Information sharing authorising framework

Comprehensive guidance for information sharing

FINAL

March 2018

v1.0.0

PUBLIC

Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. PUBLIC | | | | | |
| 1. **Date of review of security classification** | 1. March 2018 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Queensland Government Chief Information Office | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Information Strategy and Policy  
Queensland Government Chief Information Office  
[qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au)

Acknowledgements

The *Information sharing authorising framework* has been iteratively developed in conjunction with GWI Consulting and key stakeholders, including the Department of Communities, Child Safety and Disability services. We’d like to thank all those stakeholders that provided input into the development of this document

Copyright

*Information sharing authorising framework: Comprehensive guidance for information sharing*

© The State of Queensland (Queensland Government Chief Information Office) 2018

Licence

[](http://creativecommons.org/licenses/by/4.0/)

This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au).

To attribute this material, cite the Queensland Government Chief Information Office.

The licence does not apply to any branding or images.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1. Introduction 6](#_Toc507594596)

[1.1. Purpose 6](#_Toc507594597)

[1.2. Audience 6](#_Toc507594598)

[1.3. Scope 6](#_Toc507594599)

[1.4. Definitions 6](#_Toc507594600)

[2. Background 7](#_Toc507594601)

[2.1. Why has this framework been created? 7](#_Toc507594602)

[3. Overview 8](#_Toc507594603)

[4. Prepare phase 13](#_Toc507594604)

[4.1. Organise 15](#_Toc507594605)

[4.2. Evaluate 16](#_Toc507594606)

[4.3. Enable 18](#_Toc507594607)

[5. Formal agreement instruments 19](#_Toc507594608)

[6. Escalation pathway 20](#_Toc507594609)

[7. Permitted usage conditions model 23](#_Toc507594610)

[7.1. Permissions model 24](#_Toc507594611)

[7.2. Permitted conditions 24](#_Toc507594612)

[7.3. Example scenarios 25](#_Toc507594613)

[8. Manage phase 28](#_Toc507594614)

[8.1. Create/Capture 30](#_Toc507594615)

[8.2. Use and manage 31](#_Toc507594616)

[8.3. Retire 32](#_Toc507594617)

[9. Exchange phase 34](#_Toc507594618)

[9.1. Test 36](#_Toc507594619)

[9.2. Validate 37](#_Toc507594620)

[9.3. Go-live 37](#_Toc507594621)

[10. Use Phase 39](#_Toc507594622)

[10.1. Access 41](#_Toc507594623)

[10.2. Manipulate 42](#_Toc507594624)

[10.3. Monitor 42](#_Toc507594625)

[Appendix A Supporting output artefact summary 44](#_Toc507594626)

[10.4. Prepare phase 44](#_Toc507594627)

[10.5. Manage phase 44](#_Toc507594628)

[10.6. Exchange phase 44](#_Toc507594629)

[10.7. Use phase 45](#_Toc507594630)

[11. Document history 46](#_Toc507594631)

Figures

[Figure 1: Overview – Information sharing authorising framework 9](#_Toc507429508)

[Figure 2: Key documents of the Information sharing authorising framework 11](#_Toc507429509)

[Figure 3: Overview - The Escalation pathway and the Permitted usage condition model. 12](#_Toc507429510)

[Figure 4: A full overview of the Prepare phase 14](#_Toc507429511)

[Figure 5: The Organise sub-phase of the Prepare phase 15](#_Toc507429512)

[Figure 6: The Five Safes Framework 16](#_Toc507429513)

[Figure 7: The Evaluate sub-phase of the Prepare phase 17](#_Toc507429514)

[Figure 8: The Enable sub-phase 18](#_Toc507429515)

[Figure 9: Formal Agreement Instruments Hierarchy 20](#_Toc507429516)

[Figure 10: Escalation pathway 22](#_Toc507429517)

[Figure 11: Permitted usage conditions model 24](#_Toc507429518)

[Figure 12: The Manage phase 29](#_Toc507429519)

[Figure 13: The Create/Capture sub-phase of the Manage phase 31](#_Toc507429520)

[Figure 14: The Use and manage sub-phase 32](#_Toc507429521)

[Figure 15: The Retire activity 33](#_Toc507429522)

[Figure 16: The Exchange phase 35](#_Toc507429523)

[Figure 17: The Test sub-phase 36](#_Toc507429524)

[Figure 18: The Validate sub-phase 37](#_Toc507429525)

[Figure 19: The Go Live sub-phase 38](#_Toc507429526)

[Figure 20: The Use phase 40](#_Toc507429527)

[Figure 21: The Access sub-phase 41](#_Toc507429528)

[Figure 22: The Manipulate sub-phase 42](#_Toc507429529)

[Figure 23: The Monitor sub-phase 43](#_Toc507429530)

Executive summary

The Information sharing authorising framework (ISAF) provides a suite of guidance and advice for Queensland Government agencies that are seeking to establish and manage an information sharing activity. The primary objective of the framework is to assist the practitioner in implementing a successful information sharing activity by focusing on the benefits of sharing while managing the risks and understanding the constraints. It can be used for activities that involve all types of data (from closed or shared to [open](https://www.qld.gov.au/data/qld-data-policy-statement.pdf)), that concern a large and varied number of stakeholders, from government and non-government, and for a broad range of uses (such as to facilitate service delivery, inform or implement policy, provide input to analytics projects or [publish open data](https://data.qld.gov.au/)).

The ISAF was instigated after numerous service delivery issues identified a need to improve information sharing across Queensland Government. This resulted in a comprehensive analysis of the evidence of information sharing activities and led to the identification of several barriers, enablers and opportunities. Generally, the evidence indicated a deep avoidance to sharing information driven mostly by a broad ‘risk aversion’ culture in the wider public sector. The ISAF has been designed to remove this and other barriers through clear and consistent understanding of the risks and constraints, whilst focusing on highlighting the enablers and opportunities in every information sharing activity.

The ISAF is modular in design which allows sharing practitioners to select guidance and tools provided by the framework that best fit their individual circumstances and underlying objectives. Each item of guidance and advice is organised into four distinct phases of a sharing activity: *Prepare*, *Manage*, *Exchange* and *Use*. The *Prepare* phase is the logical starting point for implementation and provides pathways for defining, evaluating and formalising any sharing activity. The *Manage* phase is the default operating phase of the framework and is designed to manage an information sharing activity over its lifecycle. The *Exchange* phase contains guidance on how to conduct the exchange of information in a sharing activity, whilst the *Use* phase provides guidance to maximise the access, use and analysis of the information shared. Within each phase there are subordinated sub-phases that focus a key objective, and within each sub-phase there are key activities and output artefacts.

A cornerstone to any information sharing activity is the development and endorsement of agreement instruments that formally authorise the sharing activity. The ISAF provides a hierarchical set of standardised formal agreement instruments that in conjunction, can be used for authorising a sharing activity. These items are the master sharing agreement (MSA) and the information exchange schedule (IES). The MSA describes the commitment to information sharing between two or more agencies for a specific contextual purpose. The MSA is high-level in nature and defines an agreed set of principles that underpin sharing within its specific context. The subordinate IES provides the details of sharing and includes items such conditions of exchange, roles and responsibilities and any agreed formats or standards required. Essentially, the MSA authorises the information sharing activity, whilst the IES enables it.

Supporting these formal agreement instruments are two additional mechanisms, the *Permitted usage conditions model* and the *Escalation pathway*. The permitted usage conditions model provides a standardised way for an information custodian to control the permitted uses of the information shared. Using the four categories of constraints - *Time Frame/Trigger, Uses, Access* and *Authority* – the model empowers custodians to clearly and consistently identify constraints on the usage of the information shared. The escalation pathway provides a process to remediate any points of disagreement between parties in establishing an MSA. It has been designed to surface visibility of the information sharing activity to key decision makers in government to bring about the resolution of any disputes between parties.

# Introduction

## Purpose

This framework provides a suite of guidance and advice for agencies that are seeking to establish and manage information sharing activities. It can be used for activities that involve all types of data, from closed or shared to [open](https://www.qld.gov.au/data/qld-data-policy-statement.pdf), and for a broad range of uses (to facilitate service delivery, inform or implement policy, provide input to analytics and machine learning projects or [publish open data](https://data.qld.gov.au/)). This guidance and advice are provided for assistance, information and utility only. While some information and guidance provided in the Framework communicates other mandatory obligations which may be relevant (e.g. legislation, privacy, policy), agencies are strongly recommended to further investigate these obligations considering their own business requirements, and seek legal/expert advice where necessary.

## Audience

This document is intended for anyone who is interested in establishing and managing information sharing activities between two or more distinct entities. These may include (but are not limited to):

* information custodians, owners and managers
* information architects
* solution designers
* data scientists
* service delivery program officers
* policy officers.

## Scope

This framework does not form a mandatory component of the [Queensland Government Enterprise Architecture](https://www.qgcio.qld.gov.au/information-on/qgea/about-the-qgea) (QGEA) and is provided as a guideline only. The framework notes where existing QGEA documents apply and all mandatory policies must be adhered to where relevant.

## Definitions

To improve clarity and to promote alignment with other QGEA documents, this document will apply terminology from the QGCIO glossary.

# Background

## Why has this framework been created?

On the back of numerous service delivery failures attributed in part to a failure in the effective sharing of information, a need was identified to improve information sharing across Queensland Government. The Information sharing authorising framework has been developed to address a broad information sharing need while protecting confidentiality and privacy rights of citizens. This is particularly the case as government service delivery increasingly occurs in a diverse and sometimes innately complex environment.

While there have been significant advances in relation to Open Data as a result of the release of the [Queensland Open Data Policy Statement](https://www.qld.gov.au/data/qld-data-policy-statement.pdf), amendments to the [Information access and use (IS33) policy](https://www.qgcio.qld.gov.au/documents/information-access-and-use-policy-is33) and the availability of the [Open Data portal](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au), negotiating successful and proactive sharing of other information resources continues to raise challenges for Queensland Government agencies. Therefore, although elements of this framework may be applicable to Open Data, it is highly recommended that [existing resources](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au/resource/19a9a82f-b3ba-48f9-9134-4ee9b76cdd28) are used to make these datasets available through the [Queensland Government Data Portal](https://data.qld.gov.au/).

This framework is the result of several analyses of a broad range of evidence on information sharing across Queensland Government. These analyses highlighted the key barriers, enablers and opportunities for information sharing across the sector. Subsequently, the design philosophy of the framework is to provide a set of modularised guidance that works together to remove these identified barriers, whilst maximising the emerging opportunities and value of information sharing to agencies. The framework aims to change the nature of information sharing conversations from being primarily about ascertaining and remediating risk (either real or perceived) to identifying and enabling opportunities for improved policy decisions or service delivery outcomes.

This framework does not replace, negate or override legislative provisions that are in place to protect the privacy and confidentiality of citizens, but aims to better inform decisions that balance the risks associated with sharing activities and the business outcomes sought. Privacy, legislation and policy considerations are specifically included with several documents designed to designed to capture these considerations for inclusion for a holistic assessment of a sharing activity. Further information about privacy issues and their potential impact on sharing agreements can be found in the [Information Privacy Principles](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/key-privacy-concepts/overview-of-the-information-privacy-principles) and the [Privacy Impact Assessment](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process) (PIA) process on the [Office of the Information Commissioner](https://www.oic.qld.gov.au/) (OIC) website.

Strikingly, the analysis of the evidence indicates a deep and broad avoidance to information sharing across the sector, which in part stems from a broader public service ‘risk aversion’ culture. This risk aversion is propagated in part by bias in legislative interpretations of disclosure risk and exaggeration of associated penalties. While in many instances specific legislation does explicitly mandate restrictions on sharing information and provide penalties for non-compliance, there are many other instances where the legislative restrictions are perceived rather than real. These perceptions can be formed by a reliance on outdated legislative advice on the restrictions of sharing, absence of legal advice altogether, or the general acceptance of an inaccurate interpretation of legislation. This often manifests as a default position of not sharing. An agenda for broad legislative reform for sharing is currently being explored and will aim to identify and remove unnecessary legal barriers to information sharing (noting that many important and valid legislative instruments for the protection of an individual’s right to confidentiality and privacy exist).

The framework comprises of process guidance, artefact templates and references to other relevant resources for establishing and managing sharing activities. The primary outcomes are:

* an endorsed formal agreement to share information
* a solid and transparent understanding of the permissions, controls and acceptable use conditions of the shared information
* the successful exchange and use of the shared information.

Secondary outcomes of the framework include:

* increase the discoverability and visibility of existing information assets and information sharing activities and agreements between agencies
* increase the consistency of sharing activities and agreements using standardised models and architectures
* reduce the time taken to establish and implement a sharing agreement by using a standardised process.

Obtaining signatures for a sharing agreement often incurs lengthy delays because of the prudent action taken by many agencies of obtaining legal advice for the sharing activity. When these actions are considered in totality across Queensland Government, it becomes obvious that much inefficiency in this uncoordinated process exists. In providing a consistent, hierarchical structure in form and function of all sharing agreement instruments, the framework aims to provide precedent to reduce the time and effort required to execute an individual agreement and reduce inefficiency more broadly across Queensland Government.

The human conversation regarding the opportunities and risks of information sharing always precedes any technical implementation activity. The framework is designed to capture these human conversations and use them to inform both the sharing agreement and subsequent implementation. As such, many outputs are intended to be easily transformed into components of any implementation – both technical and otherwise.

The development of the framework has been informed by the Queensland Government [Information management principles](https://www.qgcio.qld.gov.au/documents/information-principles). These principles are a set of ambitions or values that Queensland Government aspires to when making decisions on the management of information assets and information sharing activities. These principles form a central component to the design philosophy of the framework.

# Overview

The framework has four distinct phases that mirror the lifecycle of any sharing activity: ***Prepare, Manage, Exchange*** and ***Use.***

Figure 2 on page 9 is an overarching representation of these four phases including a view of the interactions between each phase and descriptors of the supporting roles and tools.

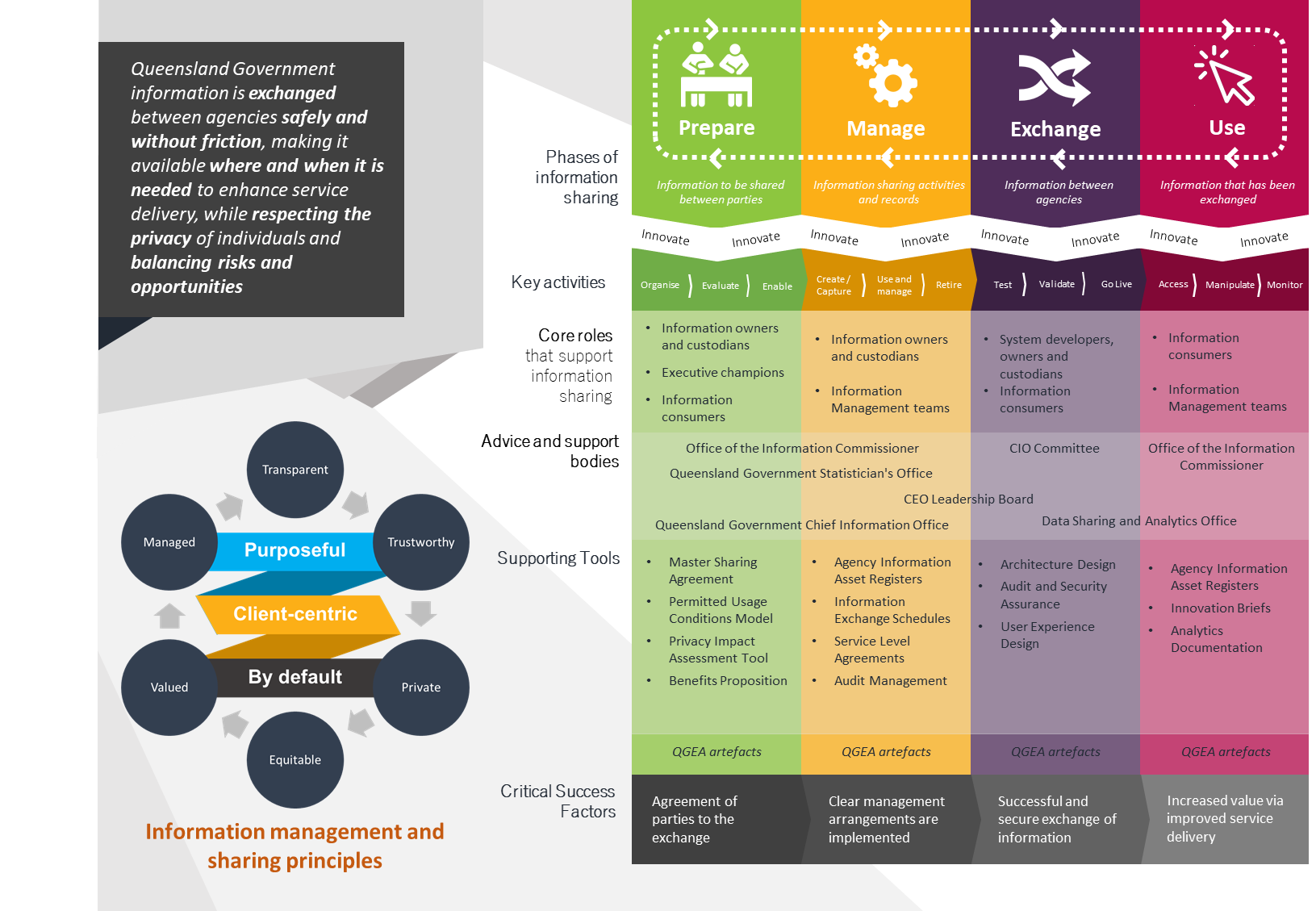


Figure 1: Overview – *Information sharing authorising framework*

While the representation in figure 2 appears linear, information sharing phases, sub-phases and activities do not always proceed in a linear fashion. In fact, the primary relationship between the phases is cyclic, reflecting the iterative lifecycle of an information sharing activity. The cyclical and iterative nature is key for a successful information sharing operation.

The framework scope covers sharing across a broad spectrum of data (from closed, shared and open data), between a large and varied number of stakeholders (from government and non-government) and for a broad range of uses (such as to facilitate service delivery, inform or implement policy, provide input to analytics projects or [publish open data](https://data.qld.gov.au/)). This broad scope has led to a modularised design philosophy that guides the usage of the framework. This modular design allows practitioners to select the guidance and tools that best fit their individual circumstances and underlying objectives. This allows the tailoring of the operation of the framework to the uniqueness of each individual sharing activity. For example, the success of one information sharing activity might hinge on a single output artefact, however, in another sharing activity the same artefact may not be as critical - or even required at all.



Figure 2: Key documents of the *Information sharing authorising framework*

The following key relationships assist in the frameworks operation:

* each phase of the framework has subordinated sub-phases - comprised of activities, with each activity producing or contributing to an artefact
* the *Prepare* phase should always occur first as its primary output is the information sharing agreement
* the *Manage* phase is core to all other phases and can be considered the default operating phase of the Framework (i.e. the phase where a sharing activity resides when in operation)
* innovation can occur in any phase (and the *Use* phase provides specific direction to include innovation direct from the users/consumers)
* information sharing ends in the *Retire* sub-phase of the *Manage* phase.

A cornerstone to any information sharing activity is a formal agreement between parties that authorise the sharing activity. The ISAF provides a hierarchical set of standardised formal agreement instruments that in conjunction, can be used to establish a formal agreement and authorise a sharing activity. These instruments are the master sharing agreement (MSA) and the information exchange schedule (IES). Further information on these formal agreement instruments and how they work together can be found in section 5.

Supporting these formal agreement instruments in authorising an information sharing activity are two additional mechanisms, the *Permitted usage conditions model* and the *Escalation pathway*. The Permitted usage conditions model allows an information custodian to clearly define the permitted uses of the information shared. The Escalation pathway provides a consistent process to remediate any points of disagreement between parties in an information sharing activity. Both mechanisms support the establishment of a formal information sharing agreement by ensuring transparency, trust and clear communication between parties forms a key component of any information sharing activity. Figure 3 presents an overview of both mechanisms:

**Escalation pathway**



**Permitted usage condition model**



Figure 3: Overview - The *Escalation pathway* and the *Permitted usage condition model.*

# Prepare phase

APPLICABLE QGEA POLICIES

* Information security (IS18)
* Information access and use policy (IS33)
* Information security classification framework (QGISCF)
* Information asset custodianship policy (IS44)

KEY PHASE OBJECTIVES

* Definition of benefits and value of the information sharing activity
* Assess and evaluate the key constraints for the information sharing activity, including legislation, privacy and information security
* Clear classification by information custodians on the permitted usage conditions of the shared information
* Establish an endorsed Master Sharing Agreement (MSA)

**PREPARE**

The *Prepare* phase is the logical starting point for implementing a sharing activity and provides a pathway for defining, capturing and formalising any information sharing conversation. The primary objective of this phase is to establish an information sharing agreement endorsed by all participating parties. The information sharing agreement is the key authorisation of any information sharing initiative and forms the basis of several key activities in subsequent phases. Resultantly, all activities and resources defined in this phase are targeted to supporting the development and final endorsement of an agreement. This includes activities such as determining the overarching value and measurable benefits of the sharing activity, identification and documentation of risks and subsequent controls, and the assessment of the [privacy impacts](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process) of the sharing activity. This phase will also introduce supporting resources such as the *Permitted usage conditions model* and the hierarchy of *Formal agreement instruments*. The cumulative result of this phase is a comprehensive set of resources and evidence base that provide clarity on the benefits and value of sharing, highlights and addresses all underlying risks and issues, and presents a robust and considered case for sharing. Figure 4 on page 14 provides for a full overview of this phase.

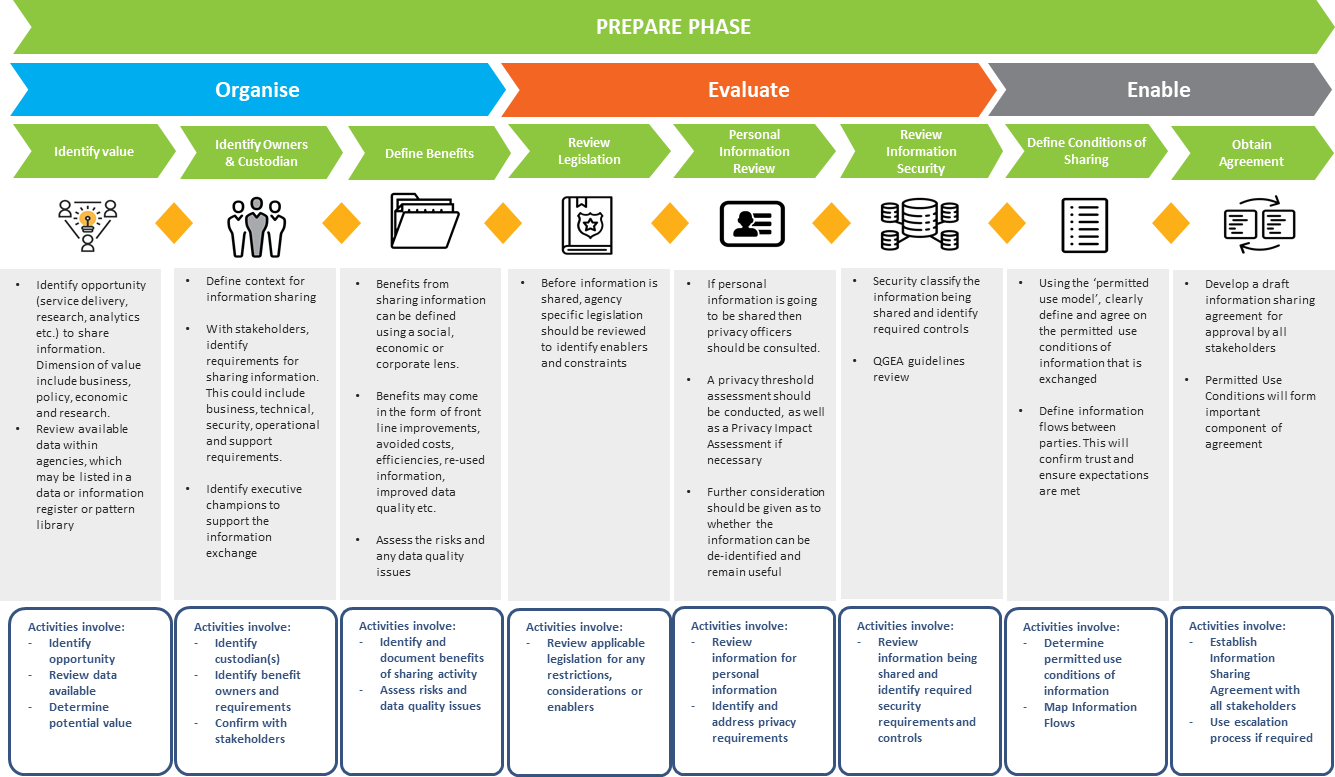


Figure 4: A full overview of the *Prepare* phase

## Organise

The *Organise* sub-phase forms the cornerstone of the *Prepare* phase. In this sub-phase, the information to be shared is defined, the information owners and custodians are identified, the benefits and value associated with sharing is determined, and any risks that accompany the sharing activity are assessed and controls defined (this includes assessing the critical risk of not sharing). Figure 5 below shows the detailed tasks of this activity.

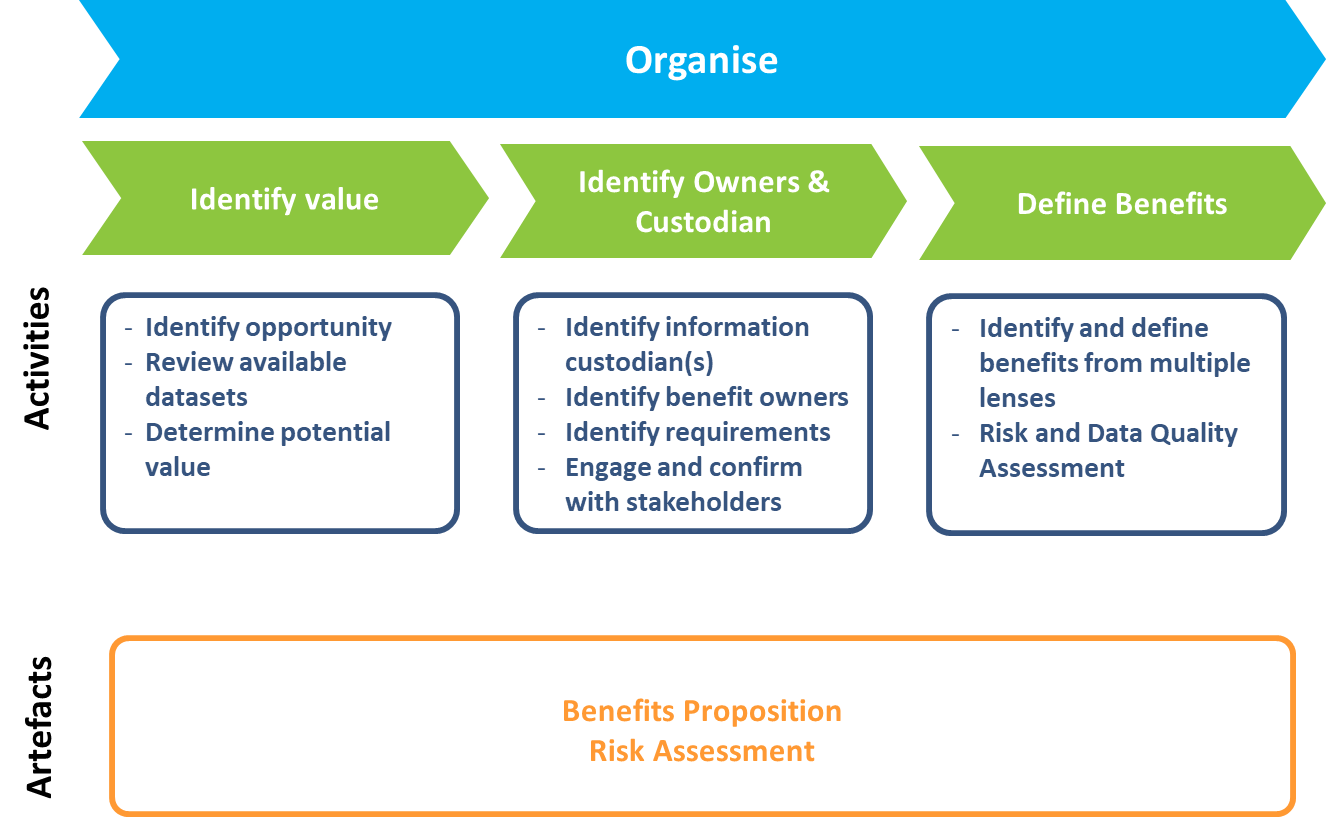


Figure 5: The *Organise* sub-phase of the *Prepare* phase

The artefacts of this sub-phase comprise of a benefits proposition document and a risk assessment document. The benefits proposition defines the value and benefits created through the information sharing activity and considers these through multiple lenses - including social, economic and corporate. Clear articulation of the value and benefits should include items such as direct or indirect benefits, derived or intended value, and who the recipients are. It is suggested that practitioners use their agency standard benefits realisation methodology (usually part of a project/program management methodology) to assist in this benefits definition activity. In the absence of specific agency guidance, QGCIO provides [project and program best practice guidance](https://www.qgcio.qld.gov.au/information-on/best-practice-methodologies) which includes resources on benefits definition and management. Finally, the quality of the information considered for the exchange should be preliminarily assessed at this point and any issues documented for further consideration.

The benefits proposition should also outline the key stakeholders of the sharing activity. At a minimum, this should include:

* executive sponsor/s
* information asset custodian/s
* information asset owner/s
* information recipient/s
* incident manager/s.

In this sub-phase, the risk assessment for the information sharing activity should also be considered. The risk assessment identifies and manages the risk associated with the information sharing activity across its entire value chain and throughout its life-cycle. A specific risk management methodology for information sharing is yet to be developed and agencies are advised to use their own risk methodologies for assessing risk, in conjunction with a consideration of personal information disclosure risk. One such emerging framework that could be used by an information sharing practitioner in assessing personal information disclosure risk is the ‘Five Safes’ Framework. The individual components of this risk framework are shown in Figure 6. Further information about the Five Safes Framework can be found in the QGCIO knowledge base.

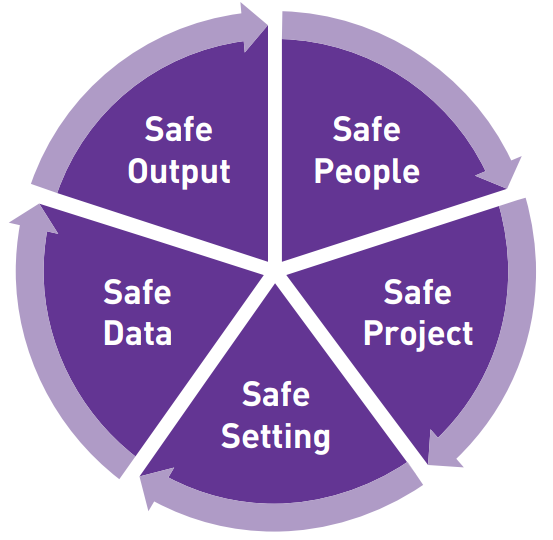


Figure 6: The Five Safes Framework[[1]](#footnote-2)

## Evaluate

With the value proposition for sharing established, the next step is to evaluate, assess, and manage the constraints of the sharing activity through the *Evaluate* sub-phase. This sub-phase assesses and evaluates any applicable legislation which might constrain or enable the sharing activity, assesses and understands the privacy impacts of sharing and evaluates the security classification of the information being shared. Figure 7 on page 17 illustrates the activities and output artefacts of this sub-phase.

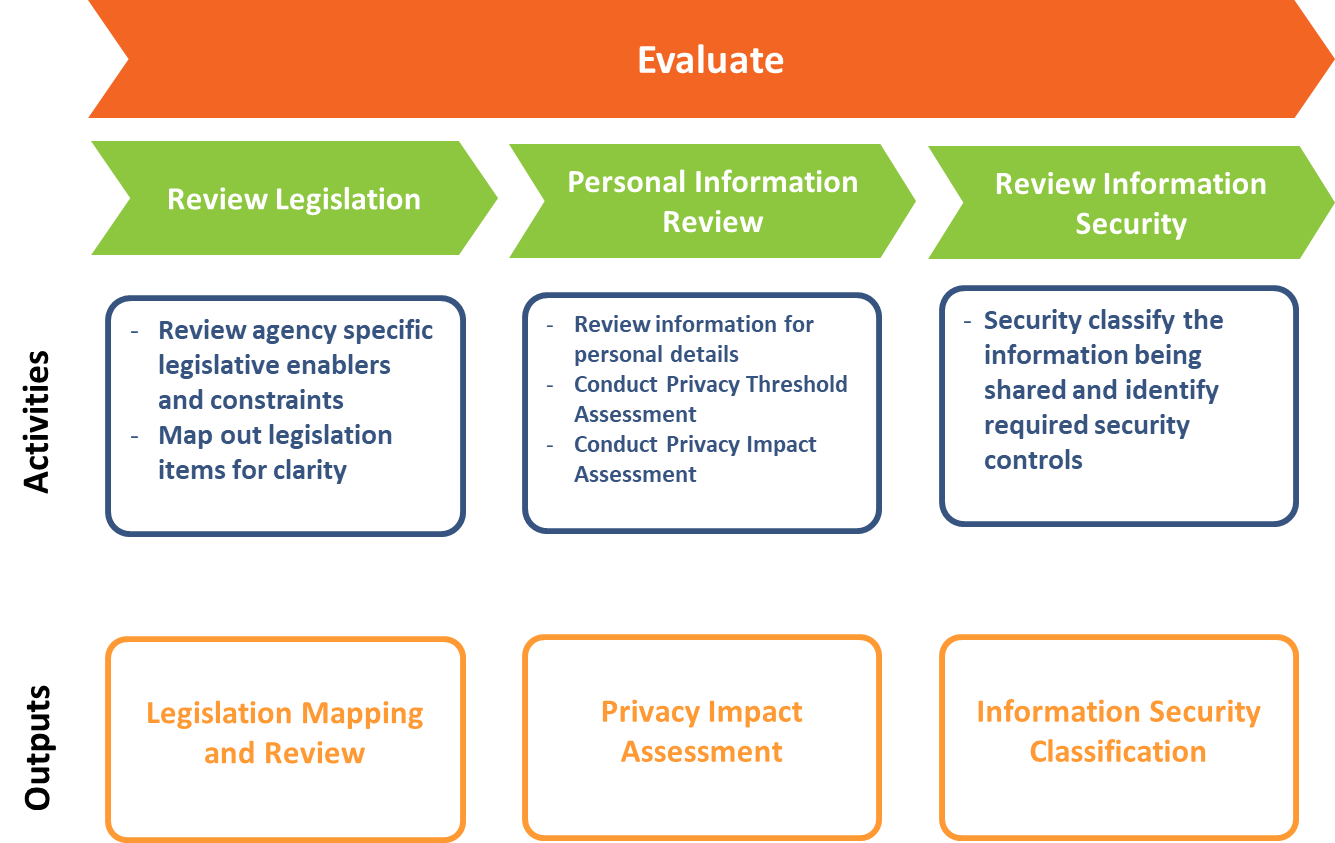


Figure 7: The *Evaluate* sub-phase of the *Prepare* phase

Legislation can be a key enabler or barrier to an information sharing activity and resultantly, any relevant legislation which may impact on the information sharing activity must be reviewed. An understanding of any applicable legislation will be crucial in forming a successful information sharing activity, as any legislative constraints on sharing can be identified, documented and understood by all parties. This outcome of the legislation review will significantly impact the direction and structure of any information sharing master agreement.

If personal information is under consideration for sharing, then a [privacy impact assessment (PIA)](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process) should be completed. The PIA guideline developed by the Office of the Information Commissioner[[2]](#footnote-3) firstly determines whether any personal information is in scope of the project through a privacy threshold assessment, and if so, then allows agencies to assess privacy impact and identify ways where privacy obligations can be met. Respective privacy officers from individual parties should be engaged to assist with completing the PIA. The final PIA report will determine the privacy impacts of the information sharing activity and identify options to address these impacts. It will be important that all parties work closely together in completing the PIA process as an agreement on the privacy impacts and controls is vital to success of any information sharing activity.

As part of the Personal Information Review activity, agencies may also need to consider the de-identification of information which contains personal information. Although the privacy of individuals must be protected in accordance with the [*Information Privacy Act 2009*](https://www.legislation.qld.gov.au/view/html/inforce/current/act-2009-014) (Qld) when sharing information, the existence of personal information should not in itself be a barrier to sharing. The [Office of the Information Commissioner](https://www.oic.qld.gov.au/) provides a range of advice on [dataset publication and de-identification techniques](https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/dataset-publication-and-de-identification-techniques) as well as information on [dataset publication and privacy.](https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/dataset-publication-and-privacy)

The security classification of the information considered for sharing must also be determined using the [Information Security Classification Framework](https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf) (QGISCF). This determination is a mandatory activity under QGEA policy and must consider the confidentiality of the information to be shared in both the existing and new usage contexts. Once the classification of the information has been determined, any required security controls should be identified and documented. It is important that all parties agree on the security classification of the information to be shared and confirm the required controls. Maintaining clear communication of the security obligations of all parties is critical for the success of any information sharing activity.

## Enable

The *Enable* sub-phase is the penultimate conclusion of the *Prepare* phase. This sub-phase collates the sharing activity definition and evaluation outputs together to ultimately present a thorough and compelling case for the establishment of an information sharing activity. This case forms the basis for defining permitted usage conditions and the creation and endorsement of a Master Sharing Agreement (MSA). Figure 8 outlines the key task of the Enable sub-phase.

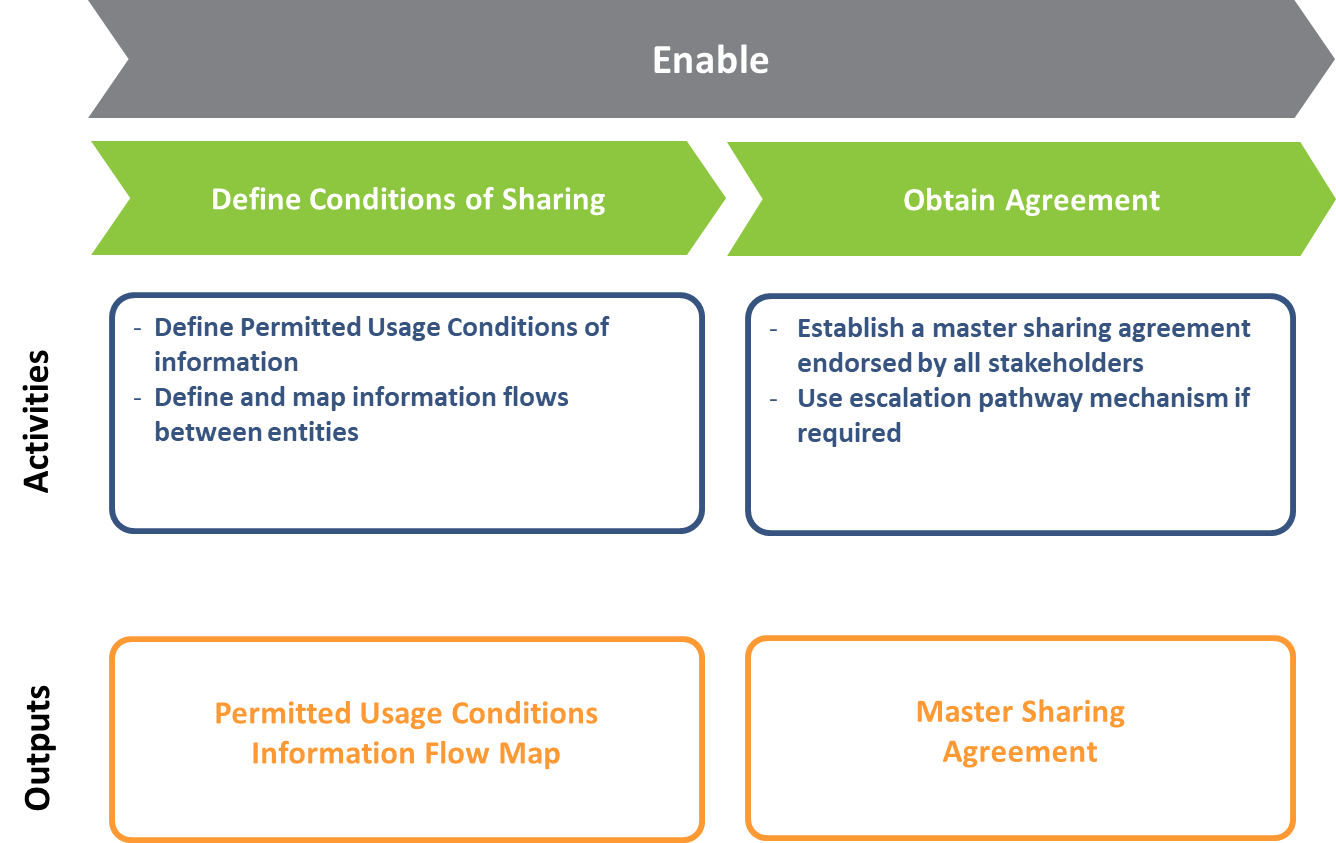


Figure 8: The *Enable* sub-phase

The Framework provides the *Permitted usage conditions model* to allow information custodians to clearly define permissions on how shared information can be used in a sharing activity. A key benefit of using a standardised model is that it allows a consistency and familiarity in how shared information can be used for both sharing and receiving parties. This consistency and clarity reduces the risk of mistrust developing in the sharing activity through ambiguous or unclear permissions. A standardised model is a critical component of the trust through transparency philosophy of the Framework. For further information please see the description on the Permitted usage conditions model in section 7.

The definition and documenting of information flows proposed under the information sharing initiative should also occur during this sub-phase. Documenting information flows will ensure that the information custodians expectations are met through a clear, consistent and shared understanding of how information traverses throughout the sharing activity.

Once all parties are satisfied with the scope, strength and quality of the artefacts developed in this sub-phase, a MSA can be developed for the sharing activity. The MSA is the authorising vehicle that describes a commitment to an agreed set of principles for information sharing between two or more agencies in a specific context.

The MSA is a cornerstone component of the formal agreement instruments defined by the Framework. These hierarchical instruments aim to provide a consistent, structured and reusable authorisation pathway for all information sharing activities established using the Framework. Further detailed information on these can be found in Section 5.

# Formal agreement instruments

The framework defines a hierarchical group of formal agreement instruments whose objective is to provide a standardised authorisation pathway for all information sharing activities. These formal agreement instruments and their sponsorship levels are described below in table 1.

|  |  |  |
| --- | --- | --- |
| Instrument | Level of Sponsorship | Description |
| 1. Data and information sharing charter **(PROPOSED)** | 1. Director-General | 1. Whole-of-government executive agreement on the core principles of information sharing |
| Master sharing agreement | 1. Deputy Director-General | 1. Contextual executive agreement for information sharing between all relevant parties for a particular purpose |
| Information exchange schedules | 1. Executive Director 2. (or CIO) | 1. Comprehensive details of information sharing activities for endorsed context and purpose. |

Table 1: Formalised Information sharing agreement instruments

To address systemic cultural barriers to broad information sharing, the framework proposes the development of a Data and information sharing charter that outlines a commitment by Chief Executives to effective, efficient and safe information sharing across Queensland Government. The proposed charter aims to obtain endorsement by all Directors-General and Chief Executives of Queensland Government agencies.

Supporting the execution of the Charter, the master sharing agreement is the authorising vehicle that describes a commitment to information sharing between two or more business areas for a specific purpose. The Information exchange schedule/s (IES) is a subordinate artefact of the MSA and contain the specific details of the information sharing activity. In other words, the MSA authorises the information sharing activity, while the IES enables it. As an example the MSA confirms a commitment from signatories to define clear roles and responsibilities for an information sharing activity and the IES contains detailed definitions of these roles and responsibilities. The IES is completed in the *Manage* phase of the Framework.

The MSA, as well as defining the participating parties and the objective of the agreement, defines an agreed set of principles that underpin the information sharing activity. These high-level principles include (but are not limited to) domains such as accountability, security controls, governance models and success measures. The signatories on any MSA agreement should be senior executive sponsors of the information sharing activity with the delegated authority to approve data and information sharing.

The specifics of any information sharing activity are documented and endorsed in the subordinate IES. These include items such as conditions of the exchange, defined roles and responsibilities, impacting legislation and exchange formats and standards. Any agreed principle described in the MSA is extrapolated in detail within the IES.

Together, the Data information sharing charter, the MSAs and their related IESs form a standardised set of formal instruments that allow consistent and granularised authorisation of an information sharing activity. The relationships between each instrument is shown in figure 9 on page 21.

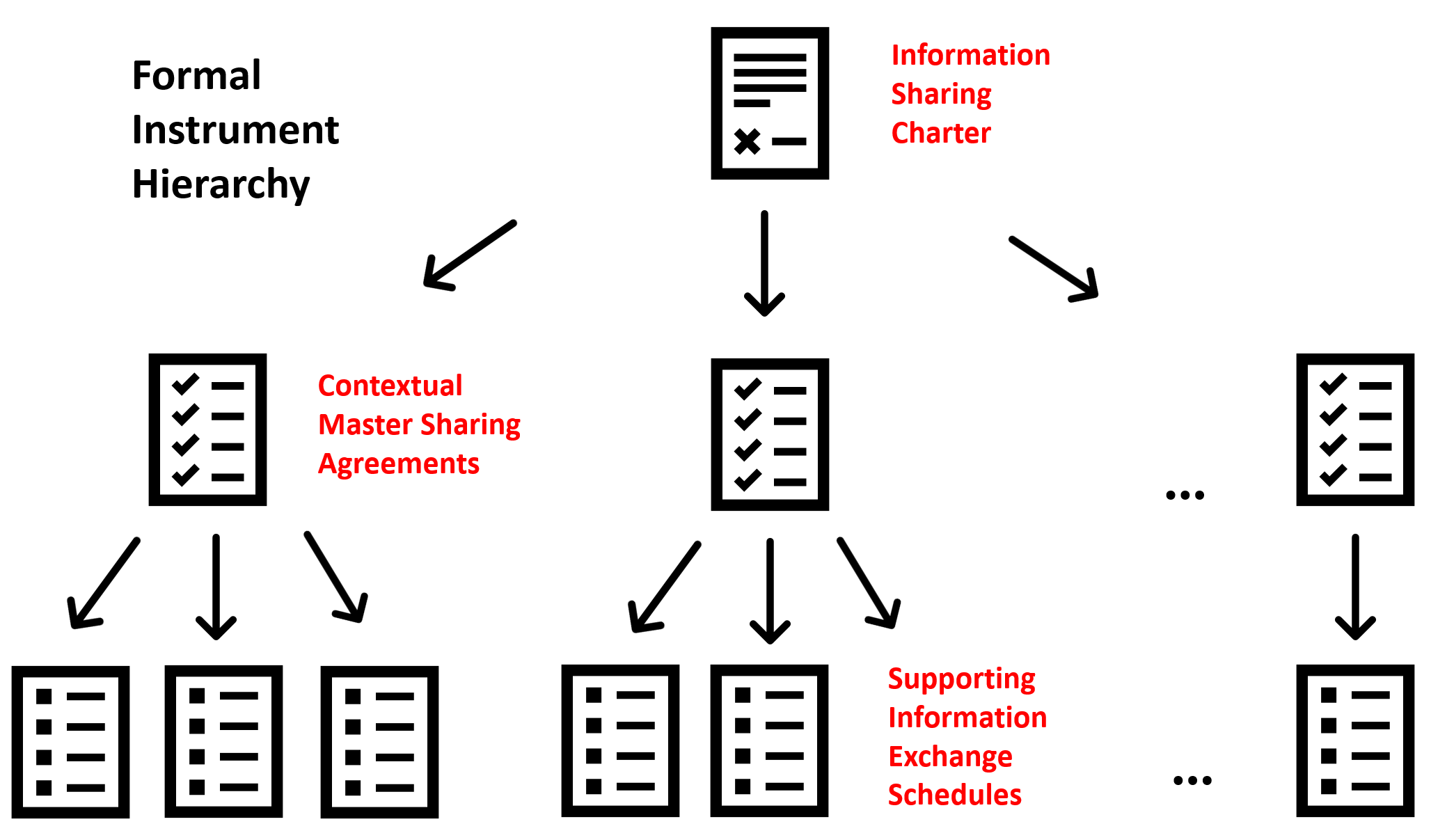


Figure 9: *Formal Agreement Instruments* Hierarchy

# Escalation pathway

If all the activities in the *Prepare* phase are completed, then a large body of evidence should exist to support the case for the information sharing activity and an MSA should be endorsed by all parties. However, there may be some instances where an information sharing agreement cannot be reached. In these instances, the framework provides an *Escalation pathway* mechanism to facilitate the remediation of any points of disagreement between parties. The *Escalation pathway* is illustrated in figure 10 on page 22.

The *Escalation pathway* outlines various roles and responsibilities that facilitate the remediation process. These include information owners and custodians.

Information owners are recognised officers who have been identified as having the authority and accountability for the collection and management of information on behalf of the State of Queensland. Where appropriate, the information owner can delegate information ownership to another appropriate person within their organisation.

The information owner/s or delegated information owner/s can then delegate their responsibilities around implementing and maintaining their information assets to an information custodian. The information custodian is responsible for enforcing the rules set by the information owner for the entire life cycle of the information asset.

These roles are also referred to as information asset owner/s and information asset custodian/s, see the [QGEA Information management roles and responsibilities guidelines](https://www.qgcio.qld.gov.au/documents/information-management-roles-and-responsibilities-guideline) and the [Information asset custodianship policy (IS44)](https://www.qgcio.qld.gov.au/documents/information-asset-custodianship-policy-is44).

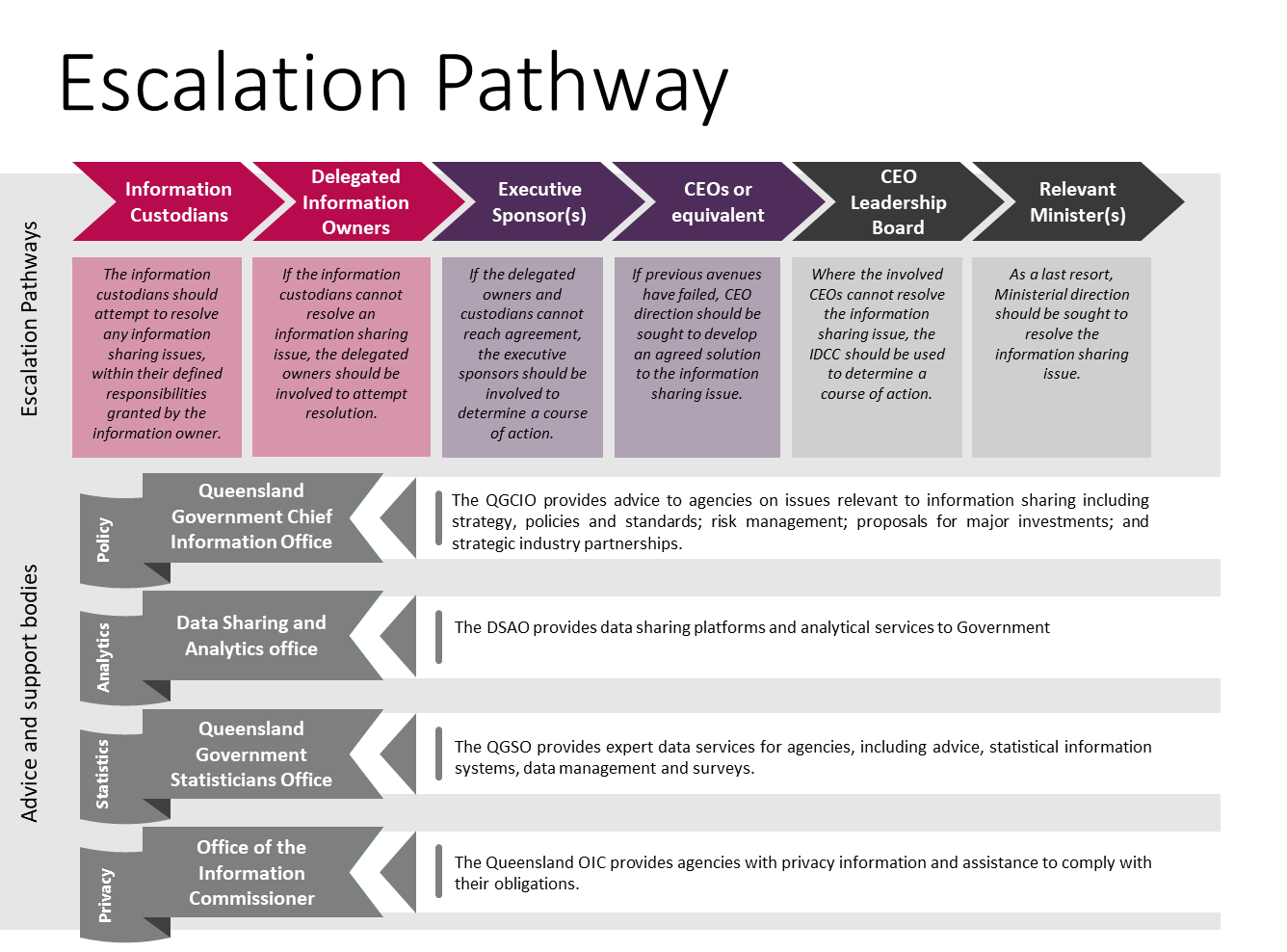


Figure 10: *Escalation pathway*

In the first instance, parties should engage the identified Information custodians and owners for dispute resolution. If no progress can be made, then the sharing activity should be escalated to the Executive sponsor/s. At each escalation point in the pathway, the case for information sharing is presented and a decision is made on whether the information sharing agreement should proceed. Through this process, several other Queensland Government organisations may provide a specialist assistance and advice in dispute resolution, including:

* Queensland Government Chief Information Office
* Data Sharing and Analytics Office
* Queensland Government Statistician’s Office
* Office of the Information Commissioner.

# Permitted usage conditions model

Providing a standardised way to give permission to use shared information is crucial to addressing the issue of cultural change across the sector, particularly as Queensland Government service delivery occurs in a diverse and complex environment. This is similar to the Open Data model, where a mature set of [publishing standards](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au) already exists, including guidance on [privacy](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au/resource/eb191c58-2ae5-4f09-abb2-778fdde7c9e0), [risk assessment](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au/resource/d67132f8-27ac-4fdd-a0d9-d4bb639490d0), [de-identification](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au/resource/a64ee488-794a-4154-ad75-ecaf35c2674e) and [categorisation](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au/resource/19a9a82f-b3ba-48f9-9134-4ee9b76cdd28). Therefore, while the Permitted usage conditions model could be used to provide access to Open Data, it is highly recommended that existing resources are utilised to make this sort of information available through the [Queensland Government Data Portal](https://data.qld.gov.au/).

Empowering information owners and custodians to define permitted uses of shared information through a standardised model guarantees consistency of structure and provides conceptual familiarity for any parties engaging in a sharing activity. The permitted use model defined by the Framework leverages approaches and standards used in open licensing domains (including the Creative Commons[[3]](#footnote-4)).

When defining permitted uses of information under the model, the key activity is to identify and clearly describe any constraints on the usage of the shared information. Once defined, these constraints are clearly documented using the models structure and communicated to all parties of the sharing activity. The documenting of a set of usage permissions using a consistent structure ensures all parties are aware of the responsibilities and obligations when using information shared under an agreement.

There are four questions to consider when identifying constraints on shared information use. These are:

1. When can the information be shared or used?
2. How can the information be used?
3. Who can use information?
4. How can the exchange be approved?

Continuing the modularised philosophy of the Framework, not every information sharing activity will need to articulate constraints under each category and it is left up to the information custodian or owner to determine what constraints to identify when defining permitted uses of their shared information.

## Permissions model



Figure 11: *Permitted usage conditions model*

As illustrated by figure 11 above, there are four categories of constraints defined by the model. These are:

* **Time Frame / Trigger:** Restrictions on the timeframe in which information can be accessed and used. This includes the ability to define a ‘trigger’ event for execution (or the circumstances in which information can be released under the agreement).
* **Uses:** Restrictions on the way the shared information can be used.
* **Access:** Restrictions on who can access the shared information.
* **Authority:** Restrictions on who can approve the release of the shared information.

It is important to clearly articulate and define the constraints within each category with a focus on removing ambiguity and providing precision of intent. While the permitted usage condition model provides consistency in structure of permission definition, any implementation instance of the model is only as good as the clarity of the defined constraints. Any ambiguous constraint could be maliciously or inadvertently construed as to allow usage of information which contravenes its original intent. Therefore, it is crucial that any constraint is unambiguously defined.

## Permitted conditions

To assist with the clarity in constraint definition, the following set of permitted conditions are provided. These conditions aim to inform and guide the user of the permitted use model on best practice constraint definition. This list is by no means exhaustive and care should be taken by the user of the model to ensure any constraint accurately reflects their intent and ultimate information sharing objectives.

|  |  |
| --- | --- |
| 1. Constraint category | 1. Permitted conditions |
| 1. Time frame/Trigger | * No Restrictions * Between the dates of <date> and <date> * Until permission expires on <date> * Until superseded by <artefact> * Until the date of completion for the project / program as defined by Information Exchange Schedule (IES) * On the occurrence of an event or circumstance (as a trigger) |
| 1. Uses (based on the [Creation Commons](https://creativecommons.org/licenses/) licensing model) | * No Restrictions * Creative Commons derived licensing restrictions (such as Attribution, Non-Commercial, No Derivative Works, Share Alike) * Detailed scope of use descriptions which provide clear and unambiguous direction on usage of the information shared. * References to other binding artefacts (such as statement of work, project scoping document or specific legislation) which provide clear guidance on permitted uses of shared information |
| 1. Access | * No Restrictions: * By verified registration of an individual * Nominated groups / roles * Named individual * Only members of the project team as defined by the Information Exchange Schedule (IES) |
| 1. Authority | * No restrictions * Standard Approval process for release of information * Endorsed Master Sharing Agreement (and subordinate Information Exchange Schedule) * Nominated group/roles * Named individual |

Table 2: Standard *permitted conditions* table

## Example scenarios

### Disaster management

Six hours ago, Cyclone Waldo crossed the coast between Townsville and Ingham with widespread damage anticipated across the region. In response to the extreme weather event, the Premier has declared the area a natural disaster under the *Disaster Management Act 2003*. An MSA for disaster management has been previously established and endorsed by the Chief Executives of all participating agencies to allow sharing of information in a declared disaster situation.

The following is an example of the permitted usage conditions that could be defined under this scenario.

**Definitions**

|  |  |
| --- | --- |
| Information to be shared | Parties to the agreement |
| 1. Any information pertaining to the provision disaster management operations and services | 1. All parties responsible for the emergency support functions when a disaster has been declared |

**Permitted usage conditions**

|  |  |
| --- | --- |
| 1. Time frame/Trigger | 1. In the event of the Premier declaring a disaster, the information defined by the MSA and subordinate IES may be shared with all parties under that agreement. |
| 1. Uses | 1. The information defined by the agreement may only be used by all parties of the agreement for the strict purposes of ‘Disaster Management’ and ‘Disaster Operations’ as defined by the *Disaster Management Act 2003* and subordinate legislation. |
| 1. Access | 1. Access to the information shared under the agreement is restricted to persons defined by the *Disaster Management Act 2003* and subordinate legislation |
| 1. Authority | 1. The Authority to share the information is given by the Master Sharing Agreement for Disaster Management which has been endorsed by the Chief Executive of each participating agency. |

Table 3: Disaster Management Scenario Example

### Data insights and analytics

The Department of Housing and Public Works (HPW) Data Analytics and Insights team have been asked to conduct some analysis on cross-agency workforce data by the Public Service Commission (PSC). The objective is to identify trends in the public-sector workforce to assist in developing Whole-of-Government workforce management strategies. A Master Sharing Agreement for workforce data has been established with both HPW and the PSC listed as signatories. Additionally, an Information Exchange Schedule has been developed and endorsed for this distinct engagement.

The following is a proposed example of what the Permitted Usage Conditions may look like for this scenario.

**Definitions**

|  |  |
| --- | --- |
| Information to be shared | Parties to the agreement |
| 1. The Minimum Obligatory Human Resource Information (MOHRI) dataset of which the PSC is the primary custodian (as defined by the Information Exchange Schedule) | 1. Both HPW and PSC are signatories to Whole of Government Master Sharing Agreement for Workforce Data. |

**Permitted usage conditions**

|  |  |
| --- | --- |
| 1. Time Frame/Trigger | 1. The HPW Data Analytics and Insights team may only have access to the defined dataset for the length of the defined analytical engagement (defined by the Analytical Approach Definition), or for a period of 6 months (whichever occurs first). |
| 1. Uses | 1. The dataset shared under the information exchange schedule must only be used for the purposes and objectives as outlined under the “Analytics Approach Definition”. No further derivative works may be conducted on the outputs of this process |
| 1. Access | 1. Access to the shared dataset is limited to the explicit project team members as defined by the Information Exchange Schedule. Access to the outputs of the engagement (defined by the Information Exchange Schedule) is also restricted to project team members and must not be shared |
| 1. Authority | 1. The Authority to share the dataset for this engagement is provided by  * the Master Sharing Agreement for Workforce Data which has been endorsed by the Chief Executives of HPW and the PSC; and * the subordinate Information Exchange Schedule for this analytics engagement which has been endorsed by DDG PSC and ED of HPW.   The Authority to share for this engagement may be modified or altered at any time by the either Chief Executive of both agencies. |

Table 4: *Data Insights and Analytics* Scenario Example

# Manage phase

**MANAGE**

APPLICABLE QGEA POLICIES

* Information asset custodianship policy (IS44)
* Retention and disposal of public records (IS31)
* Recordkeeping (IS40)

KEY PHASE OBJECTIVES

* Validate and review key aspects of the information sharing activity
* Define (and review) the Information Exchange Schedule (IES) which provides detail on how the sharing is enacted
* Define and review audit and compliance requirements of the information asset owner/s to assure trust over the sharing activity
* Define obligations and responsibilities when ending an information sharing activity.

The *Manage* phase is the core phase of the Framework, as its primary focus is to manage The *Manage* phase is the core phase of the Framework as its primary focus is to manage an established information sharing activity over its lifecycle. This phase is the ‘default’ phase of the Framework and where the information sharing activity resides once it has successfully entered a production state.

For any new information sharing activity, the *Manage* phase should occur immediately after the conclusion of the *Prepare* phase (and the establishment of a MSA). The first activity is to define the detail of the sharing activity into an IES for further endorsement. The IES also validates the defined controls, permitted usage conditions and assumptions for the sharing activity and positions it for implementation. Importantly, any assurance requirements are defined in this phase. These assurance requirements should confirm the adherence to any defined controls and provide clarity on the accountabilities for the sharing activity. These assurance requirements form a key component of the trust through transparency philosophy which underpins the Framework.

The *Manage* phase can also be used as a periodical review mechanism for any active information sharing activity. The revalidation of assumptions, controls and conditions defined in the agreement allows the evaluation for relevancy, value and purpose. Additionally, any innovation or improvement opportunities identified elsewhere in the framework are formally evaluated and implemented in this phase.

This phase also includes a sub-phase for the ending of an information sharing activity. The premise is to ensure that all retention and disposal obligations and deletion requirements are met and the activity is retired cleanly. Figure 12 on page 29 provides an overview of the *Manage* phase.

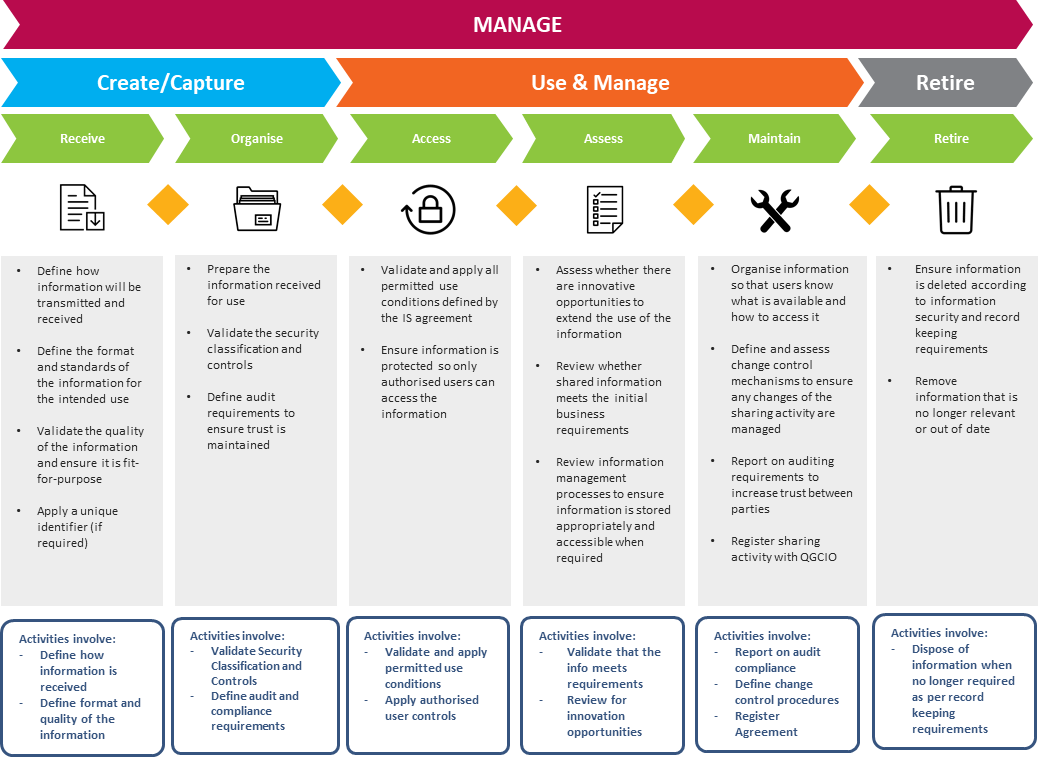


Figure 12: The *Manage* phase

## Create/Capture

This sub-phase validates the objectives and conditions defined in the MSA (which was established in the previous *Prepare* phase). If the MSA is well formed and complete (which is assumed to be in most cases) these validation activities should be a ‘tick-and-flick’ type exercise, however, the importance of conducting the validation task should not be understated. This is particularly important if a large amount of time has lapsed since establishing the MSA, or if large personnel differences exist between the team who established the MSA and the team defining the IES. The identification of any errors, omissions or inaccuracies in the MSA or the identification of any significant data quality issues present in the information to be shared, will prevent unnecessary remediation or scope change costs in subsequent phases.

It is also important in this sub-phase to collate all controls, permitted uses and legal requirements defined in the previous phase for inclusion into the IES. By formalising requirements, conditions, and standards into a single authorising artefact, it allows any gaps to surface, provides clarity when moving to subsequent phases and forms a single source of truth for all constraints on the sharing activity. For example, the MSA may define the information to be shared and describe who may access it, but it may not determine how and where this access might take place (for example on a mobile device) or provide enough granular detail on user access controls for implementation. In the case where an existing IES is being periodically reviewed, this sub-phase confirms that the requirements and controls defined in the IES are still relevant and valid.

This sub-phase also defines how the information will be transmitted and received by all parties and importantly, what audit and compliance artefacts are required to assure the information sharing activity. Any audit requirements should focus on providing a clear and detailed view on the operation of all critical sharing conditions and controls crucial to maintain high levels of trust across all parties. Some options for the audit requirements are:

* registering each information transmission activity between parties across the entire information flow (may include a unique identifier for traceability)
* providing a comprehensive log of all user access to the information shared under the agreement
* providing real-time access to all audit mechanisms for all information custodians defined under the agreement.

Well-formed audit requirements should aim to foster greater trust in the sharing activity - not only within the participating parties, but also within the broader community. It is important for the Queensland Government to demonstrate that it is using the information it has, in the best interests of the community it serves. All assurance requirements once defined should be agreed to and endorsed by all parties to the information sharing activity. Figure 13 on page 31 outlines the key activities of this sub-phase.

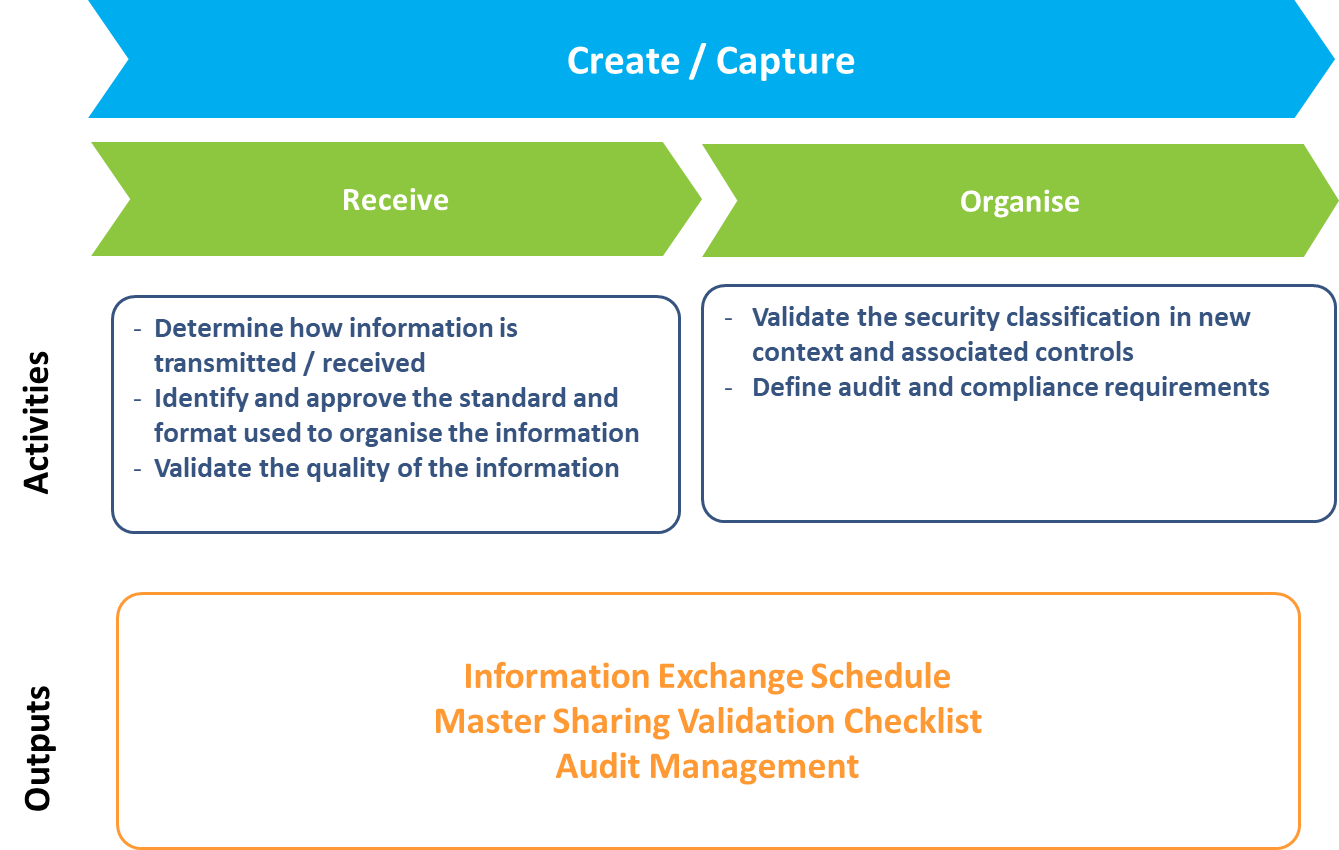


Figure 13: The *Create/Capture* sub-phase of the *Manage* phase

## Use and manage

Primarily, the core focus of this sub-phase is to define and review the management structures that control the information sharing activity. This involves assessing the sharing activity for alignment with the stated benefits. Also, any change control processes to manage change over the lifecycle of the sharing activity are defined here and any innovation opportunities can be formally assessed and incorporated into the sharing activity at this point too. If an operational service level agreement is required to confirm the ongoing availability of the information, it also is defined and agreed to through this sub-phase. Figure 14 on page 32 outlines the key activities.

While this sub-phase focuses on defining controls for using and managing the information sharing activity, the method in which this is achieved is left up to the practitioner. The key point here is that these management items are considered in this sub-phase, and if required, implemented. For example, if the sharing activity requires change control mechanisms to manage change over its lifecycle, then these should be considered and included in this sub-phase. The methodology used to define these change control mechanisms is left up to the practitioner. It is recommended that practitioners consult their agency specialists and align with agency best practice when selecting appropriate methodologies or standards.

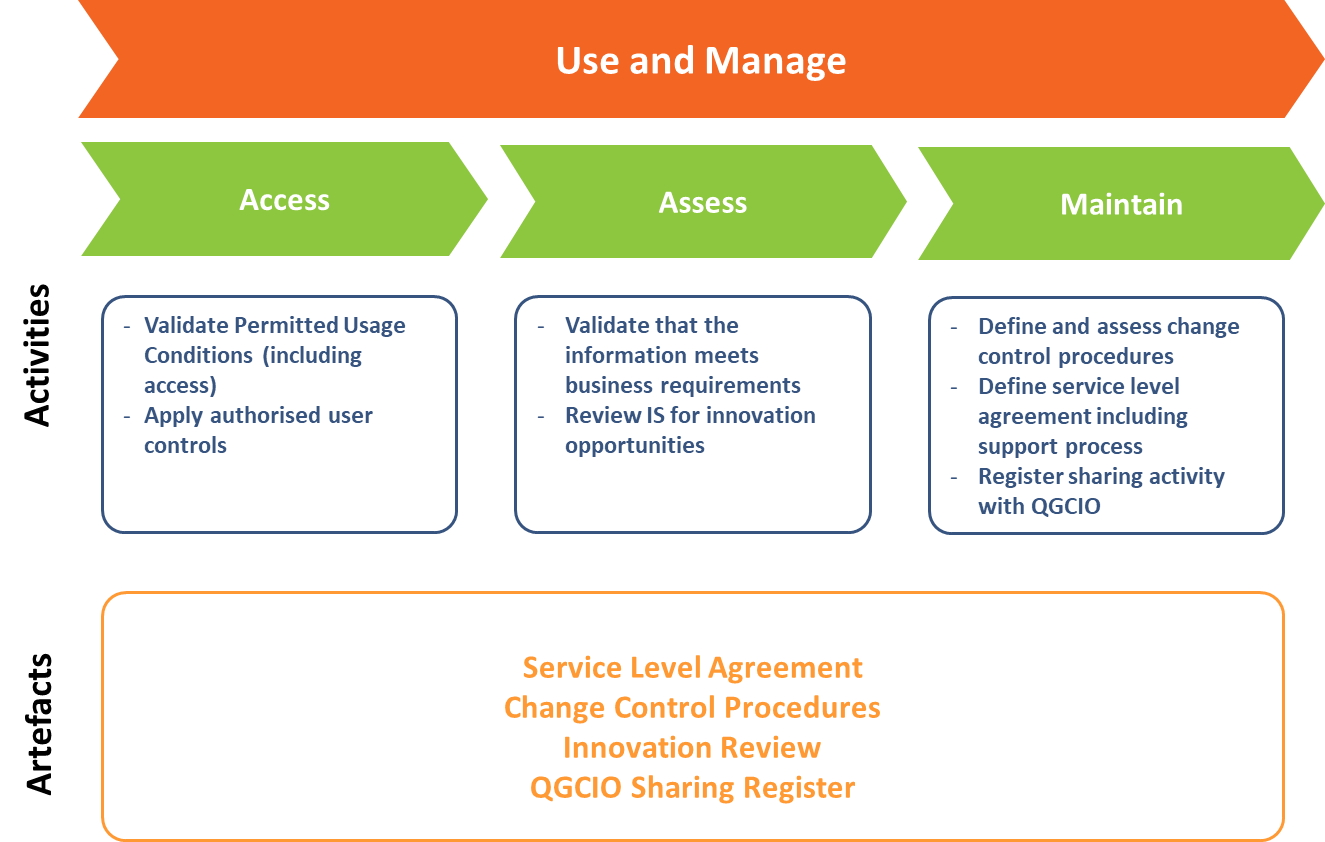


Figure 14: The *Use and manage* sub-phase

## Retire

The *Retire* sub-phase defines the process for ending any information sharing agreement. It ensures that disposal obligations and deletion requirements (considering any recordkeeping responsibilities) are met by all parties once an information sharing activity has reached its end of life. Retaining disposal documentary evidence is an important output of this sub-phase as it confirms that the information shared under the agreement has been disposed of in the correct manner. In some circumstances, the retention of this evidence is mandated by legislation. Further information regarding recordkeeping responsibilities, including disposal can be obtained from [Queensland State Archives](https://www.qld.gov.au/dsiti/qsa), the [Public Records Act 2002(Qld)](https://www.legislation.qld.gov.au/view/html/inforce/current/act-2002-011) and the relevant [Retention and Disposal schedule](https://www.forgov.qld.gov.au/find-out-how-long-keep-records-sentence-records). Figure 15 on page 33 outlines the key task of this sub-phase.

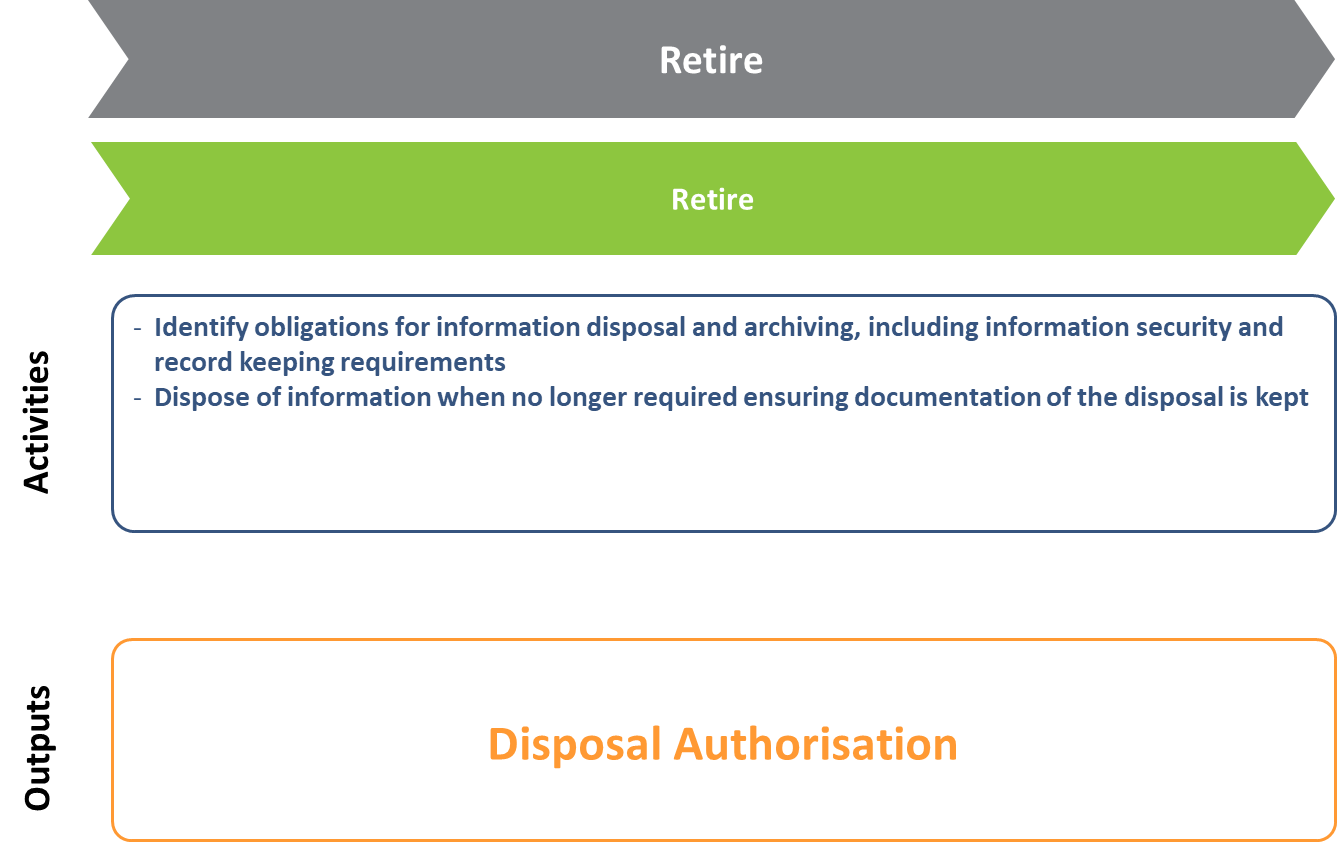


Figure 15: The *Retire* activity

# Exchange phase

KEY PHASE OBJECTIVES

* Technically validate the information sharing activity
* Design the architecture of exchange and presentation of information in scope of the sharing activity
* Build, test and validate the exchange for integrity, accuracy and compliance
* Implement the information exchange activity

APPLICABLE QGEA POLICIES

* Information security (IS18)
* Customer details management policy

**EXCHANGE PHASE**

The *Exchange* phase contains all implementation activities to enable the exchange and use of shared information. This phase will evolve the IES, permitted usage conditions, and other important artefacts defined in previous phases into several design constructs for implementation. These include technical architectures, transmission structures (including use of standard data schemas) and user interface (UI)/user experience (UX) wireframes for presentation of the information. A test environment is then built based on these design constructs and subsequently validated across several metrics including integrity, usability, accuracy, consistency and auditability. Once fully tested and validated, the information exchange solution is launched into production for users to consume the information shared under the agreement.

In accordance with the philosophy of the framework, the number of design constructs required will be determined by the complexity and objectives of the information sharing activity. For example, if the information exchange activity is a once off exchange of data to contribute to an analytics process, then the architecture and UI wireframe design constructs may not be required. However, this might not be the case if the analytics activity is ongoing and regular automated transmission of information is required between multiple parties. Likewise, if the information sharing activity involves the real time sharing of information for consumption by a user in a service delivery scenario, then it will be important to design architectures, transmission paths and UI/UX presentation constructs accordingly. Figure 16 on page 35 provides an overview of the *Exchange* phase.

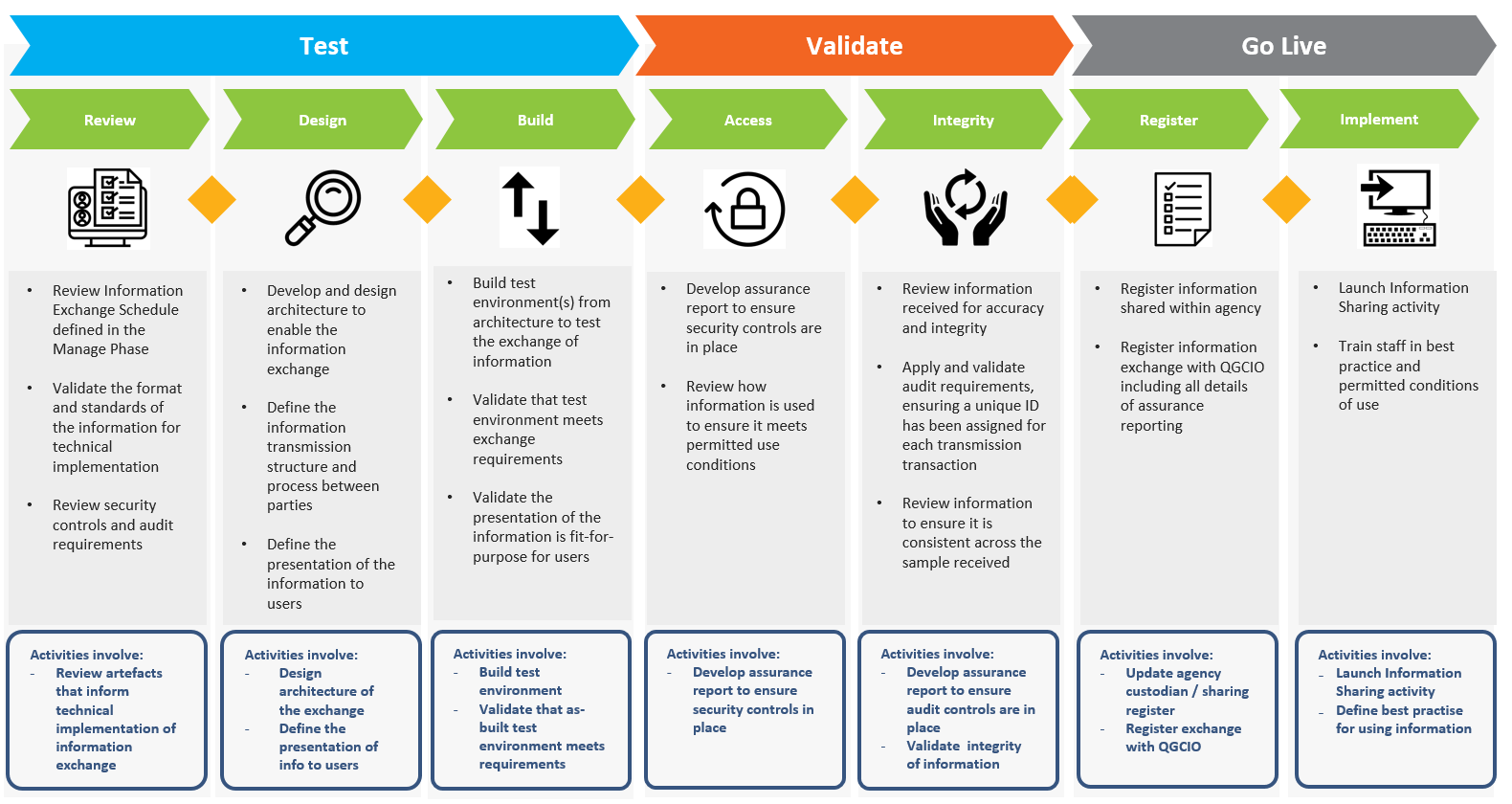


Figure 16: The *Exchange* phase

## Test

Where appropriate, the development of a fully featured test environment is the first step in developing an information sharing solution. To achieve this, it is important to review and technically validate the IES, the format and standards of information to be shared and the security and assurance controls defined in previous phases. A review of the schedules, requirements, formats and controls through a technical lens will ensure any issues or errors are identified and remedied prior to build commencement.

Once reviewed for technical suitability, the design of the information exchange can begin. This involves the design of the architecture, transmission paths and the presentation for the exchange. As mentioned, the detail in the design constructs will vary depending on the complexity and the underlying objectives of the information sharing activity. However, it will be important that some design thinking and documentation takes place for all information sharing activities. It is crucial that design documentation is approved and agreed to by all parties and relevant stakeholders responsible for implementation of the information exchange.

The last step in the test sub-phase is to build the test environment based on the agreed design specifications. The build process will focus on validating that the information exchange aligns with the intended benefits and that the presentation of the information to the user is fit-for-purpose. Engagement with representatives from customer experience or insight teams in this activity may be useful. Figure 17 below outlines the key task of this sub-phase.

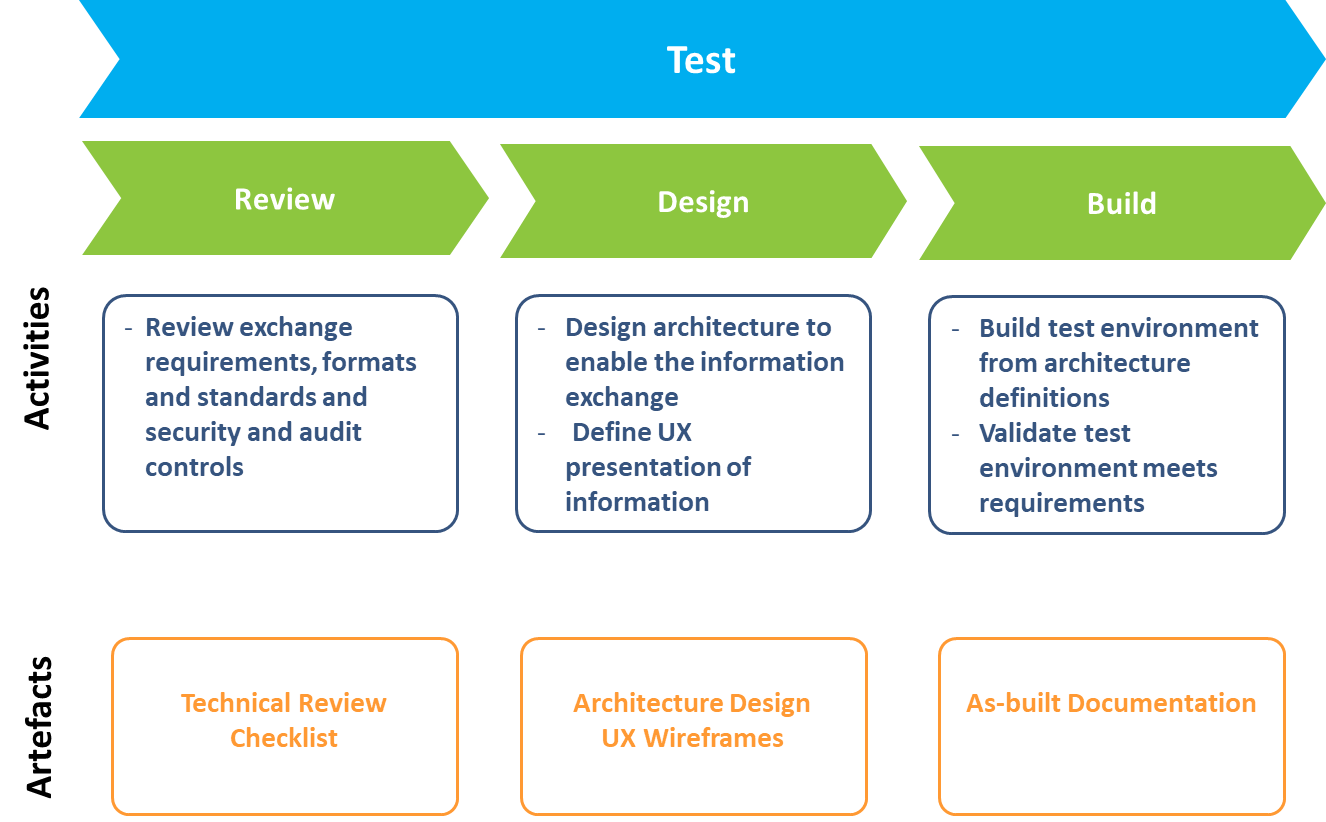


Figure 17: The *Test* sub-phase

## Validate

Validation of the built test environment is a crucial sub-phase as it confirms the appropriateness of the technical implementation across several metrics including integrity, usability, accuracy, consistency and auditability. Ensuring that the implementation of the sharing activity includes all the required security controls, provides visibility on use through sufficient auditing requirements, and verifies the integrity of the information across the information flow, are all crucial to success. The critical output of this sub-phase is a suite of assurance reports that validate the implementation of the sharing activity. Providing clear visibility to all parties of these assurance reports will support trust through transparency for all aspects of the sharing value chain.

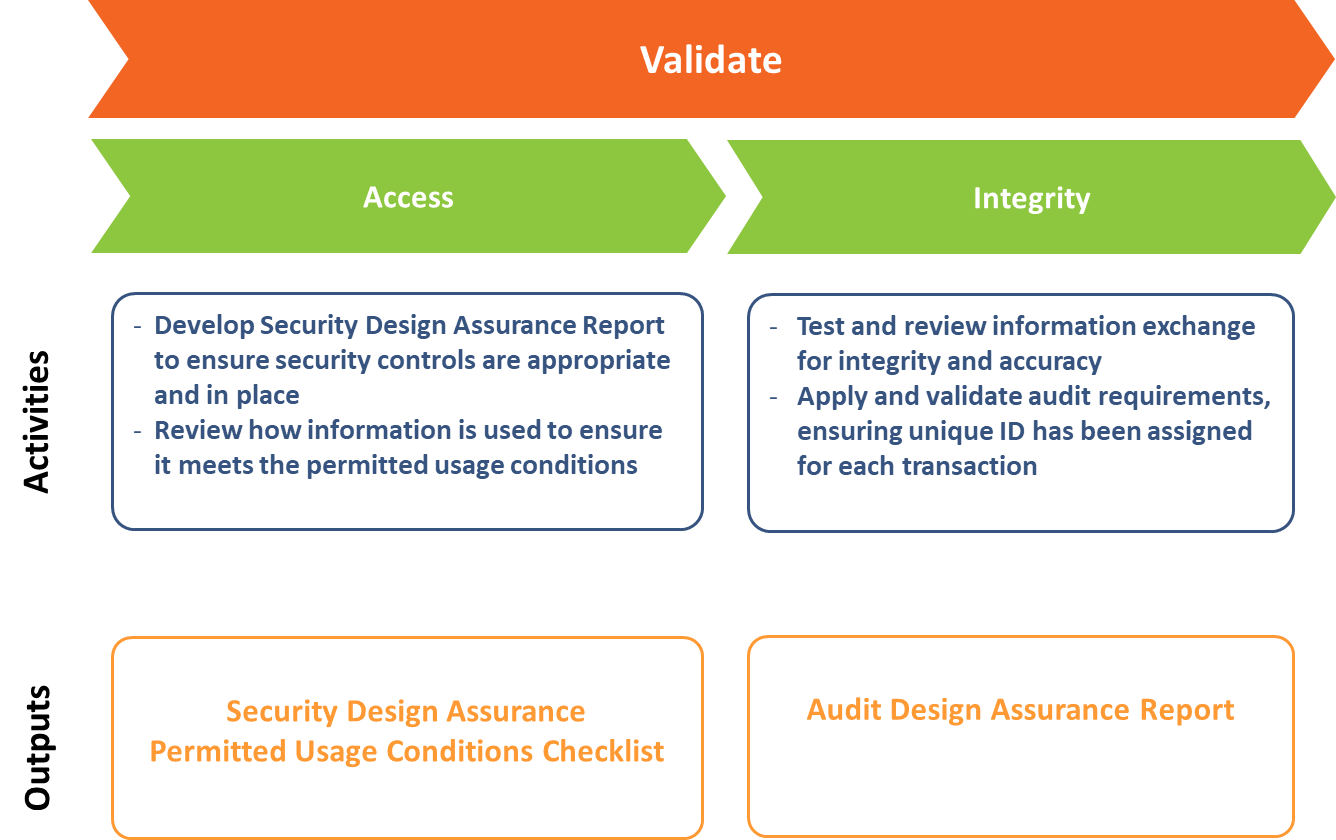


Figure 18: The *Validate* sub-phase

## Go-live

Once the test environment is built and validated across the entire information flow, the information sharing solution is ready to enter its production state. In addition to the state change to production, the ‘go-live’ sub-phase involves several administrative processes to support the wider information sharing ecosystem - both internal to the sponsoring agencies and across Queensland Government. These include:

* The addition of the information sharing activity to the agency information exchange register that contains all information assets shared with other entities by the agency (this is complementary to the information asset register as defined by the [Information asset custodianship policy](https://www.qgcio.qld.gov.au/documents/information-asset-custodianship-policy-is44)). To enable potential leverage from these sharing initiatives, agencies are encouraged to consider publishing this register (subject to confidentiality, privacy and security considerations) on their website in alignment with requirement 2 of the [Information access and use (IS33) policy](https://www.qgcio.qld.gov.au/documents/information-access-and-use-policy-is33).
* Including the information sharing activity in the QGCIO managed WoG [Information sharing agreements exchange register](https://www.qgcio.qld.gov.au/information-on/information-management/what-information-is-shared/information-sharing-agreement-register) (Queensland Government employees only) which will not only increase the visibility of existing sharing initiatives, but also promote the re-use of existing agreements.
* Providing the details of the sharing initiative for inclusion in the QGCIO’s [Information Sharing Pattern Library](https://www.qgcio.qld.gov.au/information-on/information-management/what-information-is-shared) (ISPL) which provides information about the potential benefits agencies gain from sharing information. The ISPL also aims to highlight the common barriers that inhibit information sharing as well as enablers that support effective sharing arrangements.

It is important that detailed documentation be developed for users that outlines how shared information is to be used (based on the permitted usage conditions defined in previous phases) and that users are ready to begin further training on the use of the shared information. This initial best-practice documentation will form key part of training program development in the next phase (the *Use* phase). Figure 19 below outlines the key task of this activity.

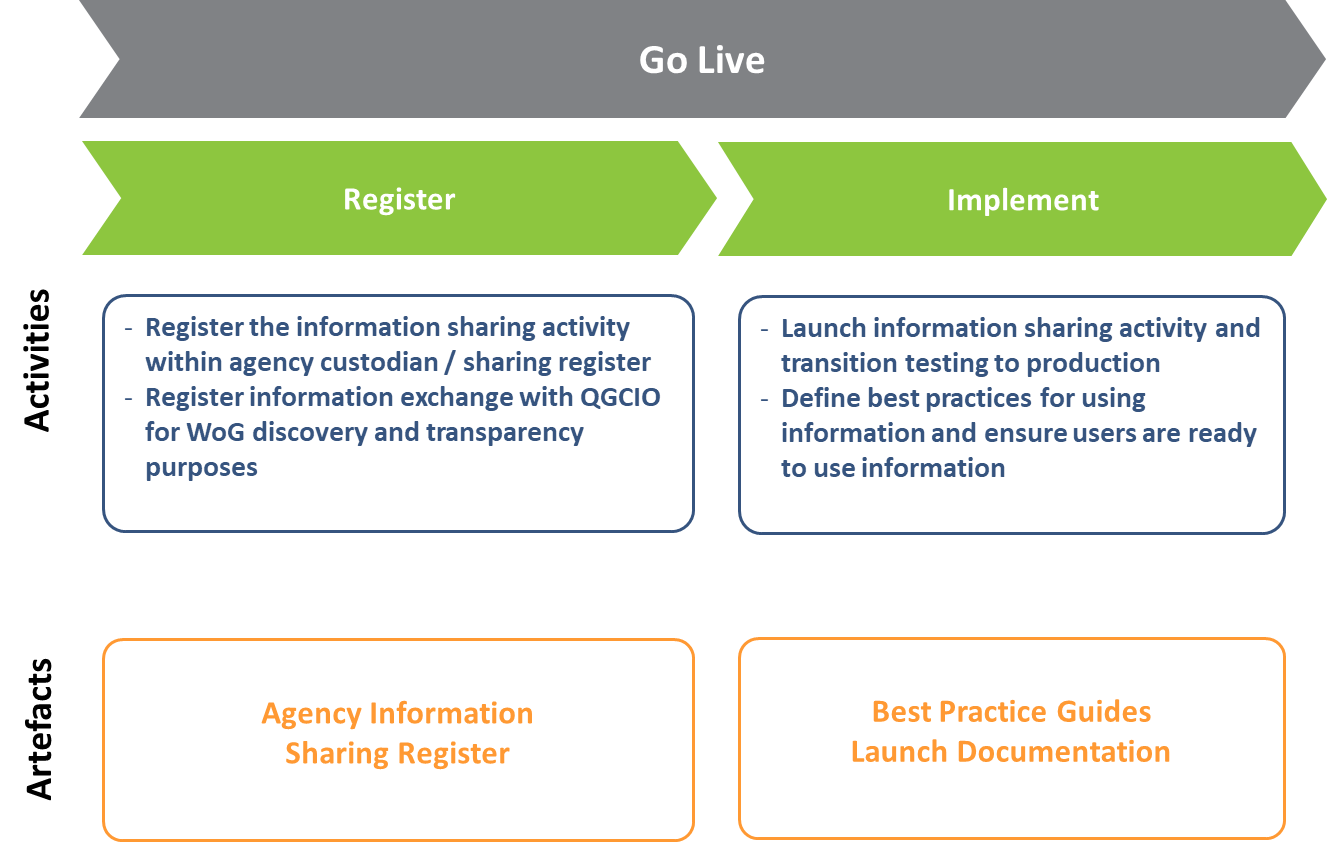


Figure 19: The *Go Live* sub-phase

# Use phase

**USE PHASE**

APPLICABLE QGEA POLICIES

* Information security (IS18)

KEY PHASE OBJECTIVES

* Provide training resources and programs so that consumers of the shared information maximise its utility
* Define and conduct analytics activities on shared information ensuring outputs are documented and controlled
* Assure information is being used and consumed as permitted by defined controls

The *Use* phase provides structures and outputs for the access, use and analysis of the shared information. This includes building and strengthening user’s awareness on the scope and limitations of use of the shared information, educating users on the support channels where issues with the information can be resolved and providing innovation and improvement channels where users can improve the sharing activity. This phase also provides guidance on structuring and documenting any analysis and insights activities conducted on the information and tracks the usage and utility of the information sharing activity. Like other phases defined in this framework, the use of the activities in this phase will be dependent on the type of information sharing activity being undertaken and the overall intended outcomes. Figure 20 on page 40 provides an overview of the *Use* phase.

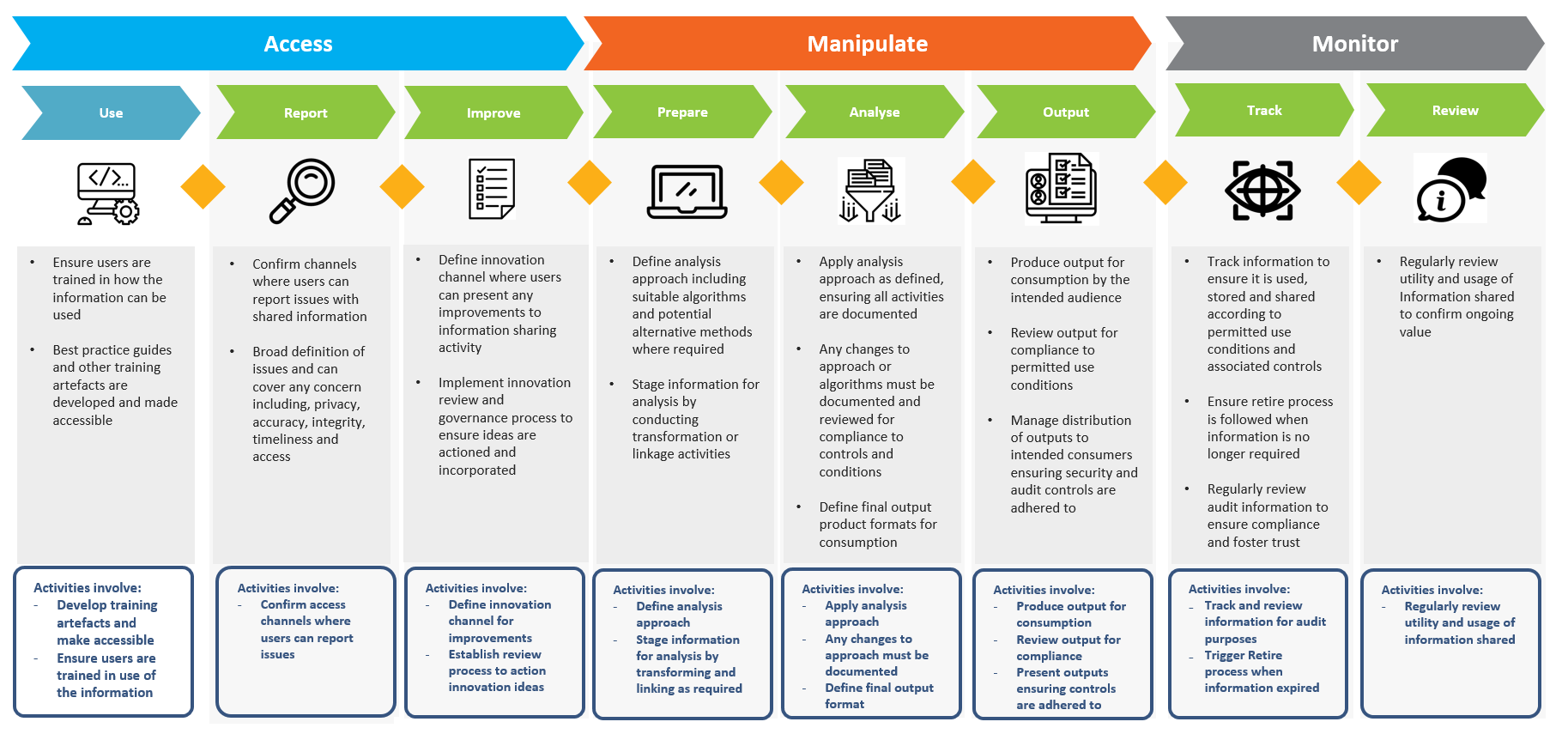


Figure 20: The *Use* phase

## Access

The *Access* sub-phase focuses on maximising the usage value and utility of the information shared. This involves providing comprehensive, structured training programs and associated artefacts to all users to build an awareness of the overarching purpose and limitations of the shared information. This awareness and knowledge aims to reduce inadvertent disclosure of any information and foster greater trust through transparency across all parties.

Furthermore, this sub-phase confirms the support channels defined by service level agreement and focuses on educating users on the process to resolve any issues with the shared information. The definition of an ‘issue’ in this context is very broad and can include (but is not limited to) items such as privacy, accuracy, integrity, timeliness and access control. Providing a clearly defined and structured approach to issues management will allow any issues impacting the usability of information to be addressed in a timely manner.

Additionally, this sub-phase provides a structured approach to eliciting innovation and improvement ideas from the users and consumers of the information. Generally, everyday users and consumers of information are best placed to provide guidance on innovation or improvements. Any innovative ideas captured as part of this process can be included for evaluation and incorporation in the *Assess* activity under the *Manage* phase. Figure 21 below outlines the key activity of this sub-phase.

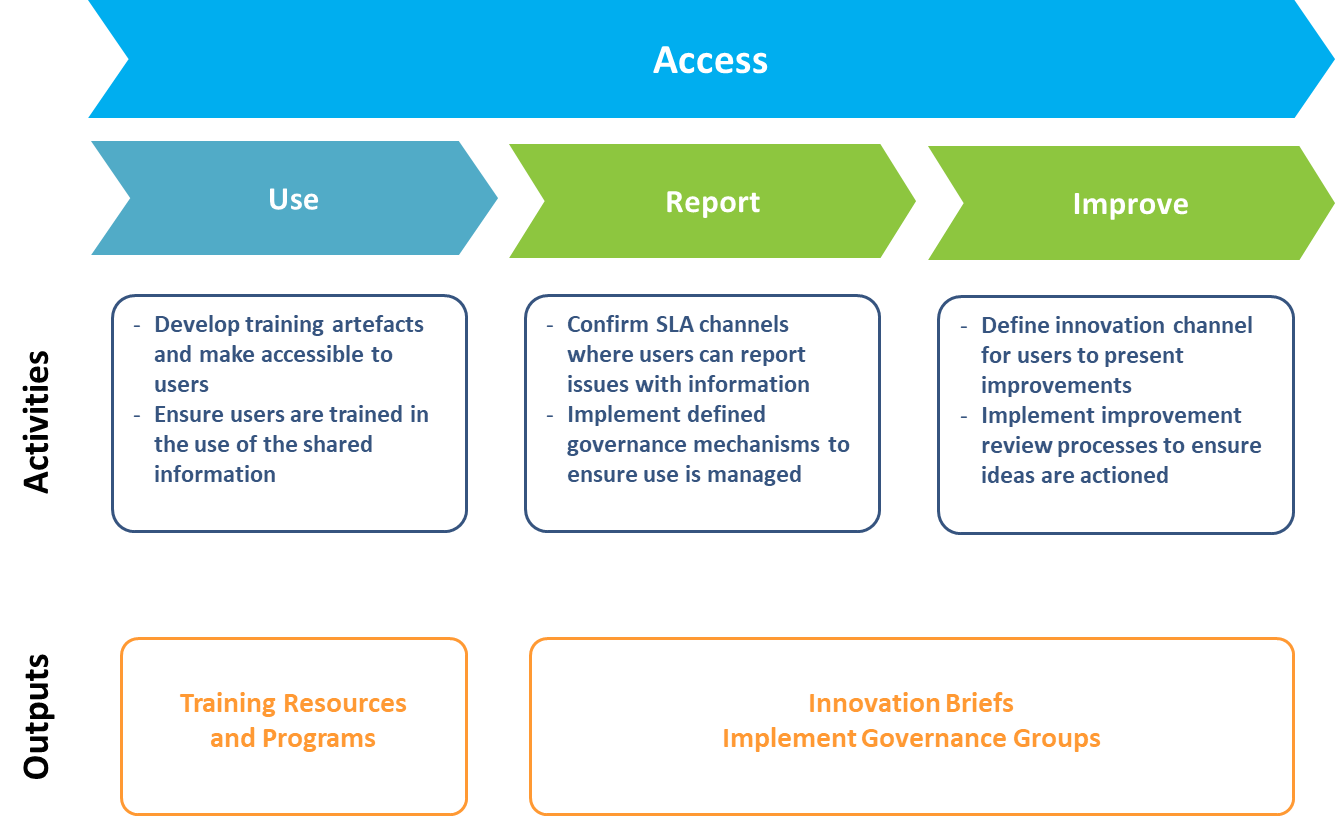


Figure 21: The Access sub-phase

## Manipulate

The *Manipulate* sub-phase provides a high-level structure for defining and documenting the preparation, analysis and final output of analytics or data science analysis activity. Clear and transparent documentation on approach, execution and output of the analytics activity will ensure the quality of the output and trust maintain trust across the information sharing activity.

The *Prepare* activity documents the analysis approach and stages the information for use by transforming, linking or de-identifying as required. Importantly, the analysis definition here should include any expected outputs of the analysis and identify any alternative approaches that might be required. The *Analyse* activity then proceeds to execute the approach with clear points for documentation and review as the analysis progresses.

Once completed, the final output format is defined and reviewed for alignment with the permitted usage conditions defined in the MSA and the final output is produced and distributed to the intended consumers. For auditing purposes, it may be important to define how the output is transmitted (i.e. through secure channels – this particularly true if the output is sensitive in nature) and keep an audit log of who has received the output. Figure 22 below outlines the key task of this sub-phase.

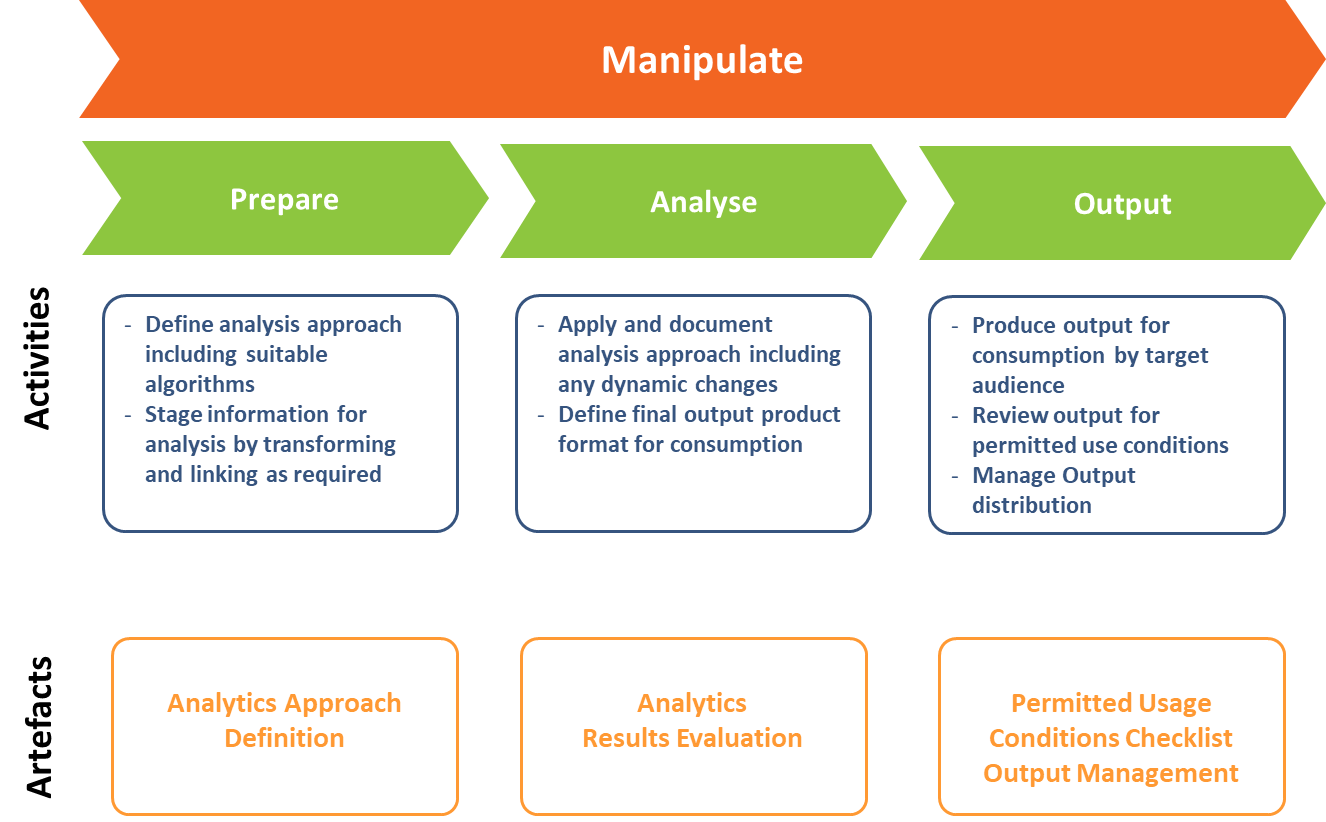


Figure 22: The *Manipulate* sub-phase

## Monitor

The *Monitor* sub-phase confirms that all access, use and storage of the information shared is audited and tracked as per the defined requirements. This process also links back *Retire* sub-phase to ensure the appropriate process is followed when the information or output is no longer required.

Additionally, this sub-phase links to the review and validation mechanisms defined in the *Manage* phase, including the audit requirements review and the fit-for-purpose review. The *Monitor* sub-phase is the end of the *Use* phase and confirms the return of the information sharing activity back to the *Manage* phase. Figure 23 below outlines the key task of this sub-phase.

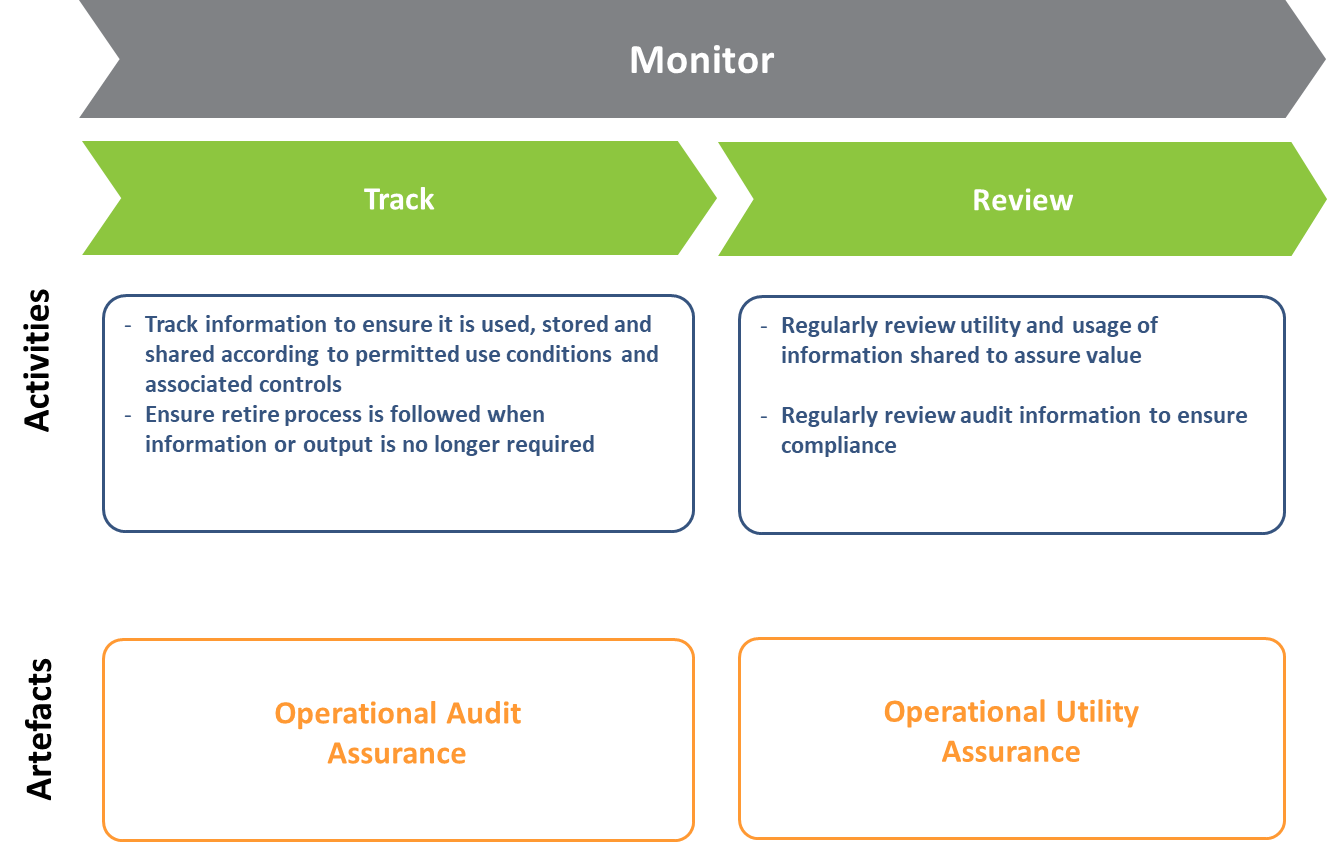


Figure 23: The *Monitor* sub-phase

1. Supporting output artefact summary

Prepare phase

|  |  |
| --- | --- |
| Core activities by sub-phase | Key outputs |
| 1. Organise  * Identify value * Identify owners and custodians * Define benefits | 1. Benefits proposition Summary (Information sharing business justification) 2. Risk assessment |
| 1. Evaluate  * Review legislation * Personal information review * Review security classification | 1. Privacy impact assessment report 2. Legislation mapping and review report 3. Information security classification report |
| 1. Enable  * Define purpose of sharing * Obtain agreement | Information flow map  Permitted usage conditions document  Master sharing agreement |

Manage phase

|  |  |
| --- | --- |
| Core activities by sub-phase | Key outputs |
| 1. Create and capture  * Receive * Organise | 1. Information exchange schedule 2. Master sharing validation checklist 3. Audit requirements |
| 1. Use and manage  * Access * Assess * Maintain | 1. Service level agreement 2. Change control procedures 3. Innovation briefs 4. QGCIO sharing register |
| 1. Retire  * Retire * Dispose | 1. Disposal authorisation |

Exchange phase

| Core activities by sub-phase | Key outputs |
| --- | --- |
| 1. Test  * Review * Design * Build | 1. Technical review checklist 2. Architecture design 3. UX wireframes 4. As-built documentation |
| 1. Validate  * Access * Integrity | 1. Security design assurance 2. Permitted usage conditions checklist 3. Audit design assurance |
| 1. Go Live  * Register * Implement | 1. Agency information sharing register 2. Best practice guides 3. Launch documentation |

Use phase

|  |  |
| --- | --- |
| Core activities by sub-phase | Key outputs |
| 1. Access  * Use * Report * Improve | 1. Training resources 2. Innovation briefs |
| 1. Manipulate  * Access * Integrity | 1. Permitted usage conditions checklist 2. Analytics approach definition 3. Analytics results evaluation 4. Analytics output management |
| 1. Monitor  * Track * Review | 1. Operational audit assurance 2. Operational utility assurance |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Key changes made |
| 0.0.1 | 18th Sept 2017 | Jay Sindorff | Initial version. Translation of GWI consultancy outputs into QGEA Guideline |
| 0.0.2 | 25th Sept 2017 | Shane Marshall | Review and update |
| 0.0.3 | 9th October 2017 | Jay Sindorff | Moved the IES from Prepare to Manage, Added diagram of output artefacts  Added five safes appendix C Minor updates to lexicon for clarity |
| 0.1.0 | 13th October 2017 | Shane Marshall | Early informal consultation draft |
| 0.1.1 | 16th October 2017 | Jay Sindorff | Added updated diagrams to early informal consultation draft |
| 0.1.2 | 24th October 2017 | Jay Sindorff | Further minor updates |
| 0.2.0 | 7th November 2017 | Jay Sindorff | Incorporation of internal QGCIO feedback |
| 0.2.1 | 14th November 2017 | Jay Sindorff | Final Consultation Draft |
| 0.2.2 | 26 February 2018 | Lisa Irwin | Review and QA check |
| 1.0.0 | March 2018 | QGCIO | Approved by Andy Stokes |

1. Australian Computer Society, ‘A Framework for Trust’, *Data Sharing Frameworks: Technical White Paper*, p 65, September 2017 https://www.acs.org.au/content/dam/acs/acs-publications/ACS\_Data-Sharing-Frameworks\_FINAL\_FA\_SINGLE\_LR.pdf [↑](#footnote-ref-2)
2. Office of the Chief Information Commissioner, *Overview of the Privacy Impact Assessment (PIA) Process*, July 2017, https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process [↑](#footnote-ref-3)
3. https://creativecommons.org/licenses/ [↑](#footnote-ref-4)