Isle of Man Government
Reiltys Ellan Vannin

Health and Care Transformation Programme

Data, Information and Knowledge Project

Information Governance Strategy

Version: 1.0
Date: September 2020
Status: Approved

Contents

1. Introduction

The key driver for this information governance strategy is the publication of the Independent Health and Social Care Review Final Report[1] (Report). The Report includes 26 recommendations to be implemented to achieve a sustainable, high quality, integrated health and social care system on the Isle of Man.

The Health and Social Care Transformation Programme is tasked with implementing the recommendations and is underpinned by 14 projects.[2] This strategy seeks to provide direction on information governance to the Public Health Directorate, Department of Health and Social Care (DHSC) and Manx Care. Information governance is being led by the Data, Information and Knowledge Project.

The objective of this information governance strategy is to help the above-mentioned organisations improve compliance with the Data Protection Act 2018 (the Applied GDPR), data security, data quality and adopt information governance best practices when they process personal data and other confidential information of service users.

The key recommendations related to information governance in the Report are as follows:

"**Recommendation 5:** A statutory duty of care (applicable to organisations and the individuals who deliver health or care services) should be agreed, implemented and maintained alongside the delivery of high value clinical governance, underpinned by legislation where necessary. The new statutory duty of care would include:

- A duty of confidentiality;
- A duty to share information where appropriate to enable the delivery of safe optimal care; and
- A duty of candour – a responsibility to disclose where breaches of safety standards or harm to individuals have occurred."

"**Recommendation 21:** Ensure data sharing protocols and arrangements are reviewed, agreed and implemented in accordance with the Information Commissioner's regulations and guidance."

"**Recommendation 24:** The systematic capture of accurate data should be a priority for the Island's health and care services."

"**Recommendation 25:** A fit for purpose workforce model needs to be developed to reflect the emerging needs of the new model of care. It should maximise the potential skills available within the workforce as well as the opportunity to recruit and retain high quality professionals. It will then increase the attractiveness of the Isle of Man as a career destination."

The recommendations reinforce the importance of:

- Understanding data flows, identifying data protection obligations which arise and implementing legally binding contracts, such as, data sharing agreements (controller to controller relationships) or data processing agreements (controller to processor relationships) to protect personal data.
- Processing data in line with the accuracy principle set out in the Data Protection Act 2018 (Applied GDPR) to improve data quality.

[1] https://www.gov.im/media/1365879/independent-health-and-social-care-review-final-report.pdf
[2] An overview of the Transformation Programme projects can be found in Appendix A.

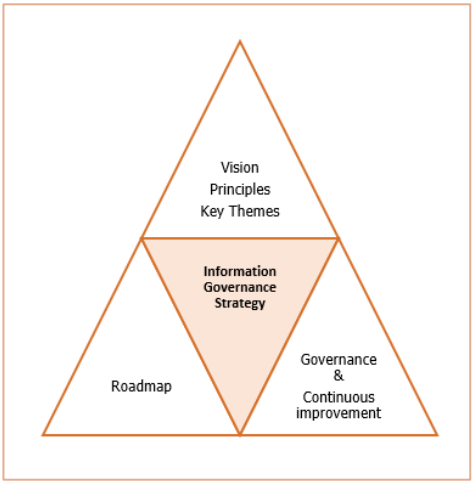
- Sharing data lawfully within the parameters of the Data Protection Act 2018 (The Applied GDPR) and duty of confidentiality. While secondary uses of data are essential for running a safe, efficient and equitable health service, service users' confidentiality must be protected when data about them are used for secondary purposes. Data that do not identify service users must be used for secondary purposes, otherwise the consent of the service users must be obtained.
- Seeking guidance from the Information Commissioner's Office (ICO) and consulting with the ICO as part of data protection by design at the beginning of new data processing initiatives, as opposed to after the commencement of the initiatives, especially in 'high risk' processing; implementing relevant guidance and codes issued by the ICO; having regular contact with the ICO.
- Training the workforce on information governance to improve compliance and to protect service users' data as the weakest point of any organisation's data security is usually its own people.

This information governance strategy seeks to address the recommendations by setting out the following:

(a) the vision for information governance, the guiding information governance principles and the key themes, such as data protection, information security and confidentiality. Together, these will drive the direction for information governance within the Public Health Directorate, DHSC and Manx Care.

(b) a long-term and short-term roadmap of the key steps that will be taken to implement the strategy.

(c) the monitoring of information governance initiatives such that they can be measured and improved.



The Transformation Programme and its constituent projects covers all aspects of an integrated health and social care system, applying equally to:

- social care as much as physical and mental health care
- wellness and prevention as much as treatment and cure
- all people, whether they are a baby, child, young person, adult or an old person.

To reflect the broad reach of this strategy, it refers throughout to health and social care. References to "service users" should be taken as meaning patients and service users.

This strategy is flexible and all-encompassing to enable the organisations in scope to meet their respective compliance requirements.

The strategy has been updated following a first round of consultation with stakeholders identified in the Stakeholders Register[3]. This paper will now be submitted to the Information Commissioner for his insight and feedback. The strategy will finally be submitted to the Public Health Directorate Board, the DHSC Board and Transformation Board for approval.

[3] See Stakeholders Register at page 20

2. The vision for information governance

Our vision for a robust and effective information governance strategy is one that achieves the following:

- ✓ Improved collaboration by fostering an environment of information sharing and ensuring information reaches the right people at the right time.
- ✓ Makes the best use of information the health and social care system holds to provide the best possible service and care to service users.
- ✓ Protects information to ensure that the confidentiality and data protection rights of service users are upheld as per the law.
- ✓ Provides information confidence and assurance, essentially through information integrity, accuracy and quality.
- ✓ Uses data lawfully to drive decisions that can lead to improvement and positive changes across the health and social care system and caters for high quality analytics.
- ✓ Establishes a governance structure which enables the organisations to achieve 'accountability' (i.e., measures in place to demonstrate compliance with the Data Protection 2018 (Applied GDPR)).
- ✓ Is supported by policies, practical procedures and processes to implement and embed the legislative and regulatory requirements.

The organisations supported by this strategy are:

The Public Health Directorate: Its centrally involved in the development, coordination and application of policies that affects more than one department. It also has a role in ensuring that the Government works better, by promoting reform and striving to improve the provision of services.

The Department of Health and Social Care (DHSC): It has responsibilities to Tynwald (parliament) for health and social care services for the people of the Isle of Man.

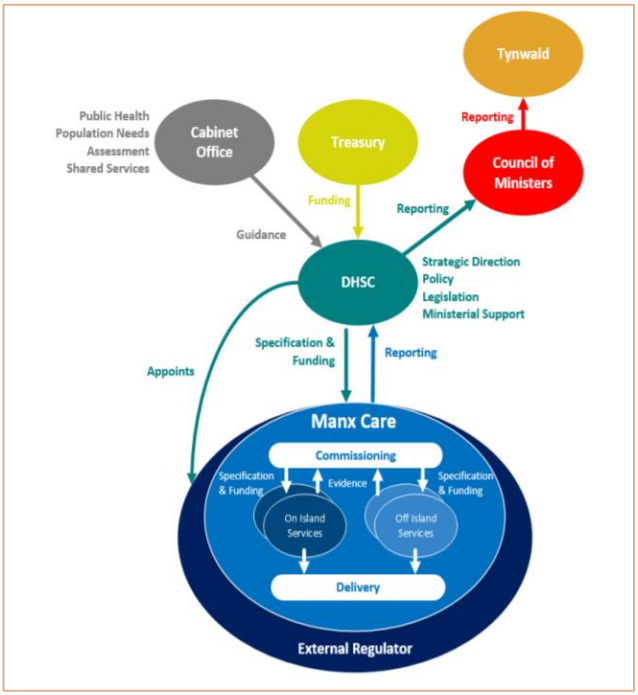


Figure 1: System Target Operating Model as of 27th August 2020

Manx Care: The new arms-length organisation responsible for the commissioning of health and social care services[4] for the people of the Isle of Man.

References to "organisation(s)" in this paper should be taken as meaning the Public Health Directorate, DHSC and Manx Care, unless specifically named.

3. Information governance & the key principles

Service users entrust their information to the health and care system to receive care. While information and intelligence are important to improve health and care services, the processing of personal and sensitive information creates distinct requirements for privacy and data protection, information security, confidentiality.

Information governance aims to balance the security of health and care information with the facility to use and optimise information. The key legislation that makes up information governance is the EU General Data Protection Regulation, implemented in the Isle of Man as Data Protection Act 2018 (the Applied GDPR).

It sets out the general principles for data protection which should lie at the heart of the organisations' approach to processing data.

The general principles are as follows:

- Lawfulness, fairness and transparency: The organisations will identify valid grounds known as lawful basis for collecting and using data. The organisations will not use the data in a way that is detrimental, unexpected or misleading to service users. The organisations will be clear, open, honest with service users about how their data is used.
- Purpose limitation: The organisations will be clear about their purposes for processing from the start as much as possible. They will record their purposes as part of their documentation obligations and specify them in privacy notices. They will only use the information for a new purpose when this is compatible with the original purpose, they get consent or when they have a clear obligation or function set out in law.
- Data minimisation: The organisations will ensure that personal data being processed is adequate (sufficient to fulfil purposes identified), relevant (has a rational link to purposes identified) and limited to what is necessary for the purposes identified.

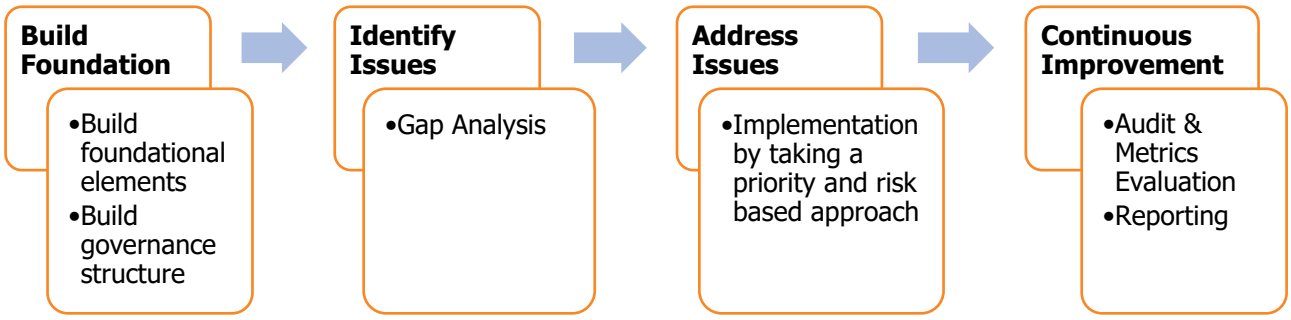
[4] The services listed in the draft mandate (dated August 2020) are: primary care, acute healthcare, community health, mental health, social care, specialist care, screening and immunisation, private health and other services

- Accuracy: The organisations will take the all reasonable steps to ensure that the personal data they hold is not incorrect or misleading.
- Storage limitation: The organisations will not keep personal data no longer than they need it. They will document how long they need personal data and be able to justify and document reason for retention. They will set out policy detailing retention periods to comply with documentation requirements. They will also periodically review the data they hold, erase or anonymise it when they no longer need it.
- Integrity and confidentiality: The organisations will ensure that they have appropriate security measures in place to protect the personal data they hold.
- Accountability: The organisations will take responsibility for what they do with personal data and how they comply with the above principles, such as having appropriate measures and records in place to be able to demonstrate their compliance. This is essential to build trust with service users and mitigate enforcement actions.

4. Implementation of information governance

Accountability is one of the data protection principles. It makes the organisations responsible for complying with the Data Protection Act 2018 (The Applied GDPR) and it requires them to demonstrate their compliance. Each organisation will implement a demonstrable privacy and data protection accountability framework to embed their accountability measures and improve their privacy culture.

The following methodology will be followed to deliver the information governance strategy:



- **Build foundation and identify issues**: Effective governance and accountability will be designed and established. A gap analysis of each organisation's information governance practices will be conducted to identify their data processing risks. Data flows will be identified and documented in records of processing activities.

- **Address issues through implementation**: Data processing obligations arising from data flows will be identified and measures will be implemented to address obligations requirements by taking a risk-based approach.
- **Continuous improvement**: Measures for monitoring, evaluating and reporting on compliance and control effectiveness will be defined and implemented to improve information governance maturity as accountability obligations are ongoing.

Twelve core privacy management control categories (PMC) will be defined for the organisations in scope to achieve compliance with the Data Protection Act 2018 (The Applied GDPR), namely:

PMC 1: Establish a governance structure

- A fundamental building block for accountability is strong leadership, key capabilities, clear reporting lines, effective information flows and oversight.
- Please refer to Appendix B for more information on key capabilities and oversight groups.

PMC 2: Identify data flows and build records of processing activities (ROPA)

- An information audit will be carried to find out what personal data is being held.
- A ROPA will be built based on the data mapping exercise.
- The ROPA will contain all the relevant requirements of Art 30. of the Data Protection Act 2018 (Applied GDPR), i.e., different functions of the organisations, purpose of processing, lawful basis for processing, categories of personal data being processed, different operations on data, recipients, the geographical location of data, the data protection obligations of the organisations.

PMC 3: Identify data sharing and implement contracts

- Data sharing policies and procedures will be implemented/reviewed to make sure that the organisations appropriately manage data sharing decisions, e.g. through Data Protection Impact Assessments (DPIAs).
- Appropriate data sharing agreements with parties with whom the organisations routinely share personal data will be reviewed/implemented.
- Procedures for managing controller-processor relationships will be reviewed/implemented (controller-processor contract requirements, processor due diligence checks, processor contract compliance reviews).

PMC 4: Provide meaningful privacy notices to achieve transparency

- Transparency is fundamental to a data protection by design approach.
- Updated privacy notices will be provided at data collection points. The aim of the information governance programme will be to keep privacy notices accurate, up to date and effective.
- Needs for tools which support transparency and control will be identified, such as, dashboards, just-in-time notices, user friendly options.

PMC 5: Embed privacy into operations through policies, broken down into processes

- Policies and processes provide staff with direction to understand their role and responsibilities regarding information governance.
- A policy framework which stems from strategic business planning for information governance and is endorsed by Leadership will be identified, designed and implemented.

PMC 6: Establish and maintain information governance awareness and training programme

- An information governance training programme which reflects operational responsibilities will be designed.
- More information can be found in Appendix C.

PMC 7: Establish and maintain records management and security

- Good records management supports good information governance while security is a legal data protection requirement.
- Standards will be implemented for the creation, location and retrieval of records.
- Appropriate retention and disposal policy and schedules outlining storage periods for personal data processed will be implemented.
- An information asset register that records asset, systems and applications used processing or storing personal data will be built.
- An information security assessment will be conducted to meet Art 32[5] of the Applied GDPR.
- More information can be found in Appendix D.

PMC 8: Respond to service users' rights requests

[5] Art 32 of the Applied GDPR requires controllers and processors to implement appropriate and organisational measures to ensure a level of security appropriate to the risks they face and one of ways to do so is by putting in place "a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security of processing".

- Data protection law empowers individuals and give them greater control over their personal data through several rights and they will need to be facilitated effectively.
- Procedures to facilitate service users' data protection rights will be reviewed/implemented.

PMC 9: Monitor new operational practices

- The need to identify, assess and manage privacy risks is an integral part of accountability.
- Data protection by design will be integrated into data processing operations by identifying appropriate policies, procedures and measures to manage information risks (such as DPIA policy, information risk policy, risk register)
- Relevant teams will be trained on DPIA.
- An end to end DPIA operational process will be implemented to ensure that the core steps[6] involved in undertaking a DPIA are followed through.

PMC 10: Manage personal data breaches

- The organisations need to be able to detect, investigate, risk-assess and record any breaches through appropriate procedures (training, resources, data breach management and response procedures, log).
- Practical ways for raising incidents will be implemented.

PMC 11: Monitor data handling practices and achieve information governance maturity

- Organisational targets for information governance will need to be set and assessed through KPIs.
- For the continuous improvement of the information governance programme, audits of the organisations will need to be conducted. The maturity level will be tracked following the methodology in Appendix E.
- Systematic documentation to demonstrate compliance and accountability will be conducted.
- Relevant certifications or accreditations (such as ISO27001, CIS Critical Security Controls, Cyber Essentials) for demonstrating compliance will be identified during the process.

PMC 12: Track external environment (fines, regulatory updates)

[6] The core steps are identifying the need for a DPIA; describing the processing; consultations with relevant stakeholders such as the ICO, service users, DPO; risks identification and mitigations; sign off by the DPO; implementation and actions closure.

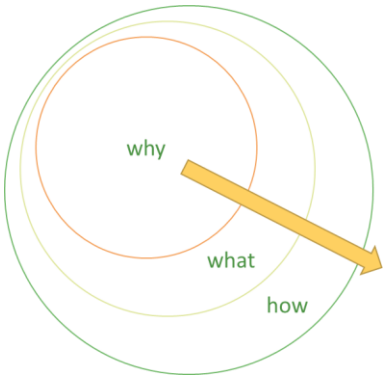
- The DPO(s) will closely monitor ongoing privacy compliance requirements and provide updates to their Information Governance Steering Committee.

5. Tools to support the information governance strategy

The information governance programme will be supported by information governance-enabling tools to support the implementation of processes for privacy and data protection, security, control, third party risk management (for example, identity and access management, mobile device management, role-based control management, vulnerability scanning, penetration testing, encryption). The tools will also offer documentation facilities to help controllers comply with the 'accountability' principle. The relevant needs will be identified during the operational assessment and budgetary constraints will be factored into a strategic roadmap for implementation.

6. Information governance roadmap

Strategy production and execution progresses through three stages:



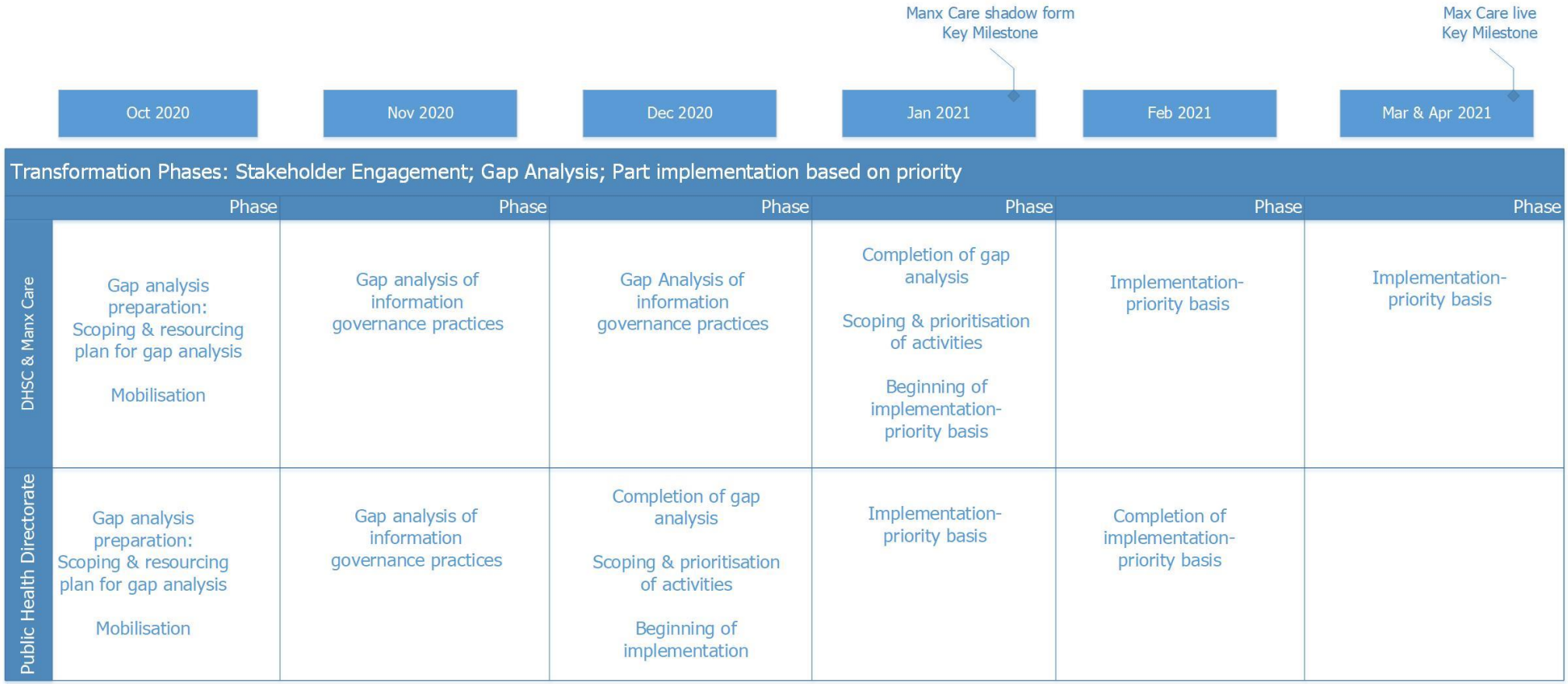
'Why' is concerned with the reasons we want to enact for the particular change and the identified needs. It sets out the vision we want to achieve. 'What' stands for what should a good information governance programme look like and 'how' stands for how do we get there, the more granular and actionable activities that need to happen at the operational level to achieve the 'what'.

The below roadmaps address the 'how' and are an indicative:

(1) short term of view of the activities that will be undertaken in the next 7 months.

(2) long term view of the activities that will be undertaken to achieve the information governance vision and maturity.

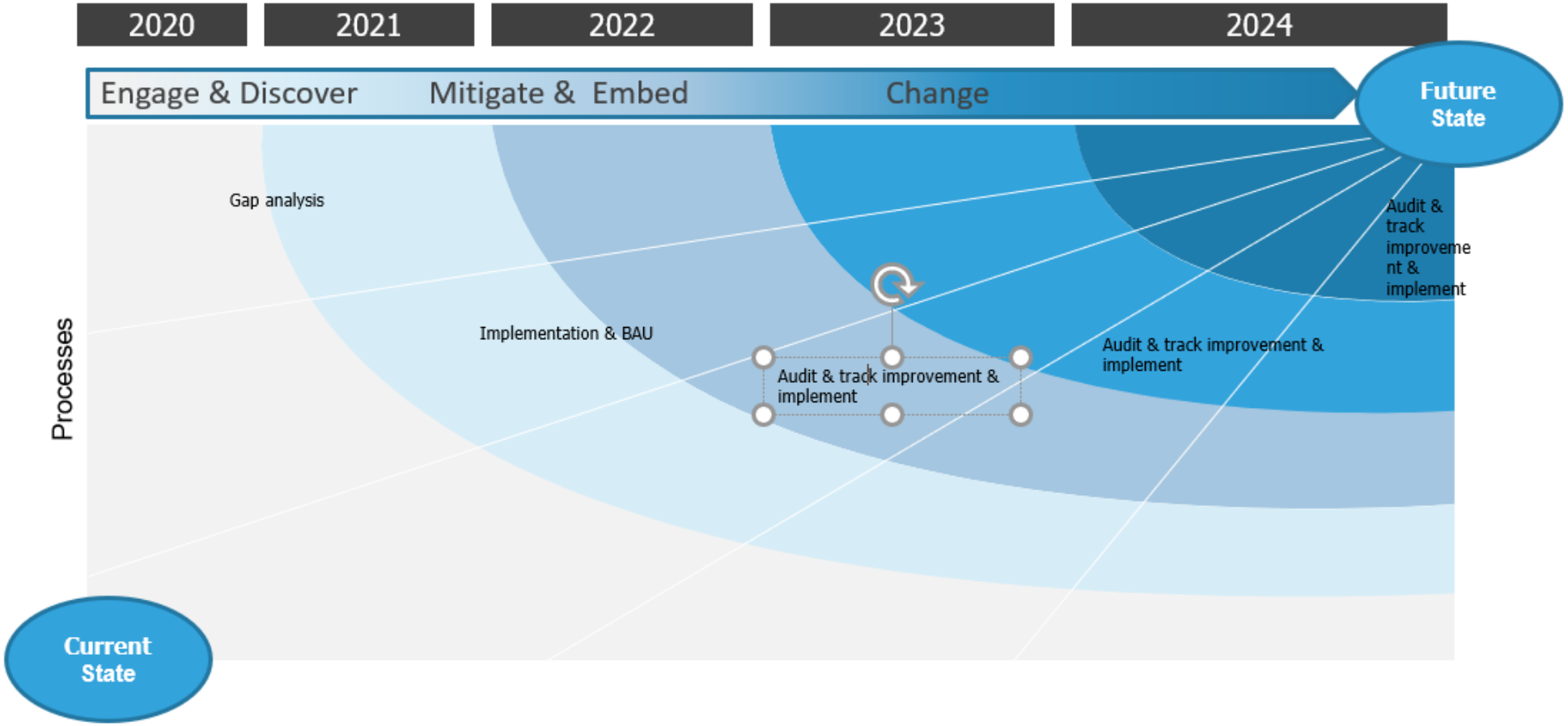
(1) Short term view:



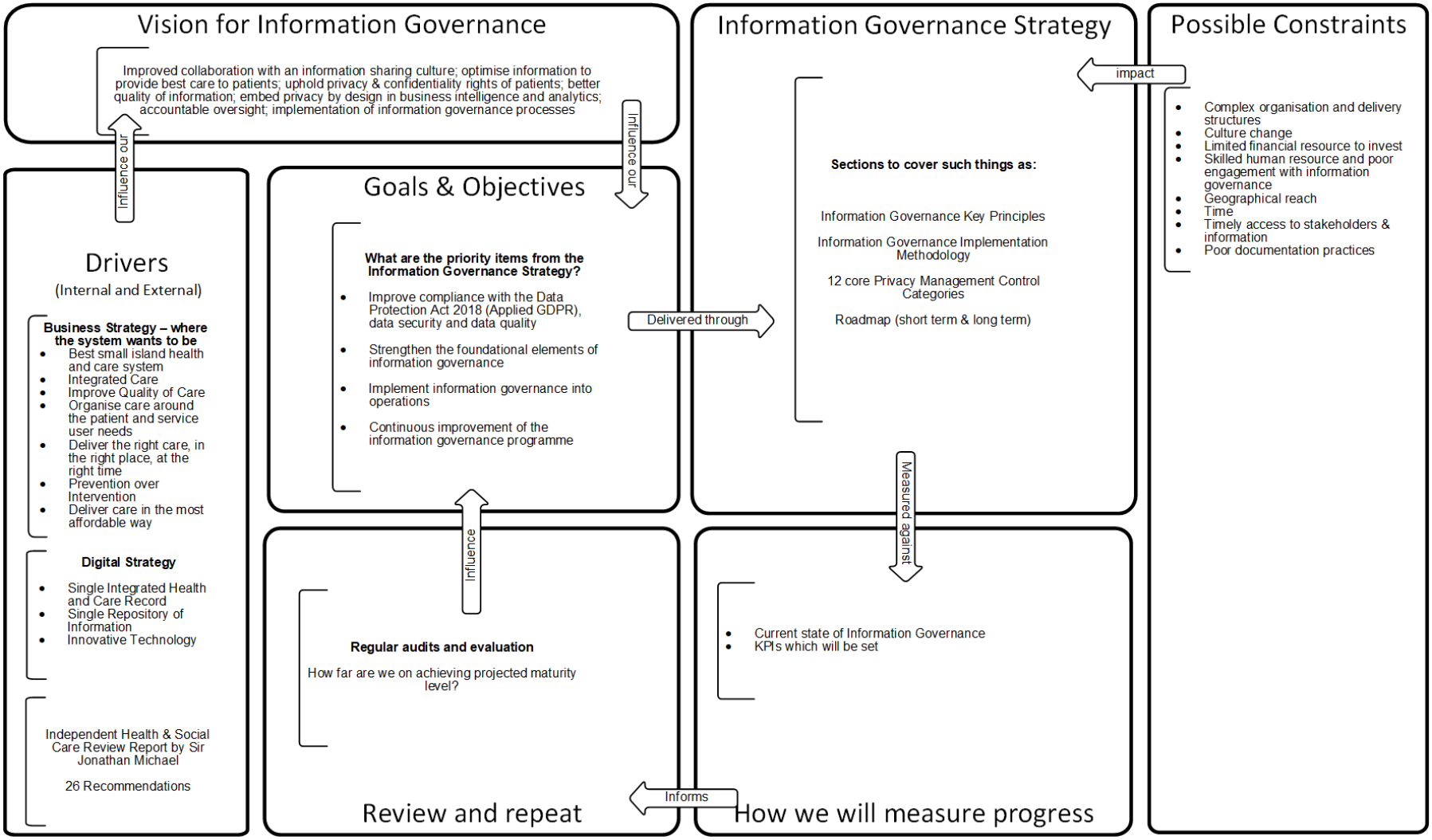
The key deliverables for the period are:

- Risk register, ROPA, Information Asset Register, Data Sharing Agreements/Data Processing Agreements.

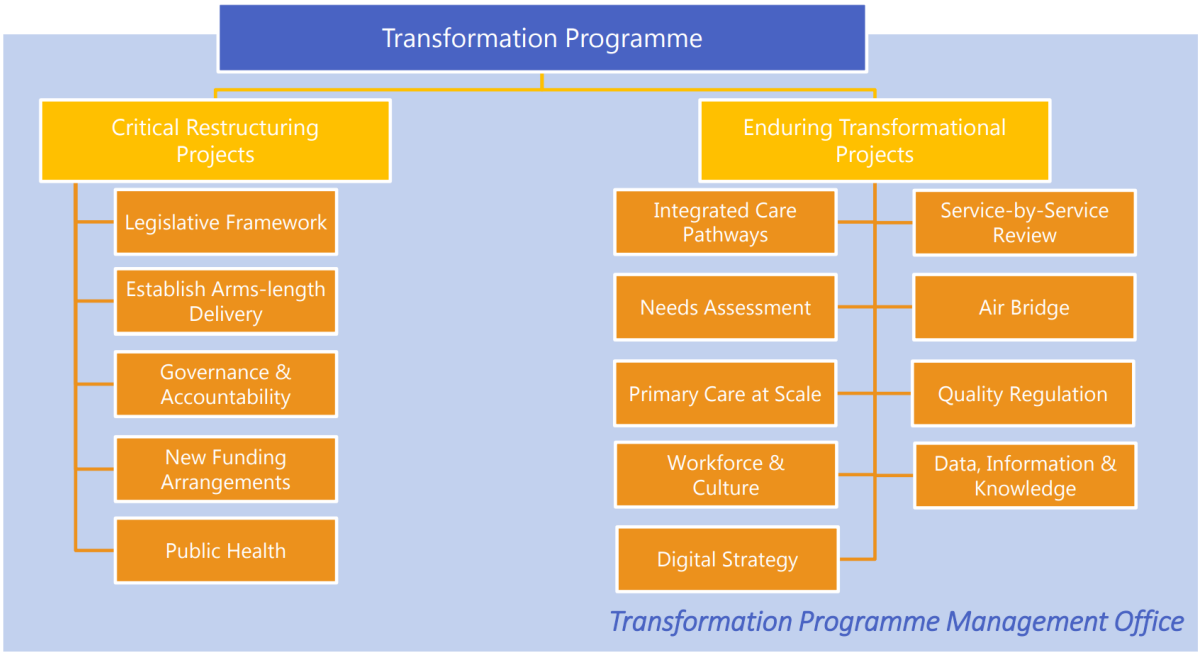
(2) Longer term view to deliver the strategy:



7. Information governance strategy on a page

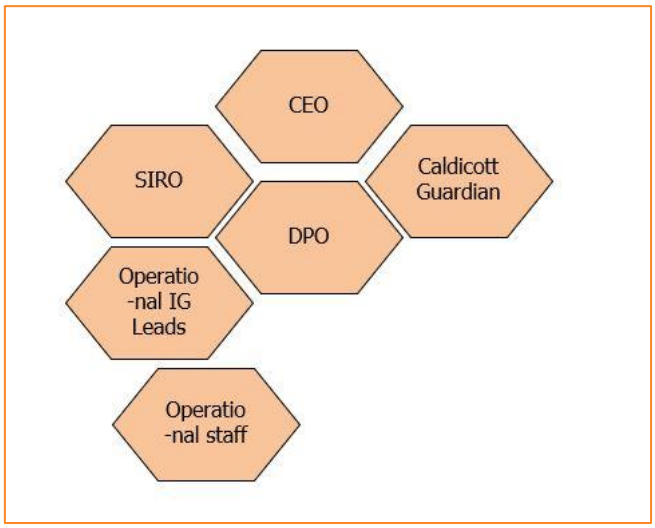


8. Appendix A: Overview of transformation programme



9. Appendix B: Key governance requirements

9.1 Key information governance capabilities to deliver the strategy



The following are the key capabilities required to deliver the information governance strategy:

- The Chief Executive of each organisation will be the sponsor for information governance.
- The role of the Senior Information Risk Owner (SIRO) will be identified within each organisation at the board level with a specific responsibility for information risk. The SIRO will be concerned with the risks to information systems generally. Information Asset Owners (IAOs) will be identified to support the SIRO.
- The role of the Caldicott Guardian will be crucial for managing the use and sharing of patient-identifiable information. A Caldicott Guardian will be appointed for health services and another one for social care services. The role of the Caldicott Guardian will consider not only the Caldicott principles, but also wider concepts of information management such as data protection, the equivalent of Section 251 of the NHS Act which is being introduced on the island, Freedom of Information Act, Human Rights Act, and information governance. The Caldicott Guardians will be members of the Senior Leadership Team. The Caldicott Guardian for health will promote clinical governance while the Caldicott Guardian for social care will promote care, quality and safety of service users.
- A Data Protection Officer (DPO) will be designated by each organisation as per Art. 37 of the Applied GDPR. The DPOs will perform their responsibilities as stipulated under Art. 39 of the DPO (Tasks of the DPO). As per the previous, Article 29 Working Party Guidelines on Data Protection Officers, the DPO(s) will be the "cornerstone of accountability" and the "compliance orchestrator". The DPO(s) will be the "intermediary between all the relevant stakeholders (e.g., supervisory authorities, data subjects and business partners)." The DPOs will have the authority, support and resources to do their job effectively. The DPOs will report to the highest management level.
- The organisations will appoint internal operational IG leads and they will be the representatives of each department. They will be responsible for the day-to-day implementation and maintenance of information governance of their respective areas and staff, with the ability to collaborate effectively with the DPO.
- Staff will be responsible for ensuring that policies and procedures are implemented.

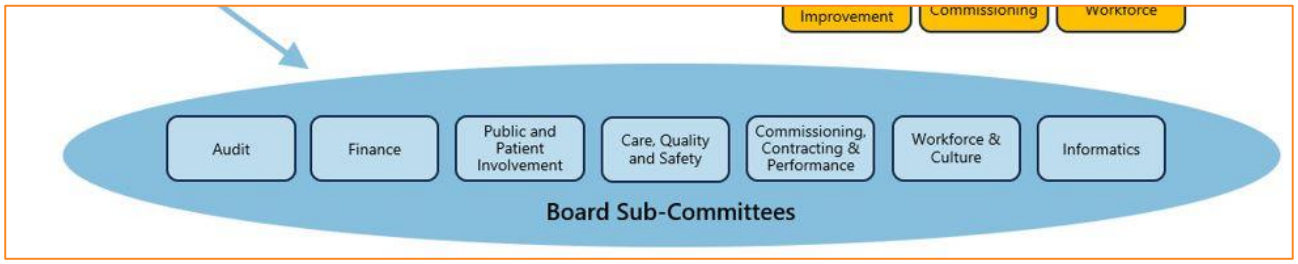
9.2 Oversight groups

9.2.1 Information Governance Steering Committee

An information governance committee will be established within each organisation to drive the information governance strategy and activities.

The committee will report on information governance issues and risks to the board of the organisation. The SIRO will chair the committee. A terms of reference will be defined to set out the committee's aim, duties, membership and reporting responsibilities.

For instance, for Manx Care, the Information Governance Steering Committee will be an additional new Board Sub-Committee alongside the other Board Sub-Committees identified in the STOM[7]:



9.2.2 Operational Group

An information governance working group will be created within each organisation to discuss and coordinate information governance activities at an operational level.

The group will produce minutes of the meetings and action plans. The agenda will show the information governance issues discussed. The information governance working group will report issues and risks to the Information Governance Steering Committee.

10. APPENDIX C: Information governance awareness & training

The accountability principle makes the organisations responsible for complying with the Applied GDPR and they must be able to demonstrate their compliance. It is therefore vital that staff who act on behalf of the organisations understand the importance of protecting personal data, are familiar with the information governance policies and put the procedures into practice so that we can deliver this strategy.

[7] Reference is being made to System Target Operating Model dated 27 Aug 2020, page 14, titled "Draft Manx Care Organisational Chart"

The organisations will establish a formal needs-based awareness and training programme (including periodic refreshers) for all their staff. The programme will cover the following key themes:

- The organisations' responsibilities under the Applied GDPR
- The responsibilities of the staff for protecting personal data
- The key information governance policies & processes they need to know about

The programme will identify the needs for:

- all staff training programme
- induction and refresher training
- additional training and professional development for specialised roles or functions with information governance responsibilities
- monitoring and reporting on information governance training so that each organisation can demonstrate that their staff have received training
- raising awareness on associated policies and process through staff meetings of forums. This will be a DPO task as stipulated in the Applied GDPR.

11. APPENDIX D: Information security

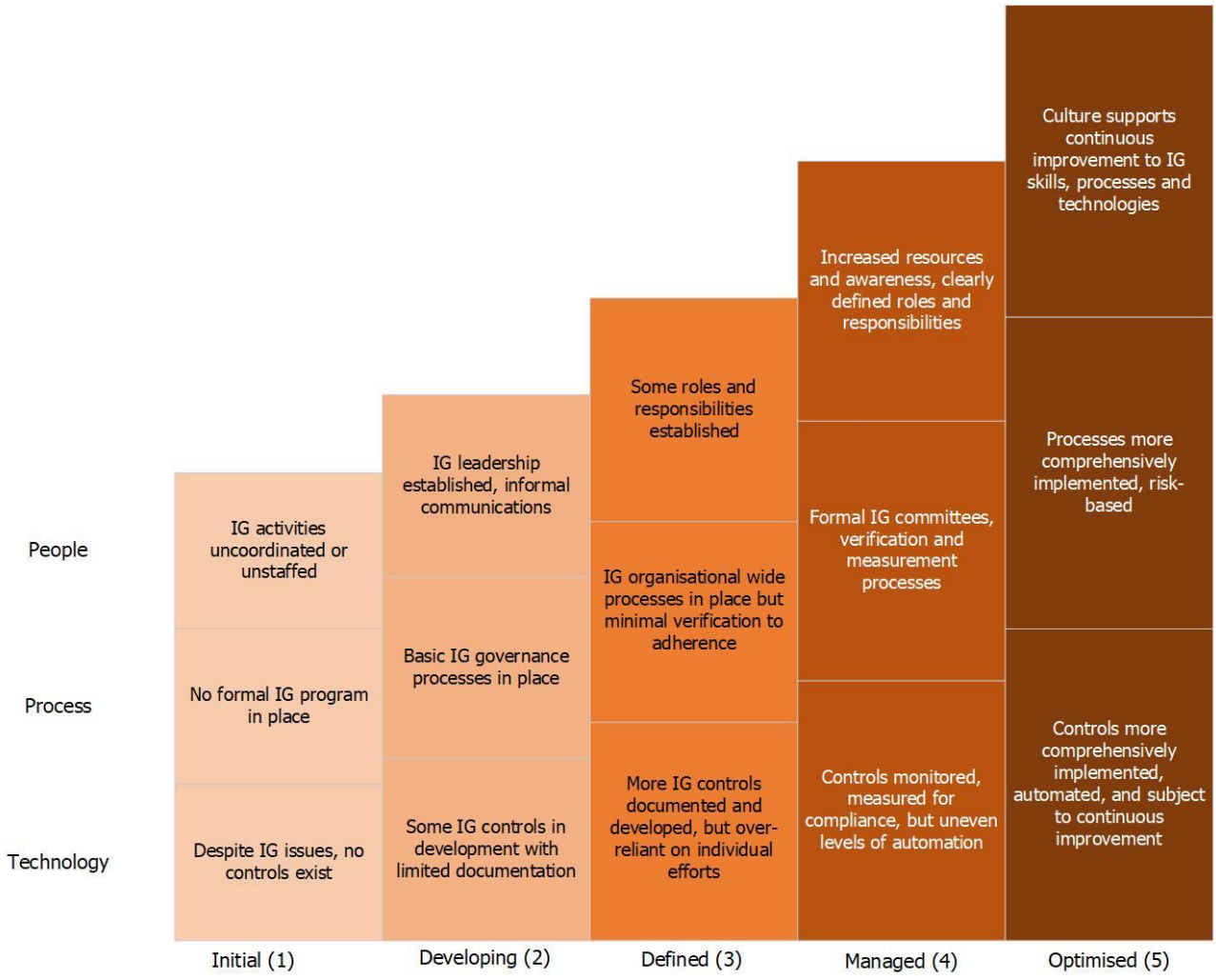
As per the security principle of the Applied GDPR, the organisations must process personal data securely by means of 'appropriate technical and organisational measures'. The organisations will have appropriate security[8] to prevent personal data they hold being accidentally or deliberately compromised which can cause real harm or distress to service users, especially if it relates to sensitive information.

An information security assessment of the risks presented by each organisation's processing will be undertaken to establish the baseline and assess the appropriate level of security that needs to be put in place. An information security policy or equivalent will be implemented. Appropriate controls will be implemented to enforce the policy. In order to implement the appropriate controls, an adequate framework will be identified and followed.

[8] For the purpose of this paper, information security also includes cybersecurity (the protection of the organisations' networks and information systems from attacks) and, also covers physical and organisational security measures.

12. Appendix E: Information governance maturity

The below model will be used to track the maturity of the information governance programme. A typical information governance maturity curve runs on a scale from 1 to 5 (1 being immature and 5 being highly mature as shown below:



How much information governance will be enough? A **minimum** 'high 4' is a desirable target. Given the vision is to optimise information, achieving level 5 should be a long-term target.

Version Control

Version	Date	Author/Contributor	Changes
0.1	12.08.2020	Natasha Singh	Author version
0.2	14.08.2020	Matthew Stevens	Contributor version
0.3	18.08.2020	Natasha Singh	First draft for internal team review
0.4	18.08.2020	Natasha Singh	First draft for stakeholders' review
0.5	11.09.2020	Natasha Singh	Included feedback received from stakeholders
1.0	25.09.2020	Natasha Singh	Approved by Manx Care Transformation Board, recognising this is a living document subject to ongoing change.

Stakeholders' Register

Names	Functions
Iain McDonald	Isle of Man Information Commissioner
Graham Hindle	DPO for Cabinet Office (not present)
Gaye Miller	DPO for DHSC
Karen Malone	Interim Deputy CEO Governance for DHSC
Gregor Peden	Chief Clinical Information Officer for DHSC
Paul Edge	DHSC Senior Information Risk Officer
Alan Chambers	G-CISO, Office of Cyber Security and Information Assurance
Madeleine Sayle	Public Health – Business Intelligence Lead
Louise Quayle	DHSC – Business Intelligence Lead
Catherine Quilliam	Caldicott Guardian
Rebecca Rowley	Head of Research and Development Public Health Directorate