Network & Information Systems Regulations 2018

Compliance Review

Structure & Reporting Guidance

Version 1.1
May 2022

Contact email:
HealthCA@gov.scot

Website:
www.healthca.scot/

Revision History:
v. 1.0 Release Document

Contents

1. Introduction

Purpose

This paper provides guidance on how to conduct and report the findings of a NIS Compliance Review to be undertaken in intervening years between NIS Audits.

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 priorities of the NIS Compliance Review.

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 and this review have been developed to ensure transparency and consistency across health boards and between auditors.

The NIS Regulations Compliance Review 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:

> **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 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.

[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)

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

Compliance Dates

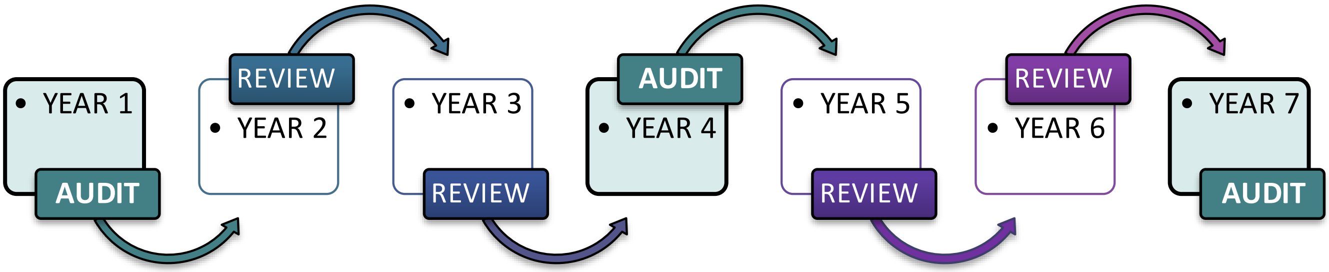
As notified[3] health boards were legally required to be compliant with the NIS Regulations from **10th May 2018**.

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 or significant system changes 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.



[3] Huggins, Geoff. EU Security of Network and Information Systems (NIS Directive), Letter to Chief Executives of NHSS Boards, 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.

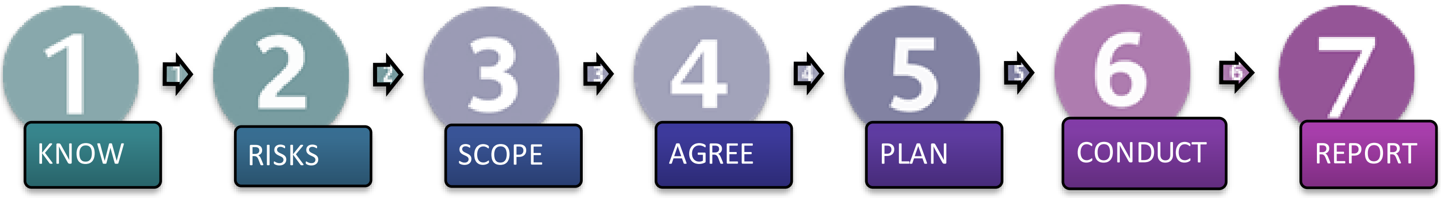
2. Compliance Review: Structure & Procedure

The Compliance Review builds upon and considers several information sources to evaluate progress, namely:

- the recommendations of the last NIS Audit or Review
- lessons learned report and mitigation measures introduced following a reportable incident
- significant changes to system architecture or structure
- new outsourcing arrangements or supply chain changes
- new or revised frameworks and standards introduced since the last audit
- information on new or emerging threats

The Compliance Review shall follow a structured approach with some stages conducted before the formal assessment commences. This is illustrated in Figure 2.1, each stage shall be described in turn.

FIGURE 2.1: Stages in the delivery of a Compliance Review



STAGE 1: Know and capture any business changes

The Review should focus on relevant changes to the business **since the last audit or review**, namely:

- **Recommendations:** Review recommendations previously made and the progress achieved in addressing these.
- **Incidents:** Identify any reportable incidents and measures taken to mitigate any reoccurrence
- **System Changes:** Identity any changes to the network, software, hardware, service delivery and associated security implications
- **People Changes:** For example to organisation governance, reporting structures, responsibilities, new staff with the implications for NIS compliance.

If a meaningful and targeted Review 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.

These aspects should already be captured and included within the Audit report, with which the auditor should become familiar. This contextual understanding must be in place to enable the auditor to define the Review and agree the Terms of Reference (see Table 2.1 as an exemplar) and can only be achieved through an understanding of the outcomes of the last Audit, on-site observations, shadowing and discussions with key staff members.

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

STAGE 2: Undertake a revised risk assessment

As an integral aspect of determining the scope and focus of the review, a new or revised risk assessment should be undertaken to identify any new threats, vulnerabilities and risks that have arisen since the last audit or review. Some exemplars that would require examination for satisfactory risk management are shown in Stages 1 and 3.

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

STAGE 3: Define the Scope

The broad scope of the Review shall be defined at least in part by the recommendations from the last audit or review reports, plus the additional information sources cited above in Stage 1. The scope of the Review could therefore be expanded beyond that of the last audit or review if there have been other significant changes to the organisation or IT systems, for example:

- business structure
- governance and reporting
- incident management and lessons identified
- network architecture
- outsourced services provision
- new firms in the supply chain

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.

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

STAGE 4: Agree the Terms of Reference

There may be a broad agreement of the purpose of the review, 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.

STAGE 5: Plan the Compliance Review

Prior to arriving on site, the Compliance Review should be planned.
This includes reviewing the previous audit/review reports and recommendations, determining the implications of any changes to organisational information systems and services, identifying the relevant personnel to interview and review of new or revised key documentation.
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 any additional potential issues for inspection and discussion and provide context for the review against progress since the previous assurance appraisal.

TABLE 2.1: Review 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 of network and application security systems • adequacy 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	Cross reference to items in the corporate risk register if relevant.
Approach	State how the audit shall be undertaken for clarity. E.g: 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 • Agree findings and recommendations
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.
Resources	List the auditors involved together with the time allocation per person.
Timetable	List milestones with dates: examples include: fieldwork commencement and completion dates; meeting dates; reports issued, both draft and final; audit committee meeting date for attendance.
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:

STAGE 6: Progress Assessment: Conduct the Review Appraisal

The categories and controls defined by the Scottish Government Cyber Resilience Framework[4] (CRF, Annex 1) shall be the basis for the audits and associated recommendations that shall be considered by the Compliance Review. To harmonise with Local Authority Care Services security assessments and to ensure consistency across public bodies, the recommendations of the Review 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.

STAGE 7: Findings, Actions & Recommendations Report

The consistency of the audit approach and methodology shall be reflected in a defined report structure, this is described in Part 4 below. As this is a Review not a full audit appraisal, the key areas of the findings focus should be:

- Progress against previous recommendations
- Progress against mitigating previously identified risks
- Identification and risk assessment of new developments and changes (i.e. as listed in Stage 2 above)
- New Threats, Vulnerabilities and Risks (TVR) assessments and mitigation measures

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

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

3. Compliance Review Report: Structure & Content

The findings and recommendations from the review 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 summary description of the health board to include services delivered, specialist provisions, organisational structure and third-party suppliers related to the essential services.

RISP Changes

This section provides context and summarises changes since the last audit/review under the following categories, namely:

- Recommendations : A list of past recommendations
- Incidents : A summary of incidents reports, impacts, outcomes and mitigation measures
- System Changes : An overview of changes to the network, software, hardware, service delivery and associated security implications
- People Changes: For example to organisation governance, reporting structures, responsibilities, new staff with the implications for NIS compliance.

Risks

Identification of new risks that have emerged from the changes highlighted above plus new threats and vulnerabilities identified.

Scope

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

Objectives

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

To consider and evaluate: progress made against previous recommendations; the emergence of new risks and efficacy of mitigation measures introduced.

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

Risk Register

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 Review. 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 previous audit/review appraisal recommendations.

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: Threat/Risk Analysis

Aim: To identify new issues to be addressed.

Tasks:

1. Review changes to systems, suppliers, services and associated new threats/risks these introduce.

2. Review implications of any new frameworks, legislation or standards on organisational risk profile.

Activity 4: 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 5: 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 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 any changes since the previous audit/review to the IT systems and services that exist in the organisations as the context for the security evaluation.

Service Suppliers & Supply Chain

Detail the IT suppliers and supply chain 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
- Outsourced systems and services

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: Progress 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. Findings & Recommendations

This section forms the basis of the assurance evaluation. Assessment should be made on progress against the recommendations made in the previous audit/review and the efficacy of risk mitigation measures.

1. Findings – Recommendations Progress

Progress against fulfilment of the recommendations previously identified should be summarised in tabular format as shown in Table 3.1. Additional narrative should be provided to summarise the extent of progress and any issues encountered by the organisation. Any additional recommendations should be made in the text and captured in prioritised ranking in Table 4.2.

2. Findings – New Developments Recommendations

This should be a narrative section that describes the context and threat/risk assessment as a consequence of new development. Recommendations should be made within each area under discussion and captured in prioritised ranking in Table 4.2.

TABLE 3.1 Progress on Past Recommendations.

Category / Recommendations	No	Previous Priority Status	Agreed actions	Owner	Timescale	Current Priority Status	Current Review Comments
CATEGORY: RECOMMENDATION:	1	Black Red Amber Yellow Green Blue				Black Red Amber Yellow Green Blue	
etc.	*etc.*	*etc.*				*etc.*	

3. Findings – Risks Mitigation Progress

Progress against mitigating risks previously identified should be summarised in tabular format as shown in Table 3.2. Additional narrative should be provided to summarise the extent of progress and any issues encountered by the organisation.

A trend in the previously identified risks should be evaluated alongside the current status to place an emphasis on changes in risk proximity. Any additional risks should be highlighted in the text and captured in prioritised ranking in Table 4.2.

TABLE 3.2: Risk Mitigation Progress Summary

Risk Area / Details	Previous Status	Mitigation Actions	Current Status	Progress	Risk Trend
Risk description	Black Red Amber Yellow Green Blue	Describe mitigation measures introduced from previous audit/review	Black Red Amber Yellow Green Blue	Summarise progress: • Achieved • No Change • In Progress	Increasing ⇑ No Change ⇔ Decreasing ⇓

4. Findings – New Risks

This should be a narrative section that describes the context and a risk description that has arisen as a consequence of new development. Recommendations should be made within each area under discussion and captured in prioritised ranking in Table 4.2.

PART 4: ANALYSIS, RECOMMENDATIONS AND ACTIONS

Section 8. Compliance Assurance Evaluation Summary

This section summarises the findings of the Review, citing progress against past recommendations, highlighting aspects of good practice, areas to be developed and risks prioritised against the 5-stage BRAYGB risk rating (Table 4.1).

Key Messages

A brief summary overview of the conclusions from the review written for easy assimilation by non-technical senior managers.

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.

Progress against past Recommendations

Summarise the number of actions that remain outstanding ranked by the risk prioritisation. Show projected timeframes for completion.

New or Emerging 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.

New or Emerging Risks to be Addressed

If during the review new areas of 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: BRAYGB Ranked 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.
Blue	Completed	Previous Recommendations and Risks have been addressed and mitigated, item complete.

Section 9. Recommendations and Management Actions

The major part of the report will be the evaluations on progress against previously identified risks and recommendations with the implications of any changes or new developments described in Section 7.

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 ease of cross reference, a recommendation identification number should be applied.

The recommendations should be discussed with the management team, from which actions, an owner and a timescale for completion should be agreed as shown in the recommended structure in Table 4.2.

These recommendations and associated actions will constitute part of future Reviews that occur between Audits.

TABLE 4.2: Past and New Recommendations Summary

Priority	Id. No	Category & Recommendations	Management actions	Owner	Timescale
Black Critical		CATEGORY: 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

Governance framework

Leadership & responsibility

- SMT
- Board

Adoption of assurance standards
Information Asset Register
Audit/assurance compliance

SUPPLIER MANAGEMENT

Supply chain security assurance & management
Roles & responsibilities defined
Access control
Security in system procurements

RISK MANAGEMENT

Risk management policy & process

Cyber / Information Risk Assessment

Risk treatment & tolerance
Risk governance

- Risk assurance & management
- Risk register review
- Board responsibility
- Risk training & culture

ASSET MANAGEMENT

Hardware assets register & management
Software assets register & management
Infrastructure management

PROTECT

INFORMATION SECURITY MANAGEMENT

Security policy & processes
Lifecycle management
Storage

- cloud/3rd party
- on premise

Information/data classification

Information assets register

Information/data transfer controls

SERVICES RESILIENCE

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

PHYSICAL/BUILDING SECURITY

Access control
Internal security

SYSTEM MANAGEMENT

Secure configuration
Secure design/development

Change control procedures

System Testing

PEOPLE

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

OPERATIONAL SECURITY

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

NETWORK SECURITY

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	