Approved July 2015

NHSScotland Information Security Policy Framework

The aim of the NHSS Information Security Policy Framework is to set out - at an appropriately high level - the mandatory common components that must be embedded in each Board-level Information Security Policy/Objectives document and own information security management system (ISMS) so that the risks relating to the confidentiality, integrity and availability of all types of written, spoken and computer information are managed.

NHSScotland is a complex federation of 14 territorial and 8 special Health Boards that vary considerably in size and purpose. For the most part, managing information risk is a core responsibility of the Chief Executive Officer for each legal entity (the Board). But in a federal group of organisations there are of course information risks which criss-cross Boards and healthcare services and it is the responsibility of the Chief Executive Officer of NHSS (Director-General Health and Social Care in The Scottish Government) and ultimately the Cabinet Secretary for Health, Wellbeing and Sport to set out the common information security components that must be in place in each Board so that information risks are managed in a consistent and effective way and are in line with the national strategies and risk appetite.

The common components (which include specific controls, NHSS standards resources, processes and leadership) are aligned as closely as possible with International Standards ISO-27001 and ISO-27002.

NHSS is committed to conforming to ISO-27001 as far as practicable so as to create the necessary trust that is required by an ever wider network of information sharing partners such as central and local government who wish to gain assurance that the information security management system which operates in all NHSS Boards are all broadly equivalent.

1) Leadership and commitment

Board Chief Executive Officers shall demonstrate leadership and commitment with respect to information security management by ensuring that the Board-level information security policy, security objectives and information security management system (ISMS) are established and are compatible with the strategic direction of both the organisation and NHSS as a whole.

- Establish a Board-level information security management system that integrates well into the other functions of the organisation such as Information Governance, eHealth and estates/physical security and Human Resources.
- Ensure that resources needed for the effective operation of the ISMS are available and is supported by top management.
- Establish a Board-level information security policy that is appropriate to the needs of both the organisation and aligned with the NHSS information security policy framework.
- Assign the role of senior information risk owner (SIRO) at executive level to ensure that the above is undertaken and performance on the ISMS reported to the management board at regular intervals.
- Ensure that all of the above is communicated to staff, business partners and the wider public to ensure that trust and confidence is maintained in health and care services.

2) Information Security Objectives

The Board shall establish high level information security objectives for the entire organisation.

The Board information security objectives shall be aligned with:

- NHSS eHealth Strategy, so that the Information security function and ISMS support all seven strategic aims.
- NHSS/SG Information Governance Improvement Plan.
- The set of specific, measurable actions relating to information security to be undertaken at national level over a defined period as part of NHSS eHealth Programme.

- The Board specific actions that need to be undertaken, the planning, resources, time-scale, persons responsible and how/when results to be evaluated.

3) Information Security Policy

Each Board shall establish its own information security policy which includes components of the NHSS Information Security Policy Framework, national controls and standards as well as specific local policies

This policy shall be communicated with all staff and interested parties and revised at regular intervals.

4) Information Security Management System

Each Board shall establish, implement, maintain and continually improve an information security management system.

'System' in this context does not mean an 'IT system' but rather the dynamic and never-ending circular business system: which starts with planning, then building, then acting, then checking then planning again.

Simply having the information security post being filled (e.g. information security officer) that can react to incidents does not equal having an ISMS. Each Board shall act upon and document the key components (detailed below) that make up its ISMS.

4.1 **Scope**

Each Board shall determine the boundaries and scope of its ISMS and associated policy. Each Board has business relationships with an array of partners, ranging from local authorities, emerging health and social care partnerships, third sector, universities and commercial suppliers. Although there should be information sharing agreements with partners/suppliers and they may share the IT network and other computing resources it would simply not be practical for the Board ISMS to cover this whole landscape. Instead, the Board ISMS and associated policy should be defined (i.e. to cover all the operations of the health Board). If the Board is to encompass the operations of other organisations (e.g. because of a shared service agreement with GPs or health and social care partnership) then this needs to be documented and resourced accordingly. Where two separate organisations enter into information sharing agreements both will need to agree on where one or more

ISMS interface (and where any differences in information security policy might lead to differences in risk management).

4.2 **Planning**

Having established scope and contours of the ISMS (where responsibility begins and ends for the Board operations and cognisant of all the interested parties) the Board shall:

- Establish the factors that provide opportunities for the setting up and running of the ISMS and ensure that these are exploited (e.g. mature risk management processes in other areas such as finance or existing ICT staff trained in ITIL or other methodology which use documented processes).
- Establish the risks that may prevent the ISMS from being established, working as intended and being able to achieve continual improvement (e.g. lack of resourcing, cultural issues, an organisational structure that has grown up organically or other factors that would prevent the smooth running of the ISMS machine).
- Consider how far the ISMS needs to work beyond the current information security function (which may be within an eHealth department) but requires interaction with resource elsewhere (information governance, records management etc.)
- Take action to address these risks at executive level.

4.3 Resources

Subsequent to planning and review the Board shall determine and provide the resources needed for the establishment and continual improvement of the ISMS. Each Board shall:

- Be clear that the roles in information security are part of a professional specialist discipline and career home (analogous to ICT, finance, procurement, statistics etc.) and not a generalist NHS administration role.
- As a minimum there should be the designated permanent role of Board Information Security Officer/Manager that encompasses all information risks (not just ‘IT Security’) and is of appropriate grade and standing.
- The appointed person(s) shall be competent and have the necessary specialist training and experience. If this is not possible on Day 1 then the Board SIRO needs to bear the risk and take action to ensure that the necessary competence is acquired as soon as possible (and for this to be documented).

- To provide on-going training and support for information security personnel (i.e. mentoring, resource to gain necessary professional accreditation and qualifications) and for this to be documented.
- To ensure that the personnel are able to participate fully in national-level communities (IG and ISO Fora) and governance structures (e.g. Public Benefit and Privacy Panel) and accreditation work (e.g. Scottish Wide Area Network and services used across Boards) so that national level information risks are addressed in an effective way.

4.4 Staff awareness and communications

The Board shall put in place the means to conduct internal and external communications and awareness relevant to its information security management system. The outcome should be:

- The Board-level information security management policy and associated security objectives should be freely available to all employees, interested parties and the wider public.
- Board level policies and guidance should be available to all staff and interested parties digitally (e.g. via the Intranet).
- There is a form of mandatory induction for all new personnel in regard to Board information security policy and that this is followed.
- There is a process to enable information security updates, advice and other content to be available in a timely manner.

4.5 Documentation

The Board shall hold documented information relating to the design and effective running of its ISMS.

- To be held in a digital format in the Board approved corporate records management system.
- For information relating to the ISMS to be held as one or more discrete functions within a file plan/business classification scheme and managed according to Board records disposal and retention schedules.

- To be easily accessible to persons requiring them to support the smooth running of the ISMS, kept up to date and subject to the security and access permissions commensurate with the sensitivity.

5) Information Risk Assessment

The Board shall identify key assets and their owners and document in a high-level Information Asset Register (IAR) following an agreed national template. Impact on assets needs to be assessed in terms of confidentiality, integrity and availability.

The Board shall use the NHSS Information security risk assessment template and associated process and the national impact levels. This ensures that repeated information security risk assessments produce consistent valid and comparable results across all Boards. In particular:

- The business context must be fully understood prior to assessment.
- Risk owners, and owner of assets must be identified.
- Plausible worst case scenarios and business impact must be understood and documented - according to the national impact scale 1-5 - if overall risks to confidentiality, integrity and availability materialise.
- Vulnerabilities and likelihood must be assessed.
- Overall risk analysis must use the criteria above.
- Analysed risks must be prioritised and summarised into a format that can be easily understood for risk owners to agree subsequent risk treatment.

The Board shall perform information security risk assessments at planned intervals when significant changes are proposed to occur or where recommended in wake of significant information security incidents. Such assessments can be at organisational-level, function-level, project or service specific level.

6) Information Security Risk Treatment

The Board must define and use consistently an information security risk treatment process that:

- Selects appropriate information security risk options for the information risk assessment results.
- Determine all the controls that are necessary to treat the information security options.

- Ensure that all the Reference control objectives and control types cited in ISO-27001 are considered and verify that none have been omitted.
- Ensure that the relevant NHSS National-level mandatory controls and standards are implemented including that of the Scottish Wide Area Network (SWAN).
- Ensure that significant incidents are reported as per national policy so that lessons learned reports feed into treatment plans.
- Ensure that the formal process of NHSS national accreditation is followed in regard to systems/services that require it. It is the responsibility of the Board(s) or other organisations using the systems/services to complete the risk management and accreditation document set for the NHSS-wide accreditor.
- Consider all controls in NHSS National Guidance and implement as far as practicable.
- Consider all the controls cited in ISO-27002 that support ISO-27001.
- Produce a statement of applicability that contains the necessary controls and justification for inclusions, exclusions and whether actually implemented.
- Consider any other control objectives and types over and above those in ISO-27001/2 that have applicability to the Board.
- Formulate an information security risk treatment plan.
- Obtain the risk owners' formal approval of the information security risk treatment plan and acceptance of the residual information security risks. Where non-NHSS organisations and suppliers are involved the Board shall seek agreement on which party is responsible for discharging the different components of the treatment plan.

The Board must implement the agreed information security treatment plans and retain document evidence.

7) Performance evaluation

The Board shall routinely evaluate the information security performance and the effectiveness of the information security management system and be clear about:

- What is to be monitored and measured including security processes, controls and analysis of incidents.
- The methods for evaluating so that there are comparable and reproducible results.
- The personnel who undertake the evaluation and how communicated to the SIRO so that any necessary action can be taken.

8) Internal audit

In addition to the above, the Board shall conduct internal audits at planned intervals that provide information on whether the information security management system conforms to the requirements of ISMS as planned and implemented. The audit shall:

- Work according to an agreed frequency (e.g. annual).
- Define the scope of the audit and criteria.
- Persons carrying out audits are qualified, objective and impartial.
- Such an audit can be incorporated into the internal audit function covering other areas such as finance.

9) Management review and improvement

The SIRO in conjunction with the executive management team should review the Board's information security management system at planned intervals to ensure its continuing suitability and effectiveness. This will be measured against the Board-level and NHSS Information Security Policy Framework. Such review will include consideration of:

- Status of actions from previous management reviews.
- Changes in external and internal issues which are relevant.
- Non-conformities in the ISMS and preventative/corrective actions.
- Monitoring and measurement of results.
- Audit results.
- Results of high-level or significant risk assessment and risk treatment plans.
- Feed-back from interested parties including patients.
- Significant security incident reports at Board and national level.

The outputs of the management review shall include decisions related to continual improvement, opportunities and any changes needed to the information security management system.

The Board, acting through the CEO, SIRO and senior management team will react when nonconformity occurs - over and above any regular audit and management review - and take action to deal with it including change to the information security management system.

The Board recognises the circular nature of the ISMS: to plan, action, check and plan again so as to make continual improvement.