Framework

Information Security Management System

NSWHP_CG_011

1. Purpose

To outline how NSW Health Pathology manages information security risks through developing, implementing and continually improving its Information Security Management System (ISMS) in accordance with the:

a) ISO/IEC 27001 information security management standard and

b) NSW Government Digital Information Security Policy (DISP).

NSW Health Pathology is committed to creating and maintaining practical information security policy and procedure that:

a) Demonstrates and ensures the integrity of its operations and

b) Secures the interests of key internal and external stakeholders.

2. Background

NSW Health Pathology must effectively manage the security of sensitive information and transfer to third parties. This is essential to maintaining the confidentiality and integrity of health data, the reputation of NSW Health Pathology and achieving clinical and corporate safety objectives.

The NSW Government Digital Information Security Policy (DISP) makes it mandatory for all NSW Public Service Agencies to have an Information Security Management System.

NSW Health Pathology must appropriately address all identified risks and must take account of:

a) ISO/IEC 27001:2013 Information security management standard

b) ISO/IEC 27002:2013 Code of practice for information security controls

c) NSW Treasury Internal Audit and Risk Management Policy for the NSW Public Sector TPP09-05

d) ISO 31000 Risk management – Principles and guidelines.

The policy provides a set of minimum information security requirements to manage the risk to NSW Health Pathology's information assets.

3. Scope

This framework is mandatory and applies to all aspects of information security in NSW Health Pathology.

This framework supports the provision of ICT services, infrastructure and applications in NSW Health Pathology's Corporate IT and Forensic and Analytical Science Service (FASS).

NSW GOVERNMENT Health Pathology
T+61 2 4920 4000
F+61 2 4920 4040
NSWPATH-Info@health.nsw.gov.au
45 Watt Street, Level 5
PO Box 846
Newcastle NSW 2300

4. Security Objectives

This framework supports the following security objectives of NSW Health Pathology:

Consistent and Proactive	Implement a consistent and structured approach to information security risk management.
Compliance Management	Comply with legal, regulatory and contractual requirements in relation to information security and the NSW Government's Digital Information Security Policy.
Continuous Improvement	Demonstrate a commitment, and develop a capability, to continually improve information security practices across NSW Health Pathology.
Aligning to Best Practice and Regulations	Implement Information Security controls aligned with industry best practice and regulation to ensure that information security risks are managed within NSW Pathology
Risk Based Approach	Establish manageable and effective security controls commensurate with the risk.
Heightened Awareness	Heighten security awareness of all personnel to ensure their understanding of their relevant information security responsibilities.
Provide Assurance	Provide assurance to stakeholders, customers and interested parties that information security is well managed within NSW Health Pathology and that the transfer of information is done securely.
Security Incident Management	Report and investigate security incidents and weaknesses to minimise any associated impact to delivering core services.
Supplier Management	Establish baselines aligned with the NSW Health Electronic Information Security Policy that all suppliers must comply with and are audited against regularly.

5. ISO 27001 Certification

The scope of the ISO 27001 certification is limited to public facing systems and the sensitive information transferred to third parties from systems and applications that are exclusively managed by Corporate IT or FASS.

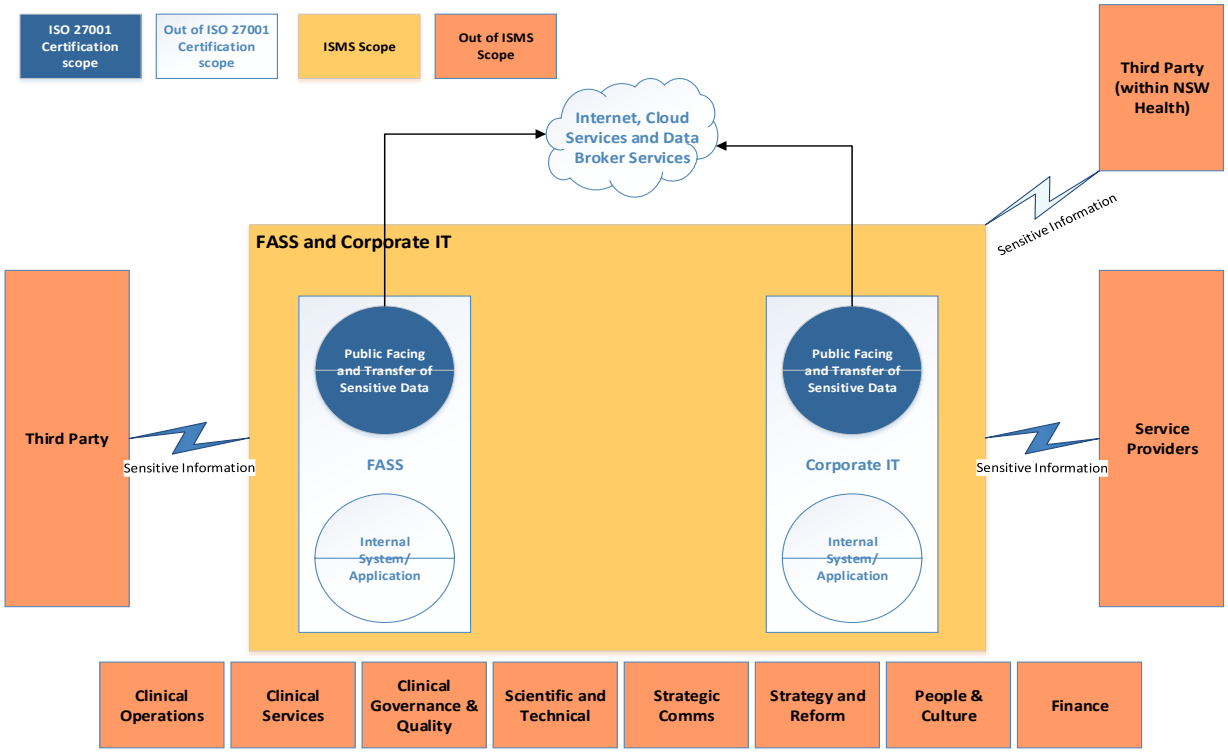
5.1 Physical Boundaries of ISO 27001 Certification

The physical boundaries of ISO 27001 certification are contained within the following locations:

- Corporate IT premises located at:
  - Level 13, Sentral Building 67 Albert Avenue, Chatswood NSW, 2067
  - Level 5, 45 Watt Street, Newcastle NSW, 2300
- FASS premises located at:
  - 480 Weeroona Road, Lidcombe NSW, 2141
  - 50 Parramatta Road, Glebe NSW, 2307
  - John Hunter Hospital Campus, Rosella Close, New Lambton NSW 2305
  - Wollongong Hospital, Level 2 Block A Loftus Street, Wollongong NSW 2500
  - Cameron Building, Macquarie Hospital, Badajoz Road, North Ryde NSW 2113

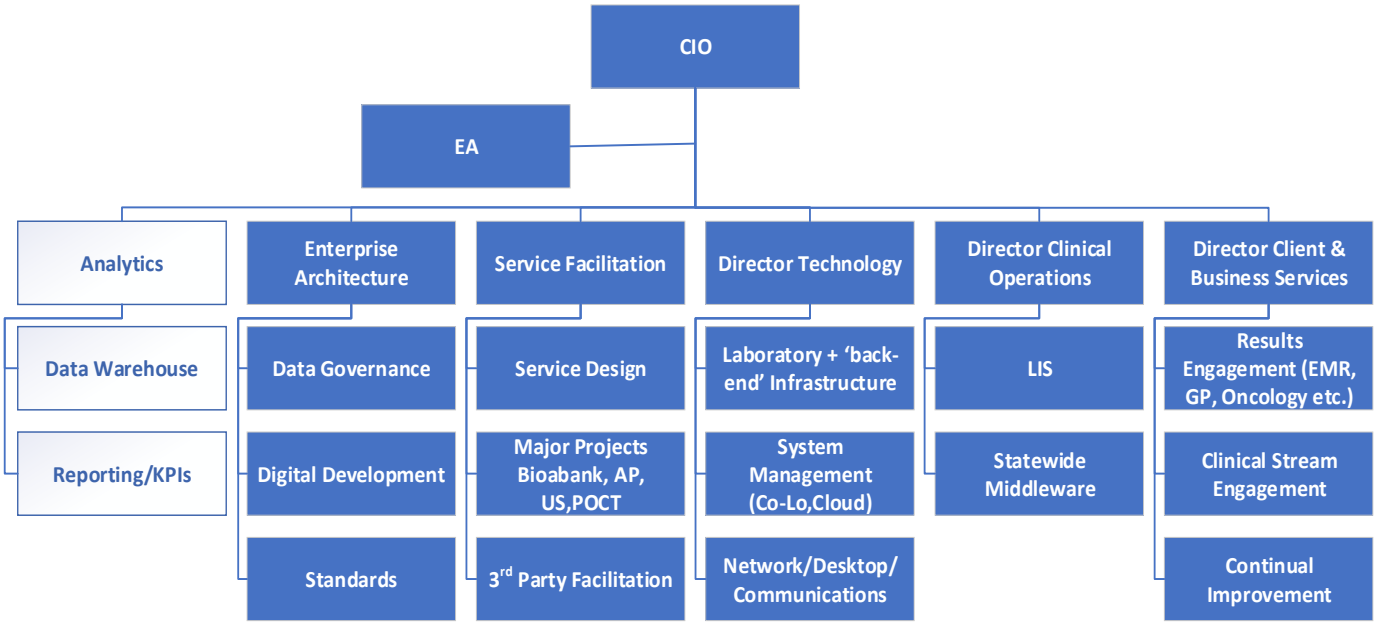
5.2 Logical Boundaries of ISO 27001 Certification

The diagram below represents the logical boundaries of the ISO 27001 certification scope.

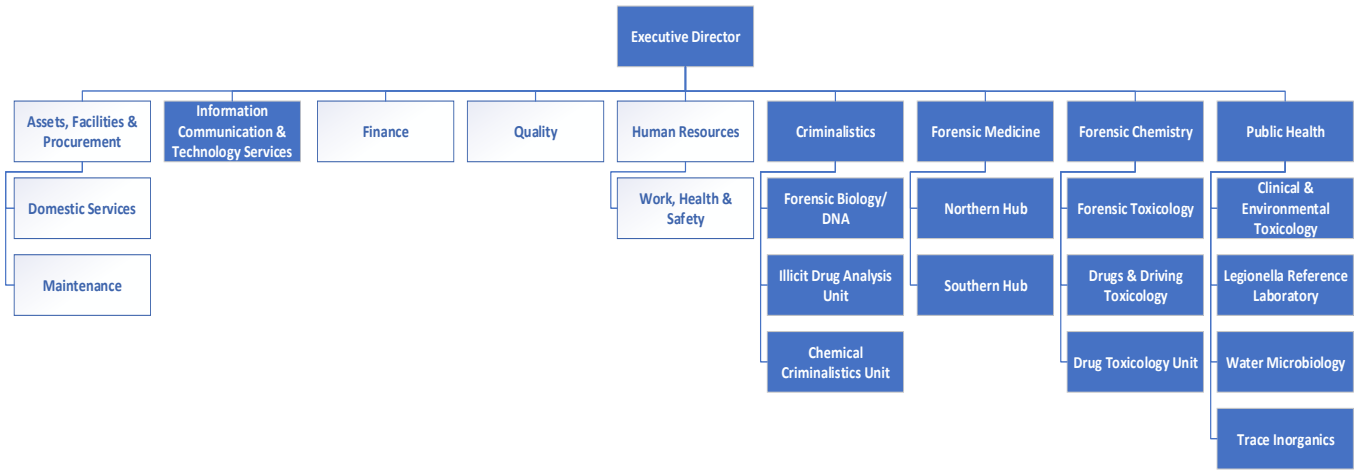


5.2.1 Organisational Boundaries of ISO 27001 Certification

5.2.1.1 Corporate IT Organisation Structure



5.2.1.2 FASS Organisation Structure



5.2.2 Exclusions from ISO 27001 Certification

The ISMS certification does not include:

a) All other ICT services, infrastructure and applications supporting NSW Health Pathology outside the services offered within Corporate IT and FASS
b) Internal systems and applications that are not public facing
c) The transfer of sensitive information with third parties within NSW Health including all agencies and Local Health Districts.

5.2.3 Interested Parties

The ISMS scope considers the following interested parties and their requirements:

Interested Party	Requirements
NSW Government	Confidentiality and integrity of data is in line with NSW government requirements. Assurance that information will not be disclosed without appropriate authority.
NSW Health and eHealth	NSW Health Pathology consumes technology services and may have access to sensitive or classified information. NSW Health Pathology also provides sensitive information to these parties.
State and Commonwealth Government Health, Justice, NSW Police, Australian Federal Police	Maintain the confidentiality and integrity of data in line with State Government requirements. Maintain the confidentiality and integrity of data in line with Commonwealth Government requirements.
Public sector employees	Assurance that personally identifiable information managed is secure, accurate, and will not be disclosed without appropriate authority.
Regulatory authorities	Confidentiality and integrity of data managed by NSW Health Pathology.
Governing boards of statutory authorities e.g. Cancer Institute of NSW	Maintain the confidentiality and integrity of data in line with State Government requirements.
Providers of essential services	Assurance that information provided in confidence to NSW Health Pathology is secure and will not be disclosed without appropriate authority.
The community	Assurance that personal information is secure and will not be disclosed without appropriate authority. Confidence that NSW Health Pathology, on behalf of the government, will appropriately manage internal and external information in its custody for the benefit of the NSW public.
Other bodies, Educational Institutions, Hospitals, Forensic Medicine Victoria	Confidentiality and integrity of data managed by NSW Health Pathology.

5.2.4 Internal and External Impacts

NSW Health Pathology recognises that the following internal and external issues potentially impact the achievement of the information security objectives:

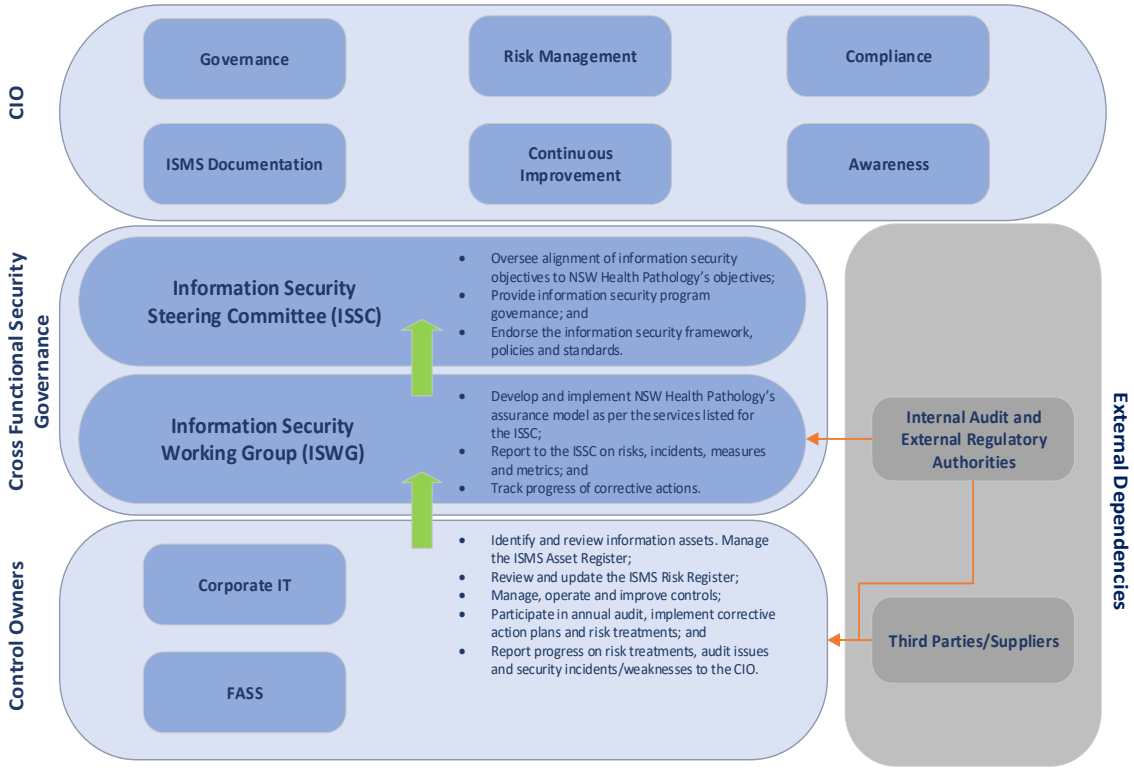
a) The breadth and diversity of the organisation and its geographical distribution
b) A strong reliance on third parties and the difficulties associated with controlling how third parties manage NSW Health Pathology sensitive information
c) Low level of information security awareness within the organisation
d) The need to comply with all relevant NSW Government and NSW Health and Justice policy
e) Changes in the political environment that influence and impact our strategic direction
f) Maintaining and managing a significant amount of infrastructure over which it does not necessarily have sufficient levels of visibility and control.

6. Governance

The governance structure ensures a common understanding of information security issues:

a) The implementation of the information security program is overseen by the Information Security Steering Committee (ISSC)
b) The Information Security Working Group (ISWG) is responsible for the functioning of the ISMS
c) The Chief Information Officer is the owner of the ISMS.

The interfaces and dependencies of the ISMS governance structure are depicted below:



7. Legal and Regulatory Requirements

The services are delivered within the legal and regulatory framework documented in the NSW Health Pathology Legislative Compliance Register.

NSW Health Pathology information security policies, standards, practices, procedures and guidelines support the ISMS to facilitate the implementation, compliance and effectiveness of this framework.

8. Roles and Responsibilities

The following table summarises groups, security functions and relevant security competencies expected for each group.

8.1 Chief Information Officer (ISMS Owner)

The Chief Information Officer shall act as the owner of the ISMS and is responsible for the successful operation of the ISMS throughout NSW Health Pathology.

The ISMS owner is responsible for the following activities:

a) Act as the owner of the ISMS
b) Be responsible for the successful operation of the ISMS throughout NSW Health Pathology
c) Provide information security programs visibility as needed to the Strategic Leadership Team

The ISMS Owner must have the following competencies/authority:

a) Good understanding of ISMS concepts and requirements
b) Good understanding of the organisation and strategic objectives
c) Authority to escalate assignment of resources
d) Good understanding of NSWHP Enterprise Risk Management Procedure

8.2 Information Security Steering Committee (ISSC)

It is the responsibility of the Information Security Steering Committee (ISSC) to:

a) Champion an effective and sustainable approach to managing information security risks throughout NSW Health Pathology
b) Ensure appropriate organisational commitment to information security activities related to the ISMS scope
c) Review results of ISMS effectiveness
d) Review results of ISMS effectiveness reporting as provided by the ISWG including incidents, metrics, KPIs and audits
e) Escalate major issues to top management and the ISMS owner as necessary
f) Facilitate provision of sufficient resources and training to ensure effective ISMS implementation
g) Review and approve ISWG recommendations on major security incidents, risks and risk treatment plans, adequacy of response and controls, security audits, and corrective actions and improvements taken

Membership of the ISSC is defined as:

a) Executive Director, Clinical Operations
b) Executive Director, Clinical Services
c) Executive Director, FASS
d) Chief Information Officer, Corporate IT
e) Director Information Communications Technology, FASS

Members of the ISSC must have the following competencies/authority:

a) Good understanding of ISMS concepts and requirements
b) Good understanding of the organisation and strategic objectives
c) Authority to escalate assignment of resources
d) Good understanding of NSWHP Enterprise Risk Management Procedure

8.3 Information Security Working Group (ISWG)

The role of the ISWG is to act as the coordinator and adviser for all information security aspects in relation to the scope of the ISMS. Its responsibilities include:

a) Responding to the direction of the ISMS owner and ISSC
b) Implementing the ISMS
c) Meeting at least monthly and maintaining appropriate meeting minutes
d) Ensuring the development and maintenance of the policies, procedures, work instructions and other operational documents to ensure compliance with this framework
e) Reviewing and endorsing core ISMS documentation including procedures
f) Promoting this framework and ensuring employees, contractors and interested parties are aware of it
g) Evaluating the risks and adequacy of controls for existing and new assets, as well as changes to the existing assets, applications, software and hardware
h) Monitoring changes to services or deliverables for interested parties and re-assessing any associated risks for such changes
i) Reviewing outcomes from information security incidents and associated corrective actions and improvements
j) Reviewing security weaknesses and facilitating improvements to remediate information security risks identified by the organisational risk management processes
k) Regularly reviewing security risks and associated controls
l) Escalating any issues, as necessary, to top management, the ISSC or the ISMS owner
m) Ensuring ISMS internal audits are carried out as per a defined schedule
n) Evaluating the results of internal and external audits and facilitating the required remedial actions
o) Communicating and providing guidance on implementation of information security policies, procedures, guidelines and other operational documents

Membership of the ISWG is defined as:

a) Chief Information Officer, Corporate IT
b) IT Service Manager, Corporate IT

c) Enterprise Architect, Corporate IT
d) Senior Analyst, FASS
e) Representative from eHealth.

Membership may change based on operational requirements and anyone may be invited to attend an ISWG meeting as necessary.

Members of the ISWG must have the following competencies/authority:

a) Strong understanding of ISMS concepts and requirements
b) Authority to approve core ISMS operational documents such as the ISMS Records Register, ISO 27001 Internal Audit Plan, ISMS Security Calendar, ISMS Measures and Metrics
c) Authority to provide the respective branches with advice to implement security controls.

8.4 ISMS Administrator

A representative from Corporate IT is responsible for the overall co-ordination of ISMS activities including:

a) Organising the ISWG
b) Maintaining ISMS documentation
c) Coordinating the annual risk assessment
d) Ensuring the activities documented in the ISMS calendar are scheduled, updated and performed
e) Monitoring the progress on agreed activities
f) Escalating any issues, as necessary, to the ISMS owner
g) Highlighting major information security incidents to the ISWG
h) Responding to the direction of the ISMS owner and the ISWG
i) Coordinating with external security vendors and specialists as necessary for expert advice
j) Reporting on various aspects of the ISMS including, but not limited to, security metrics, outstanding issues, and progress of the actions in the risk treatment plans

The ISMS Administrator must have the following competencies:

a) At least five years of operational experience in information security
b) Strong working understanding of ISO 27001
c) ISO 27001 Implementer training (desirable)
d) Good understanding of NSWHP Enterprise Risk Management Procedure

8.5 Risk Owners

Risk owners are responsible for managing risk within their level of delegation, implementing risk treatments for risks within their areas of responsibility and accepting residual risks.

Risk Owners must have the following competencies/authority:

a) Basic understanding of the ISMS
b) Authority to approve and accept risks

8.6 Control Owners / Operators

Control owners / operators are responsible for managing, operating and improving controls. They must have some understanding of ISMS concepts and requirements.

8.7 Treatment Owners

Treatment owners are responsible for progressing the treatments outlined in the ISMS Incidents and Actions Register.

Treatment Owners must have the following competencies:

a) Good understanding of ISMS concepts and requirements
b) Good understanding of NSWHP Enterprise Risk Management Procedure and responsibilities as nominated treatment owners

8.8 All Personnel (employees, contractors and third parties)

All personnel involved in the ISMS are responsible for:

a) Complying with the ISMS together with any supporting policies, standards and procedures
b) Complying with all security controls established
c) Reporting security breaches and taking necessary corrective actions
d) Taking appropriate actions to protect information assets
e) Using the information processing resources only as authorised and intended by the system owner.

9. RASCI Matrix

The RASCI functional responsibilities within the framework are documented below.

	IS Strategy	IS Program Management	IS Metrics & Reporting	Information Security Policies	IS Risk Management	Organisation of Information Security	Human Resource Security	Security Awareness Training	Asset Management	Information Classification Labelling and Handling	Identity and Access	Cryptographic Key Management	Physical and Environmental	Operations Security	Change Management	Communications Security	System Acquisition, Development and Maintenance	Supplier Relationships	Security Incident Management	Business Continuity	Legal & Regulatory Compliance
ISMS Owner (SRO)	R	A	A	R	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Information Security Steering Committee	A	R	I	A	I			S							I				I	I	I
Information Security Working Group	S	S	I	S	S			S	S										S	I	I
ISMS Co-ordinator	S	S	S	S	S			S													
FASS - Control Owners	C	S	R	S	R	R	C	R	R	R	R	R	C	R	R	R	R	R	R	R	R
Corporate IT – Control Owners	C	S	R	S	R	R	C	R	R	R	R	R	R	C	R	C	R	R	R	R	R
Pathology IT – Control Owners	C	S	R	S	R	R	C	R	R	R	R	R	R	C	R	C	R	R	R	R	R
Risk Owners	I	I	I	I	R																
All Personnel	I	I		I	I			I		I			I					I	I		I

Legend

R – Responsible A – Accountable S – Supportive C – Consulted I – Informed

Refer to Appendix A for a full description of the above assignments.

10. Monitoring and Measurement

The performance and effectiveness of the ISMS will be monitored and measured against the security objectives as per the documented and defined Information Security Measures and Metrics and ICT Assurance Map.

11. Improvements

NSW Health Pathology seeks to continuously improve the ISMS by ensuring:

a) Identified nonconformities are recorded in the Incident Management System (IMS)
b) Major security incidents, that is, those that require post incident review and the associated corrective actions are recorded in the IMS
c) Suggested improvements to the framework are captured in the IMS
d) Activities in the ISMS Security Calendar are executed in a timely manner.

12. Evaluation

In addition to the ongoing evaluation by the ISSC and ISWG, the ISWG will undertake an annual evaluation of the operations of the ISMS as outlined in the ISMS Security Calendar managed by the ISWG. The evaluation will:

a) Assess the effectiveness and practicality of the ISMS and its ability to meet organisational objectives.
b) Consider the suitability and effectiveness of the existing policies. Modifications to the policies will be tasked to the relevant personnel and documented in the IMS for tracking and management.
c) Involve an analysis of the following:
    i. The effects on NSW Health Pathology of any changes to ISO 27001, DISP and relevant legislation
    ii. The effects of planned business changes on the ISMS
    iii. The effect of business changes on NSW Health Pathology's policies, targets and objectives
    iv. ISMS audit reports and the effectiveness of the system
    v. ISMS documentation and structure
    vi. The status of corrective actions and improvements as recorded in ISWG meetings
    vii. Results of risk assessments and status of risk treatment plan
    viii. Results from effectiveness measures
    ix. Feedback from interested parties, including feedback or complaints from interested parties
    x. Review of techniques, products or procedures which could be used to improve the ISMS, evaluating emerging better practice and guidance
    xi. The follow up actions of previous management reviews
    xii. Observations/recommendations following incidents
    xiii. The extent to which targets and objectives have been met
    xiv. Results of education and awareness program
    xv. Levels of residual risk and acceptable risk.

13. Legal and Policy Framework

NSW Classification and Labelling Guidelines
NSW Government Digital Information Security Policy OFS-2015-05
NSW Health Code of Conduct PD2015_049 (Section 4.5: maintain security of confidential and/or sensitive information)
NSW Health Communications – Use and Management of Misuse of NSW Health Communications Systems PD2009_076
NSW Health Electronic Information Security Policy Directive PD2013_033
NSW Health Privacy Manual for Health Information
ISO/IEC 27001:2013 Information security management standard
ISO/IEC 27002:2013 Code of practice for information security controls

14. Review

This framework will be reviewed annually in accordance with the NSW Government DISP.

The next review date is 31 December 2020.

15. Risk Statement

Risk Statement	An ISMS outlines how NSW Health Pathology manages information security risks and improves decision-making to improve our performance by proactively identifying, understanding and managing our information security risk to meet our ISMS business objectives.
Risk Category	Leadership and Management

16. Further Information

For further information, please contact:

Chief Information Officer	Position: Chief Information Officer
	Name: James Patterson
	Telephone: 02 4920 4043
	Email: James.Patterson@health.nsw.gov.au

17. Version History

The approval and amendment history for this document must be listed in the following table:

Version No	Effective Date	Approved By	Approval Date	Policy Author	Risk Rating	Sections Modified
V1.0	18/10/18	Transformation Governance Committee	10/10/18	Chief Information Officer	Medium	New Framework

Appendix A: RASCI Matrix

Term	Label	Description
Responsible	**R**	Responsible – the group or individual who owns the functional area.
Accountable	**A**	To whom "R" is Accountable - who must sign off (Approve) on the activities before they are effective.
Supportive	**S**	Group or individual can be supportive and may provide resources or can play a supporting role in implementation.
Consulted	**C**	Group or individual that should be Consulted. This group/individual has information and/or capability necessary to perform the activity.
Informed	**I**	Group or individual that should be Informed. This group must be notified of results but need not be consulted.