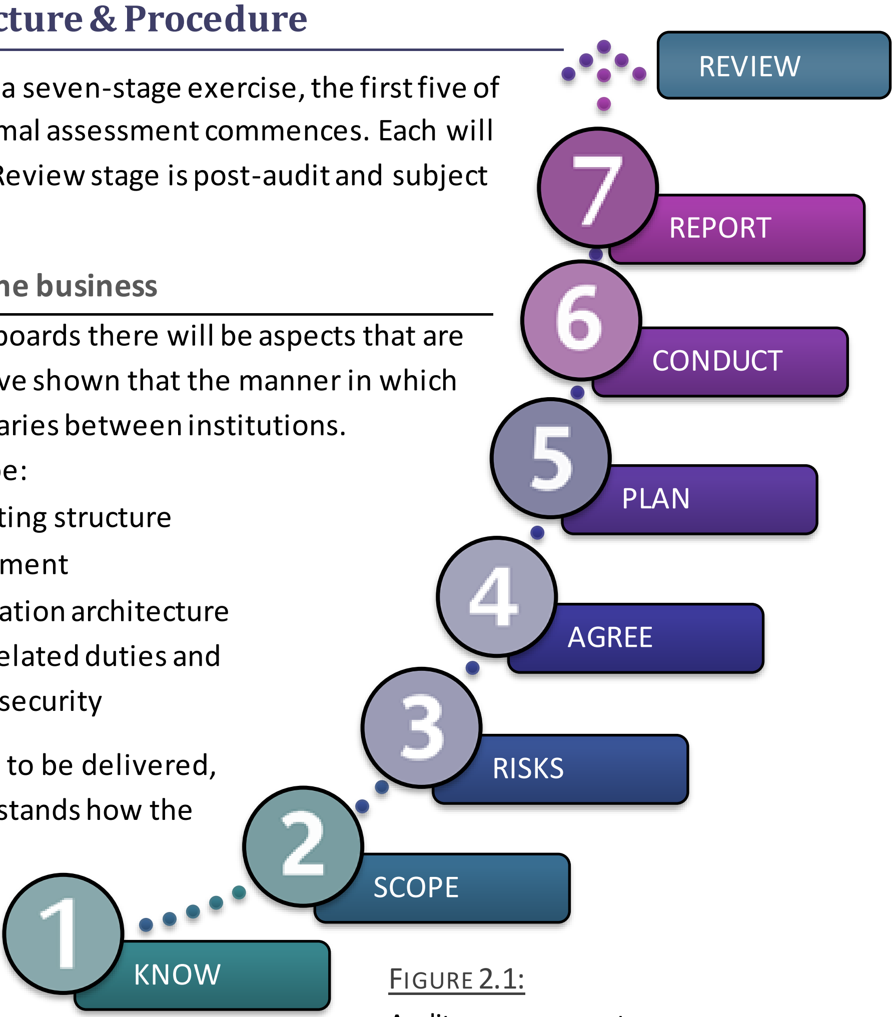


FIGURE 2.1:
Audit programme stages.

Know and understand the business

Although between health boards there will be aspects that are common to all; reviews have shown that the manner in which these aspects are addressed often varies between institutions. Exemplars of such variations could be:

- the organisational and reporting structure
- the approach to risk management
- the infrastructure and application architecture
- the distribution of security-related duties and
- culture and training in cyber security

If a meaningful and targeted audit is to be delivered, it is essential that the auditor understands how the health board addresses and manages cyber security in both principle and practice together with the drivers for change imposed upon the organisation.

This latter aspect should be captured and included within the final report, the drivers are readily summarised in a table (see Table 2.1 as an exemplar).

This contextual understanding must be in place to enable the auditor to report on the above exemplars, define the audit and agree the Terms of Reference and can only be achieved through on-site observations, shadowing and discussions with key staff members.

On-site investigations are therefore a requirement of the NIS audit.
Desktop-only or remote exercises alone are not sufficient for an audit to be accepted.
The exception being unforeseen events of an extreme nature such as the coronavirus pandemic.

Define the Scope

The broad scope of the audit shall be common to all health boards, namely the extent to which compliance with the NIS Regulations has been achieved. The scope should therefore incorporate all

[4] Network & Information Systems Regulations 2018: Compliance Review Programme: Structure & Reporting – Guidance. May 2022, 17pp.

systems, applications and services that contribute to the delivery of the essential service. This should be agreed with the organisation. There may however, be organisation-specific areas or controls that merit additional focus and emphasis due to enhanced threat of vulnerability exposure. Exemplars may be:

- Cloud storage
- Connectivity and resilience provision
- Outsourced and third party solutions and services
- Significant changes, for example to:
    - IT architecture,
    - business structure
    - governance and reporting
    - incident management and lessons identified

Note that any such enhanced vulnerability or exposure can only be meaningfully achieved through an understanding of the business and organisational practices and structures, as required by stage 1 above.

Under such circumstances, the scope should be expanded to explicitly state any additional or specific areas that shall be subject to scrutiny.

3 Undertake a risk assessment

As an integral aspect of determining the scope and focus of the audit, a risk assessment should be undertaken to identify any aspect of the organisational structure and governance around service resilience that subjects the board to additional risk. Some exemplars that would require examination for satisfactory risk management are shown in section 2.2. Others may be highlighted as the auditor gains an understanding of the business processes and operations of the health board.

These additional risks would be captured in the Terms of Reference or Audit Definition, cross referenced to the risk register and placed in-scope.

4 Agree the Terms of Reference for the Audit

There may be a broad agreement of the purpose of the audit, however production of a Terms of Reference (ToR) document with sign-off by a senior executive, ensures a common understanding is in place between the auditor and the health board.

An exemplar of a ToR is illustrated in Table 2.1. Note that the Improvement Action Grade manner of recommendation prioritisation is a requirement of the reporting structure.

5 Plan the audit

Prior to arriving on site, the audit programme should be planned. This includes determining the relevant personnel to interview and identification of key documentation for review. In addition to the formal security-related documentation; policy documents, corporate reports, audit committee minutes, incident reports may for example also be incorporated into the review. These papers aid identification of potential issues for inspection and discussion and provide context for the audit.

TABLE 2.1: Audit Terms of Reference document exemplar.

Introduction

Briefly describe the structure of the audit, the deliverables and how these shall be prioritised. For example:

At the conclusion of the audit, a Gap Analysis report shall be produced. This shall include improvement recommendations graded into five categories to enable the creation of a prioritised roadmap and action plan. The improvement action grades are defined as follows:

Improvement Action Grades	Definition	Detail
Black	Critical	Fundamental absence or failure of controls – immediate action is required.
Red	Urgent	High risk exposure – absence or failure of key controls exposing the organisation to breach or non-compliance.
Amber	Important	Moderate risk exposure – controls are in place but not working effectively, risking compliance or security breach
Yellow	Attention	Minor risk exposure – controls or procedures are working effectively but not as efficiently as possible or as required; a cost-benefit-risk assessment is advised.
Green	Low Risk	Minor control strengthening changes required or application of protocols enforced.

Audit Definition

Objectives	To consider and evaluate: • the adequacy, completeness and effectiveness of the information security policies and procedures • adequacy and effectiveness of network and application security systems • adequacy and effectiveness of physical security systems • compliance with the NIS Regulations. To make recommendations for any developments to enable the health board to protect the confidentiality, integrity and availability of information and data.
Context	Add details of any relevant changes that impact upon the health board and its compliance with the NIS Regulations. For example: • Additions to regulatory structure or legislation • Scottish Government or NHSS requirements • Additional or new security or resilience threats
Scope	Define how the information security provisions of the health board shall be assessed and include any specific aspects that shall be subject to scrutiny.
Risks	Define specific risks that have been observed or to which the health board is exposed and that shall be the subject of specific focus.
Risk Register Link	Cross reference to items in the corporate risk register if relevant.
Key Contacts	List key audit contacts for information, insights gathering and discussion. Note that this is just the key contacts and does not preclude additional staff members being interviewed as part of the audit.
Approach	State how the audit shall be undertaken for clarity. For example: This audit shall be conducted as follows: • Planning and scoping • System specifications and procedural documentation review • Discussions with key personnel • Threat trends and evaluation and relevance to the health board • Requirements gathering for any new technology required • Review of regulatory requirements and compliance • Agreeing findings and recommendations
Reporting Format	Describe how the findings of the audit shall be reported. For example: • Written report submitted to [senior executive name] • Presentations as required by [e.g. the Audit Committee].
Approved	[named officer for the health board] Name: Date:
	[auditor] Name: Date:

6 Conduct the audit

The categories and controls defined by the Scottish Government Cyber Resilience Framework[5] (CRF, Annex 1) shall be adopted as the basis for the compliance assessments and audits. To harmonise with Local Authority Care Services security assessments and to ensure consistency across public bodies, the audit shall be structured in a manner consistent with the CRF. This will have the additional benefit of enabling health boards to utilise the Scottish Government's self-assessment tool if they wish.

7 Findings & Recommendations Report

The consistency of the audit approach and methodology shall be reflected in a defined report structure, this is described in Part 3 below.

To provide clarity to health boards and to permit management and focus of resources, recommendations for developments arising from the audit shall be prioritised on a five -level risk basis. Moreover, it is expected that the auditor shall identify observed areas of Good Practice in the organisation. It is possible that good practice may not have auditable documentation, but this should not preclude the auditor from capturing observations made throughout the audit.

[5] Scottish Government Public Sector Action Plan Cyber Resilience Framework https://www.gov.scot/publications/cyber-resilience-framework/

3. Audit Report: Structure & Content

The findings and recommendations from the audit together with details of the methodology and approach should be reported in the following structure shown below.

PART 1: Context

Section 1. Introduction

This is a scene-setting description of the health board to include geographic reach, population served, services delivered, specialist provisions, organisational structure and third-party suppliers related to the essential services.

Incidents reported in the last year
A summary of incidents reports, impacts, outcomes and mitigation measures

Drivers of Change
A contextual summary of regulatory, standards and strategic impositions on health boards as drivers for compliance and change (see exemplar in Table 3.2)

Scope
Define the boundaries of the audit and any specific areas that merit particular attention, cross reference to the ToR

Objectives
Define specific objectives for the audit with any additional items under consideration with a cross-reference to the ToR. For example:

To consider and evaluate: the completeness, adoption and effectiveness of the IT policies and procedures; compliance with recognised good practice and relevant standards; staff skills and development; alignment of IT services with business needs.

To make recommendations for any developments to enable the health board to effectively assess, manage and align essential service delivery and team structure to meet business and compliance requirements.

Risks
In the context of the pre-audit preparation work, identify any risks that are specific to the health board that shall be examined for controls and mitigation measures.

Risk Register Links
List relevant risks contained in the health boards corporate risk register.

Approach
State the regulatory framework or standard against which the audit is being conducted (NIS Regulations); any specific areas that shall be highlighted or addressed; the person(s) conducting the audit with a summary of their qualifications and experience.

Section 2. Methodology

Describe the procedures and activities adopted to conduct the audit. Under each item the Aim of activity and the associated Tasks should be summarised. For example:

Activity 1: Baselining

Aim: To provide a baseline of the existing security provision against which to evaluate improvement options.

Tasks:

1. Review of papers regarding security services, operational practices and supplier management.
2. Key person meetings to provide insights into cyber security provision; common issues and concerns.

Activity 2: Good Practice Analysis

Aim: To compare security policies, practices and systems with recognised good practice guidance.

Tasks:

1. Review of existing latest guidance on security management.
2. Determine alignment of existing practices with this guidance.

Activity 3: Reporting

Aim: To ensure Key Persons are kept informed of progress of the project.

Tasks:

1. Regular Project Updates to the relevant Director.
2. Draft report with recommendations and prioritised actions for discussion with key personnel.
3. Final report with recommendations and risk assessment for Senior Leadership Team (SLT) & Audit Committee.

Activity 4: Analysis, Feedback & Recommendations

Aim: To deliver the outcome of this investigation and provide analysis and recommendations for future development of security provision and practices.

Tasks:

1. Write Final Report with Recommendations to include:

- Observations on existing practices.
- Recommendations for staff skills development.
- Comparison with guidance and compliance requirements.
- Recommendations for security service development.

2. Meetings with the relevant Director and staff to review options and agree recommendations for SLT consideration.

3. Present final report to SLT for review.

Section 3. Good Practice Guidance & Frameworks

Cite any relevant frameworks and guidance that supplement or support the audit against NIS regulations.

For example: NCSC guidance on supply chain and cloud provision.

PART 2: Sources & Systems

Section 4. Meetings and Document Review

Detail the meetings with key persons and list the documentation reviewed to demonstrate how an understanding of the business has been attained.

Staff Meetings

List persons met with dates, include a description of their role and responsibilities.

Document Discovery & Review

List the documentary evidence on policies, procedures and meeting records employed as evidence for example, of good governance, record keeping and active policy deployment.

Section 5. Services and Systems

Summarise the IT systems and services that exist in the organisations as the context for the security evaluation.

Service Suppliers

Detail the IT suppliers to the organisation with the systems, applications and services provided, including any specific security and resilience provisions. Highlight any mission-critical services and co-dependencies.

Systems

Summarise the IT network and associated in-scope key applications and devices. This summary should include:

- IT Network, to include infrastructure on-premise and outsourced
- Server locations, including back-up and disaster recovery provisions
- Connectivity to the organisation including resilience provisions, staff and guest Wi-Fi facilities
- Telephony, including any voice recording systems
- Mobile devices, including a description of security on devices

Applications

Detail applications considered mission critical and the associated resilience and security capabilities.

Section 6. Policies

List any relevant new, revised or updated policies that are in place with dates of creation, review plans and evidence of implementation. Highlight any gaps in provision and scope of the policy portfolio.

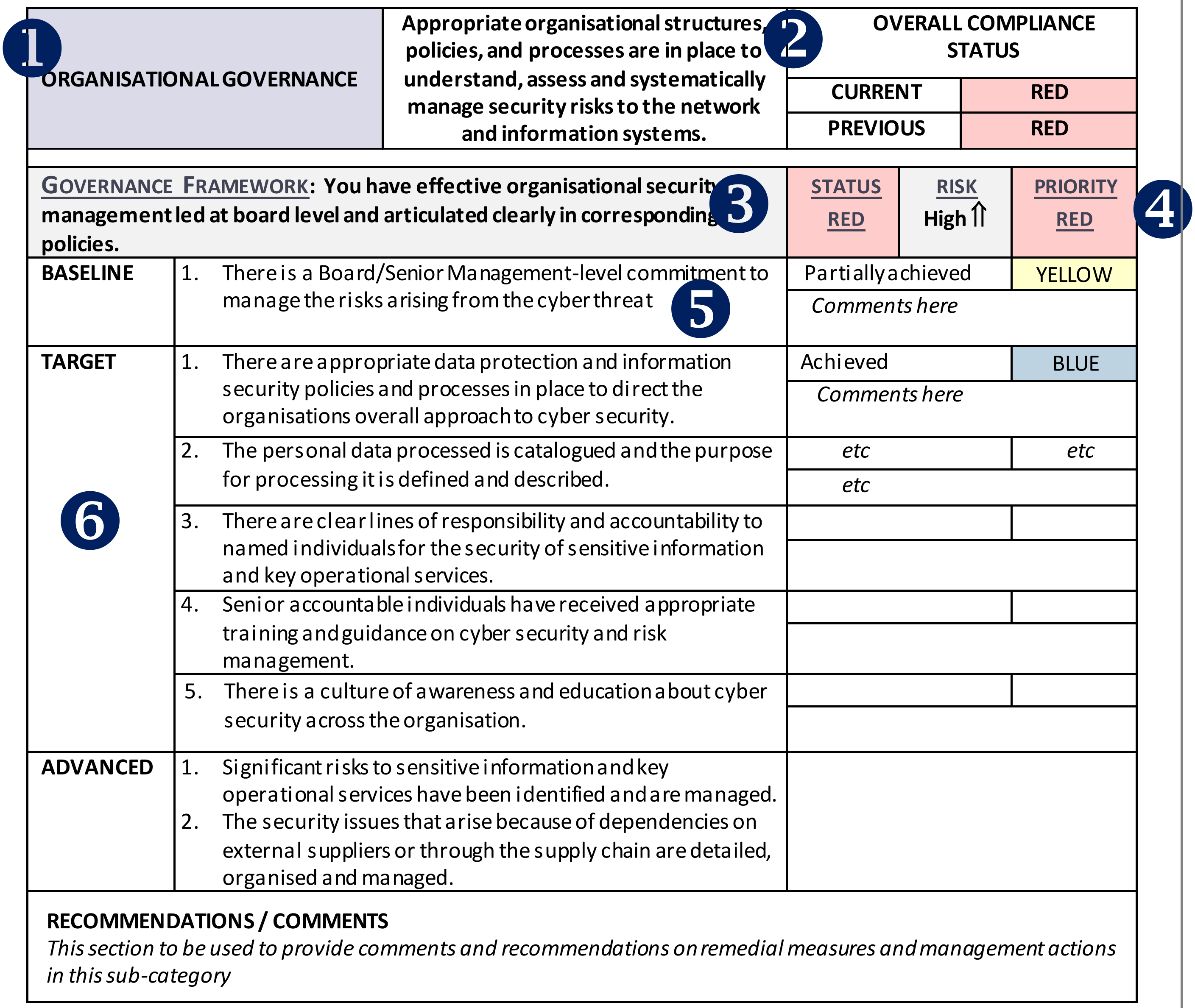
PART 3: Controls Compliance Assessment

The Cyber Resilience Framework forms the basis of the evaluation of the health board provision for fulfilment of the NIS Regulations. To ensure compatibility with Local Authority health care provision security assessments, the NIS audits are reported under the categories defined by the Scottish Government Public Sector Cyber Resilience Framework (CRF, Annex 1).

Section 7. Audit Findings

The audit should report against the CRF categories utilising the score card approach shown in Fig. 3.1.

FIGURE 3.1: Scorecard structure for summarising audit findings



ORGANISATIONAL GOVERNANCE	**Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems.**	**OVERALL COMPLIANCE STATUS**		
		CURRENT	**RED**	
		PREVIOUS	**RED**	
GOVERNANCE FRAMEWORK: You have effective organisational security management led at board level and articulated clearly in corresponding policies.		**STATUS** **RED**	**RISK** **High ⇈**	**PRIORITY** **RED**
BASELINE	1. There is a Board/Senior Management-level commitment to manage the risks arising from the cyber threat	Partially achieved		YELLOW
		Comments here		
TARGET	1. There are appropriate data protection and information security policies and processes in place to direct the organisations overall approach to cyber security.	Achieved		BLUE
		Comments here		
	2. The personal data processed is catalogued and the purpose for processing it is defined and described.	*etc*		*etc*
		etc		
	3. There are clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services.			
	4. Senior accountable individuals have received appropriate training and guidance on cyber security and risk management.			
	5. There is a culture of awareness and education about cyber security across the organisation.			
ADVANCED	1. Significant risks to sensitive information and key operational services have been identified and are managed. 2. The security issues that arise because of dependencies on external suppliers or through the supply chain are detailed, organised and managed.			

RECOMMENDATIONS / COMMENTS

This section to be used to provide comments and recommendations on remedial measures and management actions in this sub-category

Key to Figure 3.1

❶	Cyber Resilience Framework category with description in adjacent cell.
❷	Overall compliance status of category with respect to NIS Regulations, both from the Current assessment and, for comparison the Previous audit or review utilising the BRAYG criteria described in Table 4.1.
❸	Sub-category with summary description
❹	Compliance status of the sub-category together with Risk and Priority utilising the BRAYG criteria described in Table 4.1
❺	Individual evaluation criteria with compliance assessment (Achieved (BLUE), Partially Achieved (YELLOW), Not Achieved (RED)) with brief comments of explanation
❻	Baseline, Target and Advanced stage criteria groupings from the Cyber Resilience Framework. Note that all health boards must attain the ADVANCED stage and all associated criteria.

PART 4: Analysis, Recommendations and Actions

Section 8. Assessment Summary

This section summarises the findings of the audit, highlighting aspects of good practice, areas to be developed and risks prioritised against a 5-stage BRAYG risk rating.

Good Practice

To afford a balance between the areas for development, and to recognise achievements, aspects of observed good practice should be recorded. Note that these may not have evidential documentation but would be observed when on-site on meetings, interviews and shadowing exercises.

Areas for Development

List in priority order the broad categories which have been identified for development. This provides a useful overview prior to the more detailed recommendations for management actions.

Risks to be Addressed

If during the audit areas of high risk that are worthy of specific attention are identified these should be detailed and recorded in this section.

Priority Definitions

A risk-based approach is applied to both areas for development and risks to be addressed. This enables organisations to focus resources in areas of greatest need and vulnerability. These are defined in Table 4.1.

TABLE 4.1: Priority Definitions

Priority	Definition	Detail
Black	Critical	Fundamental absence or failure of controls – immediate action is required.
Red	Urgent	High risk exposure – absence or failure of key controls exposing the organisation to breach or non-compliance.
Amber	Important	Moderate risk exposure – controls are in place but not working effectively, risking compliance or security breach
Yellow	Attention	Minor risk exposure – controls or procedures are working effectively but not as efficiently as possible or as required; a cost-benefit-risk assessment is advised.
Green	Guidance	Minor control strengthening changes required or application of protocols enforced.

Section 9. Recommendations and Management Actions

The major part of the report will be the evaluations against each sub-category using the score card format shown in Figure 3.1. This section captures the recommendations made throughout the report and applies them into a prioritised listing based upon the definitions shown in Table 4.1. For each of cross reference, a recommendation identification number should be applied.

The recommendation should be discussed with the management team, from which actions, an owner and a timescale for completion should be agreed.

This recommendations and associated actions will constitute part of the NIS Reviews that occur between NIS Audits.

TABLE 4.2: Recommendations report structure

Priority	Id. No	Category / Recommendations	Management actions	Owner	Timescale
Black Critical		CATEGORY HERE: RECOMMENDATION:			
Red Urgent					
Amber Important					
Yellow Attention					
Green Guidance					

Executive Summary

Sections 8 and 9 can usefully form the basis of the Executive Summary, placed at the beginning of the report as these capture the key points that will be the subject of review at Senior management and Audit Committee meetings.

Annex 1: CRF Common Categories and related sub-categories.

MANAGE

ORGANISATIONAL GOVERNANCE	RISK MANAGEMENT	ASSET MANAGEMENT
Governance framework Leadership & responsibility - SMT - Board Adoption of assurance standards Information Asset Register Audit/assurance compliance	Risk management policy & process Cyber / Information Risk Assessment Risk treatment & tolerance Risk governance - Risk assurance & management - Risk register review - Board responsibility - Risk training & culture	Hardware assets register & management Software assets register & management Infrastructure management
SUPPLIER MANAGEMENT		
Supply chain security assurance & management Roles & responsibilities defined Access control Security in system procurements		

PROTECT

INFORMATION SECURITY MANAGEMENT	PHYSICAL/BUILDING SECURITY	OPERATIONAL SECURITY
Security policy & processes Lifecycle management Storage - cloud/3rd party - on premise Information/data classification Information assets register Information/data transfer controls	Access control Internal security **SYSTEM MANAGEMENT** Secure configuration Secure design/development Change control procedures System Testing	Malware policies & protection - AV screening - Media scanning - File scanning Email security Application security Vulnerability management & scanning - Executables prevention - Peripheral device management Data exfiltration monitoring Software supported & updated Web site screening Browser management Monitor/audit user activity Disabled auto-run
SERVICES RESILIENCE	**PEOPLE**	**NETWORK SECURITY**
ACCESS CONTROL Account management Identity authentication - Password policy - Multi factor authentication Privilege management Administrator account management **MEDIA MANAGEMENT** Storage media management -Mobile media/devices Cryptography Remote wipe capability **ENVIRONMENTAL SECURITY** Equipment location Power resilience	Prior to employment - Security screening - T&C During employment - induction - security roles & responsibilities - acceptable use policy - disciplinary procedures Staff training & awareness culture Staff skills assessment - Board - SMT - Staff - Interim & contractor	Patch management Device management Content screening Internal segregation Wireless security Boundary/Firewall management Administrator control Error message management Penetration testing IP & DNS management

DETECT

INCIDENT DETECTION		
Detection capability Security Monitoring		

RESPOND & RECOVER

INCIDENT MANAGEMENT	BUSINESS CONTINUITY	
Incident response protocol Incident reporting procedure Staff training & testing Post-incident review & learning	Data recover capability Back up policies & procedures Disaster recovery policies & procedures BC/DR testing policies & procedures Data Loss impact assessments BC contingency plan	