Data Exchange Guideline

Data Exchange Framework

VICTORIA State Government | Premier and Cabinet

Document Control

Applies to	All departments and Victoria Police	**Authority**	CIO Leadership Group
Period	2019-2021	**Advised by**	WOVG Information Management Group
Issue Date	August 2019	**Document ID**	IM-GUIDE-10
Review Date	August 2021	**Version**	1.0

Approval

This document was approved by the WOVG Information Management Group under authority of CIO Leadership Group on 02/07/2019 and applies from the date of issue.

Version history

Version	Date	Comments
0.1	14/05/2019	Version for review by stakeholders
0.2	30/05/2019	Incorporated feedback
1.0	07/06/2017	Final

Contents

Introduction

Overview

This Data Exchange Guideline (guideline) provides high-level advice to Victorian Government (government) departments and Victoria Police on evaluating, managing, authorising and undertaking data sharing. This guideline will assist data owners and custodians (from within the business), data requestors, data and information management practitioners and information technology specialists to understand and implement the Data Exchange Standard (standard) along with the supporting tools and templates.

The guideline provides further advice and clarification on the minimum considerations that need to be considered in order to exchange data, the business rules that should be applied and use of tools to help in the assessment and management of data exchanges.

There may be further requirements around data exchange that apply specifically to your department or portfolio. It is recommended that you refer to the relevant authorities (legislation, regulations, policies, etc.) for the requirements and guidance.

In this guideline, ‘data’ refers to structured data.[1] Unstructured data is not covered by this guideline.

In this guideline, ‘exchange’ is synonymous with sharing and refers to the transferring of data in a secure, authorised and predefined way, whether automated; real time or near real time; system to system; via email; via secure file transfer; bulk uploads or once-off any other form of exchange not listed above e.g. USB.

Unless stated otherwise, all references to ‘sensitive’ data have the definition as provided in the Glossary.

This guideline should be read in conjunction with the following documents:

- Data Exchange Framework
- Data Exchange Standard (business rules)
- Data Request Template
- Data Exchange Request Evaluation Checklist
- Data Exchange Technical Specification Template.

[1] 'Structured data' refers to data that can be organised and stored in fixed fields such as in a relational database record or spreadsheet. 'Unstructured data' does not conform neatly into a fixed field format. Examples include: data streams, social media data, documents, emails, videos, audio files, and images.

Rationale

Sharing data with other departments, agencies and external parties and releasing information to the public helps to increase the value of the government's investment in information by creating an opportunity for reuse and repurpose of data.

In order for government to make better decisions, create better value and services for its citizens, departments must be able to exchange and integrate data with each other in an appropriate manner, in a safe and secure environment.

Data exchange involves many variations in legislative, regulatory, policy and or contractual requirements, types and formats of data, security classifications, processes and protocols, capabilities, capacities and appetites for risk that impact the ability and for one organisation to exchange data with another organisation.

To enable data exchange to occur in a consistent manner, a Whole of Victorian Government (WOVG) Data Exchange Framework (framework) has been developed to standardise the data exchange approach, regardless of data type, classification, exchange method, platform, or intended use.

To support the implementation of the framework, a standard was developed to provide the minimum requirements (business rules) and considerations to enable data to be exchanged. This guideline, in turn, aims to assist departments in how to apply the standard and evaluate, manage, authorise and undertake data exchange in a consistent manner across all of government.

Derivation, scope and glossary

Derivation

This guideline is derived from the framework and standard and is guided by the Information Technology Strategy Victorian Government, 2016–2020 (IT Strategy).

Scope

All departments and Victoria Police, referred to collectively as 'departments', are formally in-scope. While not required, the standard may be adopted by agencies and partner organisations, if desired.

Audience

The guideline is targeted at data owners and data custodians (from within the business), data exchange requestors, data and information management practitioners and information technology specialists.

Glossary

Unless otherwise stated, the glossary of terms and abbreviations used in this document are defined in the Information Management Glossary.

Term	Definition
Data custodian	As defined in the Information Management Glossary: A custodian is a nominated individual who is formally accountable for day-to-day management of the delegated assets in their care.
Data owner	As defined in the Information Management Glossary: An owner holds responsibility for management of specified data assets within a department or organisation.
Provider	Department providing the data.
Requestor	Department requesting the data.
Sensitive data	Data with a Business Impact Level (BIL) of Limited or higher or data with a protective marking of Cabinet-in-Confidence (as per the Office of the Victorian Information Commissioner's (OVIC) guidance on Business Impact Levels and Protective Markings).

Related documents, tools and references

- Australian Government Locator Service (AGLS) Metadata Standard
- *Copyright Act 1968 (Cth)*
- DataVic Access Policy and Guidelines
- Data Sharing Frameworks (Australian Computer Society (ACS))
- De-identification and Privacy – Considerations for the public sector (OVIC)
- De-identification and the Privacy Act (Office of the Australian Information commissioner (OAIC))
- De-identification Decision-Making Framework (OAIC)
- *Evidence Act 2008 (Vic)*
- *Financial Management and Accountability Act 1997 (Cth)*
- *Freedom of Information Act 1982*
- *Health Records Act 2001 (Vic)*
- Information Management Framework, Standards, Policies and Guidelines (Department of Premier and Cabinet (DPC))
- Information Management Glossary (DPC)
- Information Technology Strategy Victorian Government 2016-2020 (DPC)
- Intellectual Property Policy and Guidelines (Department of Treasury and Finance (DTF))
- Managing the risk of disclosure: The Five Safes Framework (Australian Bureau of Statistics (ABS))
- *Privacy Act 1988 (Cth)*
- *Privacy and Data Protection Act 2014*
- *Public Records Act 1973*
- Public Records Office Victoria (PROV) Policies and Standards
- *Public Administration Act 2004*
- Risk Management Framework and Practice Guide (Victorian Managed Insurance Authority (VMIA))

- *Victorian Data Sharing Act 2017*
- Victorian Protective Data Security Framework (VPDSF) (OVIC)

Guideline

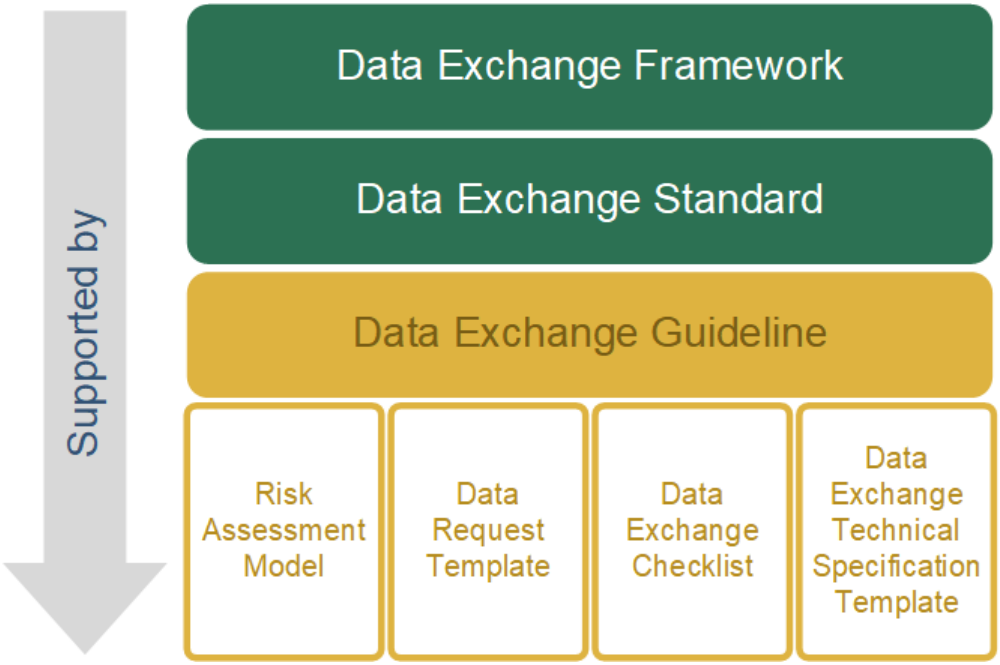
Scope of the guideline

The guideline applies to:

- structured data, which is data that can be organised and stored in fixed fields such as in a relational database record or spreadsheet
- In this guideline, ‘exchange’ is synonymous with sharing and refers to the one or two-way transfer of data in a secure, authorised and predefined way, whether:
    - automated or manual
    - real-time or near real-time
    - system to system
    - via email
    - via secure file transfer
    - bulk uploads, ongoing or once-off.

This guideline’s relationship with the standard, risk assessment model, templates and checklists as shown in Figure 1 - Data exchange documents.

Figure 1 - Data exchange documents



This guideline has been developed in alignment with the standard and framework's four steps:


Step 1 – Manage data requests, assess readiness and authority to exchange


Step 2 – Apply business rules


Step 3 – Identity mechanisms and tools


Step 4 – Exchange data.


Departments will be seen as adhering to the standard, where they have processes in place which equal or exceed the requirements outlined below. Use of the supplied tools (templates, checklist) are **optional**.


In the following guidance each step has the applicable requirements from the standard repeated and framed in a blue box.

Parties involved

The standard and guideline refer to the two main parties involved in an exchange being the requesting department (Requestor) and the department providing the data (Provider) and the following types of entities:

- internal - within the department
- external -
    - government departments and agencies
    - all other entities including government funded entities outside of government, local government, federal government, governments in other jurisdictions and any non-government entities.

Step 1 - Manage data requests, assess readiness and authority to exchange

Requesting data (Requestor)

The applicable requirements in the standard are:

1. Include in a request for data:
    a. The purpose and background context for the data request
    b. A clear description of the data required
    c. How the data will be used
    d. Whether the data will be shared or distributed and to whom
    e. Whether the request is once-off or on-going and under what conditions the data will be exchanged and managed.
2. Request data which contains ‘sensitive’ data only where authorised (allowed under law) and necessary for one or more of the Requestor’s functions or activities.

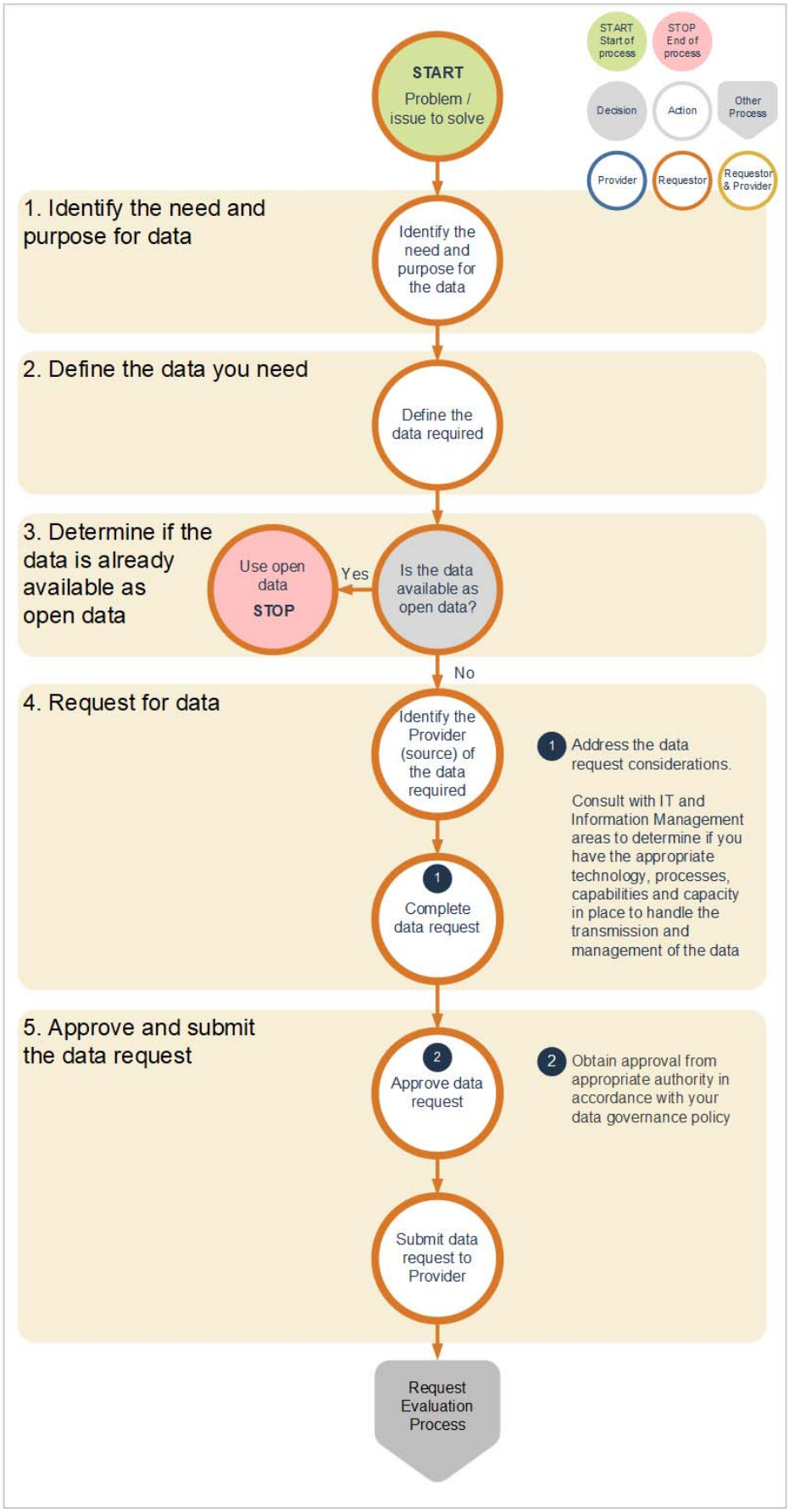
In this guideline, ‘sensitive’ data refers to data with a Business Impact Level (BIL) of Limited or higher or data with a protective marking of Cabinet-in-Confidence (as per the OVIC guidance on Business Impact Levels and Protective Markings)

The general process that a Requestor should follow to request for data is shown in Figure 2 - Data request process.

The process involves five key steps:

1. Identify the need and purpose for data
2. Define the data you need
3. Determine if the data is already available as open data
4. Request for the data
5. Approve and submit the data request.

Figure 2 - Data request process



A Data Request Template has been provided to demonstrate the key minimum requirements that should be covered when requesting for data. Additional information should be added into the request if it is relevant to strengthen the case for the request for data.

Data request considerations

When requesting for data, the Requestor should take into consideration all the elements outlined in Table 1 - Data request considerations. This will help the Requestor to not only provide a clear articulation of the data required, the purpose and use of the data, but also identify any gaps in the Requestor's ability to receive and manage the data in a manner commensurate to the risk involved.

Note that a lower level of detail may be provided in the data request form where the risk associated with the data is considered low. Data that is deemed medium to high risk will, by nature, require more information to ensure the Provider knows the exact purpose and use of the data and that the data will be secured and managed appropriately once it has been received.

Table 1 - Data request considerations

Area	Considerations
Purpose	What is the problem you are trying to solve or question you want answered?
	What is the name and objectives of the initiative you are undertaking?
	Does the initiative fall within a legislative requirement or does it respond to a government policy, initiative or directive? If so, provide details.
	What are the outputs, benefits and outcomes of the initiative you are undertaking and to whom?
	What is the severity and magnitude of impact if you do not get the data you seek, and to whom?
Data description	Identify the data you need: ▪ Data types (e.g. number of patients, by hospital, by location and average length of stay per patient) ▪ Level of granularity of the data (unit record, aggregated) ▪ Timeframe of data (e.g. data from 2010 to 2018, broken down by hourly intervals, by month and year) ▪ 'Sensitive' data.
Source of data	Is the data you need already open and publicly available? ▪ If so, use open data wherever possible ▪ If not, identify who has the data you need.
	Does the Provider have a data request form? ▪ If so, use the Provider's form ▪ If not, the Data Request Template can be used. Additional information beyond what has been provided in the template can be added if required.
Use, sharing, distribution	How will the data be used? ▪ Will the data be used to serve an operational function or be used in analysis for a particular initiative? ▪ What are the use cases for the data?
	Will the data be joined or integrated with other data?

Area	Considerations
	▪ If so, what other data will be used? ▪ What is the source of that other data? ▪ How will all the data be used collectively?
	If it is known that the data requested contains 'sensitive' data that pertains to individuals or other entities such as businesses, and if it is required to be de-identified, how will the data be de-identified? ▪ What de-identification method will be used? Guidance is provided by OVIC in the paper, De-identification and Privacy – Considerations for the public sector and by the Office of the Australian Information Commissioner (OAIC) through their guidance papers De-identification and the Privacy Act and De-identification Decision-Making Framework.
	Who will use or access the data (e.g. contractors, analysts, consumers, executive management, board members, staff, and general public)? ▪ Are they sufficiently skilled to use, handle and protect the data as required?
	Will the data or outputs from the use of the data be disclosed or published? ▪ To whom: internal and or external parties? ▪ How will confidentiality be maintained, if required?
	Are there any actual, potential or perceived conflicts of interest in having access to or using the data, for the Requestor organisation and individuals involved in the initiative?
Data exchange and management	What format is the data required to be in?
	How often do you need the data to be provided? ▪ One-off ▪ Recurring – near or real-time, daily, monthly, annually, etc.
	How do you want to receive the data? ▪ Determine the required transmission method and standards. This may require a discussion with your Information Technology (IT) specialists if the transmission of data is to occur system-system or through another automated mechanism or require specific data exchange standard (language or format). Consideration should be given to using the API Developer Portal to access the data required.
	How will the security, storage, access and disposal or deletion of the data be managed? ▪ This should align with your department's security policy, information lifecycle management policy and with the Victorian Protective Data Security Framework and Standards ▪ This may require a discussion with your IT and Information Management (IM) specialists to confirm how the data will be secured and managed. A further discussion may be needed if the Provider has specific conditions around the management of the data.
Risks	If it is known that the data requested contains 'sensitive' data, what are the risks associated with receiving, managing and using the data and what mitigations are in place? ▪ Undertake a risk assessment (particularly around Safe People, Safe Settings, Safe Data and Safe Outputs) as described in the ▪ Risk assessment section ▪ Mitigating any risks exposed from the assessment will improve the likelihood of the Provider approving the data exchange.

Area	Considerations
Request timeframe	By when is the data required? ▪ What is the reason for this deadline?
Approval	The data request should be approved in accordance with your data governance policy and or by an officer with an authority level commensurate to the risk associated with the data requested. ▪ As a guide, where the data requested is for data that is 'sensitive' in nature, the request should be authorised by an officer at a Director level or higher. Further guidance is provided in the Information Management Framework and Information Management Governance Standard.
	Additional approvals external to your department may be required (e.g. oversight committees, ethics committees).

Evaluating a data request (the right and readiness to exchange) (Provider)

The applicable requirements in the standard are:

3. Evaluate all data requests to assess whether the department has the right (or authority) to exchange the data requested including:
   - Legislative authority or obligation to share under legislation (Acts) relevant to the department or portfolio
   - Legislative authority to share under the *Privacy Act 1988 (Cth)*, *Victorian Data Sharing Act 2017*, *Public Records Act 1973* and *Freedom of Information Act 1982*
   - Other regulation and policies specifically relevant to the department or portfolio
   - If the Provider is not the owner of the data, whether there is:
     – a commercial agreement
     – personal individual consent or
     – data asset owner's consent (if the data is owned by another department or agency)

     that permits the exchange of data (noting that permission to exchange may only be for certain limited purposes).
4. Evaluate all data requests to assess whether the department is ready to exchange the data requested including:
   - Carrying out a risk assessment to determine risk to the department, Victorian Government (government) and the Victorian Public (see the Victorian Government's Risk Management Framework)
   - Ensuring that where 'sensitive' data are involved, that a privacy impact assessment is conducted to ensure reasonable steps have been taken to protect the data from misuse or loss and unauthorised access, modification or disclosure (see the Office of the Victorian Information Commissioner's (OVIC) guidance on privacy impact assessments)

- Ensuing data is de-identified wherever possible, unless identified data is essential to enable the data to be fit-for-purpose (see OVIC's guidance on de-identification Protecting unit-record level personal information)
- Assessing whether the Provider and the Requestor have the appropriate processes, technology and infrastructure in place, and sufficient capabilities and capacity to undertake the exchange
- Whether the data is of sufficient quality to be fit-for-purpose, and if not, to provide appropriate disclaimers as to its use.

5. Disclose 'sensitive' information only to the extent required to meet the objectives of the request, and only in accordance with the provisions of the authorities listed in requirement 3.

The general process that a Provider should follow to evaluate a data request is shown in Figure 3 - Data request evaluation process. The process involves three key steps:

Assessing the right to exchange:

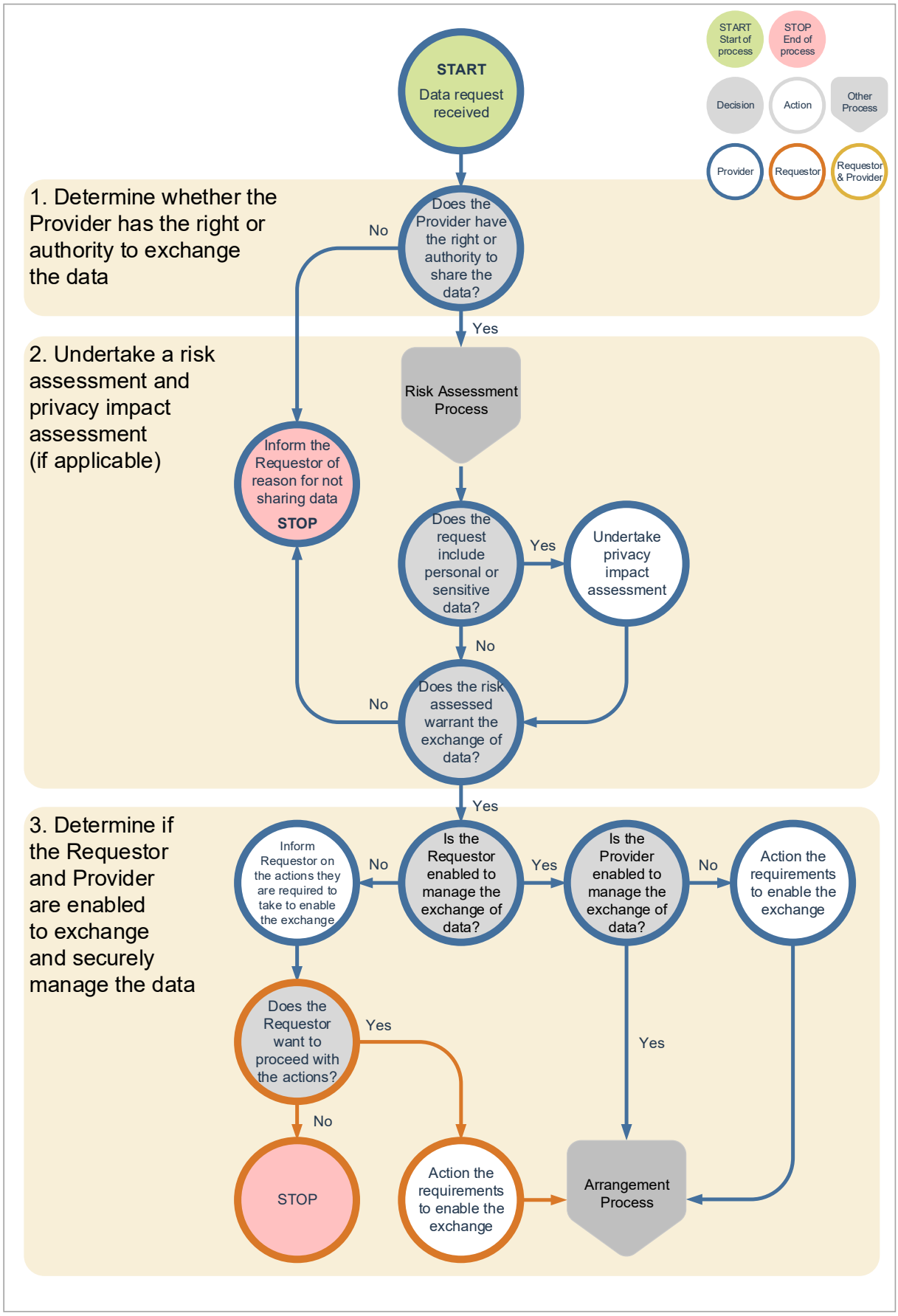
1. Determine whether the Provider has the right or authority to exchange the data

Assessing the readiness to exchange:

2. Undertake a risk assessment and privacy impact assessment (if applicable)
3. Determine if the Requestor and Provider are enabled (have the data, appropriate technology, infrastructure, policies and processes) to undertake the exchange and securely manage the data (readiness to exchange).

A Data Exchange Request Evaluation Checklist has been provided to highlight the key considerations that should be covered when evaluating a data request.

Figure 3 - Data request evaluation process



Data request evaluation considerations

When evaluating a request for data, the following considerations (Table 2 - Data request evaluation considerations) that should be taken into account.

Table 2 - Data request evaluation considerations

Area	Considerations
Right or authority to share	Is the request for 'sensitive' data?
	Does the Provider have the right or authority to share the data under: ▪ Legislative authority or obligation to share under legislation (Acts) relevant to the department or portfolio ▪ Legislative authority of the *Privacy and Data Protection Act 2014*, *Victorian Data Sharing Act 2017*, *Public Records Act 1973* and *Freedom of Information Act 1982* ▪ Other regulation and policies specifically relevant to the department or portfolio ▪ If the Provider is not the owner of the data, whether there is: – a commercial agreement, – personal individual consent[2] or – other department data asset owner's consent (if the data is owned by another department or agency) that permits the exchange of data (noting that permission to exchange may only be for certain limited purposes).
	If the request is for 'sensitive' data and the Provider does not have the right or authority to share it, the Provider could negotiate with the Requestor to provide de-identified data.
	If the Provider does not have the authority or right to share the data, the Provider should issue a response to the Requestor in writing stating the reason for not providing the data and referencing any relevant legislation or policies that prohibited the exchange.
Risk assessment	The key steps in assessing risk are: ▪ Determine the Provider's risk appetite for data sharing ▪ Undertake a risk assessment for the data request ▪ If the data request is for personal data, a Privacy Impact Assessment should also be undertaken ▪ Decide whether the risk justifies the benefit for sharing the data. Refer to the Risk Assessment section for a more detailed discussion on carrying out a risk assessment.
	If the data request is for 'sensitive' data, a Privacy Impact Assessment should also be undertaken, which evaluates compliance against the Information Privacy Principles (IPP) in the *Privacy and Data Protection Act 2014*. Refer to OVIC for guidance and templates on Privacy Impact Assessments.
	If the Provider deems that the risk and mitigations do not outweigh the benefits of sharing the data, the Provider should issue a response to the Requestor in writing stating the reason for not providing the data, referencing any policies that prohibit the exchange.
Enabled exchange	Does the Requestor have the appropriate technology, infrastructure, policies and processes to undertake the exchange and securely manage the data?

[2] For further information on consent refer to OVIC's Guidelines for sharing personal information.

Area	Considerations
	This can be determined via the risk assessment of Safe People, Safe Settings, Safe Data and Safe Outputs
	If gaps are identified, the Provider should inform the Requestor of the gaps and the required mitigations. The Requestor may choose not to proceed with the mitigations and forego the request, at which point the process ends.
	Is the Provider enabled to exchange the data? **Access to data** ▪ Is the data easy to access and extract from the system it resides in? ▪ Is the impact on the system when extracting the data significant enough to cause performance issues? If so, how will this be mitigated? **De-identification** ▪ Will de-identification of the data be required? If so, what method will be used? ▪ Guidance is provided by OVIC in the paper, De-identification and Privacy – Considerations for the public sector and by the Office of the Australian Information Commissioner (OAIC) through their guidance papers De-identification and the Privacy Act and De-identification Decision-Making Framework.How will de-identification, and maintaining the privacy of the individual, be managed and maintained if the data provision is recurring? **Process** ▪ Is there an existing data exchange process? If not, a process will need to be created ▪ Are all participants in the process aware of their roles and responsibilities and the rules of the exchange? ▪ How will errors, faults, recovery and complaints be handled and monitored? **Data Quality** It is common for organisations not to exchange data because of concerns over the quality of the data. Less than perfect data quality, alone, should not be a barrier to exchange data, however it is up to the Provider to determine whether the data quality renders the data fit-for-purpose. ▪ Is the Provider enabled to supply a data quality statement? The Provider should issue an updated statement if changes in the data impact the data quality. Refer to the WOVG Data Quality Standard, Guideline and Statement Template for further information. **Metadata** ▪ Is the Provider enabled to supply metadata? If so, what metadata standard will be used? As an option, refer to the Victorian Government Data Directory Metadata Schema. Updated metadata should be provided if changes occur. **Capacity** ▪ Does the Provider have the capacity to undertake the exchange within the timeframe and ongoing if the data provision is recurring? ▪ A lack of or limited capacity, of itself, should not be considered as a reason not to undertake the exchange, but rather a factor that may impact the scope and or timing of the exchange.

Risk assessment model

A risk-based approach to the data request evaluation is recommended, which aims to balance the risk of disclosure with the proposed benefits and outcomes of the initiative being undertaken by the Requestor.

The evaluation process involves undertaking a risk assessment using a risk assessment model (risk model) that incorporates the Five Safes Framework[3], reputational risk and public risk (Figure 4 - Risk assessment model. This risk model should align with the Provider's overall organisational risk management framework and the WOVG Risk Management Framework. A description of the risk components and assessment process is provided in Table 3 – Risk components and Figure 5 - Risk assessment process.

Figure 4 - Risk assessment model

[3] The Five Safes Framework provides guiding principles around managing the risk of disclosure and has been adopted by organisations like the Australian Bureau of Statistics (ABS), United Kingdom's Data Archive, Eurostat and Statistics New Zealand; and incorporated into legislation like the *Public Sector (Data Sharing) Act 2016* (SA) and the proposed new Commonwealth Data Sharing and Release legislation. For more information, refer to the Five Safes Framework on the ABS website.

Table 3 – Risk components

Component	Description
SAFE PROJECTS	**Is this use of the data appropriate?** ▪ Refers to the legal, moral and ethical considerations surrounding the use of the data.[4] ▪ Are the objectives, outputs, benefits and outcomes of the initiative reasonable and in alignment with the purpose and functions of the Requestor organisation? ▪ What are the risks of loss, harm or detrimental impact to the department, individuals, wider government, general public of sharing (or not sharing) the data? Are there any mitigations? This should be described in the section in the data request around the purpose for the request, the objectives, outputs, anticipated outcomes and benefits of the initiative.
SAFE PEOPLE	**Is the user authorised to access and use the data?** ▪ Refers to the knowledge, skills and incentives of the users using the data.[4] ▪ Is the Requestor organisation reputable and trustworthy? ▪ Do the staff possess the knowledge (e.g. skills and experience) to effectively use the requested data for the proposed purpose? How will the Provider or Requestor ensure that their staff have appropriate and sufficient knowledge? ▪ What are the roles and responsibilities for all the staff (or user groups) who will have access to the data and what level of access will they have? This should be described in the section in the data request around who will have access to the data and how they will use the data.
SAFE SETTINGS	**Does the access environment prevent unauthorised use?** ▪ Refers to the controls on the way the data is accessed, including physical, procedural and compliance controls.[4] ▪ Does the Requestor possess the technical requirements (e.g. equipment, software), governance, policies and processes to effectively manage and enable the use of the requested data for the proposed purpose? ▪ Where will the data be stored and used? ▪ What security and technical safeguards are in place to ensure data remains secure and protected from unauthorised access and use (e.g. governance, physical safeguards, personnel and cyber security arrangements)? Safeguards must align with the classification of the data being shared ▪ How will the data be dealt with after it has been used for this purpose? This should be described in the section in the data request on how data will be managed.
SAFE DATA	**Has appropriate and sufficient protection been applied to the data?** ▪ Refers to whether the data itself contains sufficient information for confidentiality to be breached[5]? ▪ Is 'sensitive' data requested? Is the data required to remain identified? ▪ If not, the Provider should ensure that the data is de-identified. Guidance on de-identification is provided by OVIC in their paper, De-identification and Privacy – Considerations for the public sector as well as the DataVic Access Policy Guidelines ▪ If identified data is required, the Requestor should outline how they will de-identify the data and ensure that confidentiality is maintained

[4] As described in Data Sharing Framework, Sep 2017, Australian Computer Society (ACS)

[5] As described by the ABS in Managing the risk of disclosure: The Five Safes Framework

Component	Description
	▪ If the data is going to be joined or integrated with other datasets, how will this happen and how will the resulting data be used? Does this increase the risk of disclosure? ▪ Are there any potential data quality, matching, reconfiguration, interpretation or other issues regarding the data being requested? This should be described in the section in the data request on how the data will be managed.
SAFE OUTPUTS	**Are the analytical results non-disclosive i.e. individuals or groups cannot be re-identified from the outputs from the initiative?** ▪ This is the final check on the information before it is released which aims to reduce the risk of disclosure to a minimum ▪ Will the results of the data or analytics work on the shared data be published or disclosed? If so, what is the nature of the proposed publication or disclosure? ▪ Who will be the audience for the publication or disclosure? ▪ What is the likelihood and the extent to which the publication or disclosure may contribute to the unauthorised identification of a person in the data? This should be described in the section in the data request on how the data will used and managed.
REPUTATIONAL RISK	**Refers to whether there are any:** ▪ **threats or danger to the good name or standing of the department and or** ▪ **risk that the outputs or results of the initiative could contradict or refute any government-wide policy or directive**. This can be ascertained by reviewing the purpose of the request, how the data will be used and who the audience for the outputs of the initiative.
PUBLIC RISK	**Refers to whether there are any risks to the safety, security and or well-being of the general public.** This can be ascertained by reviewing the purpose of the request, how the data will be used and who the audience for the outputs of the initiative.

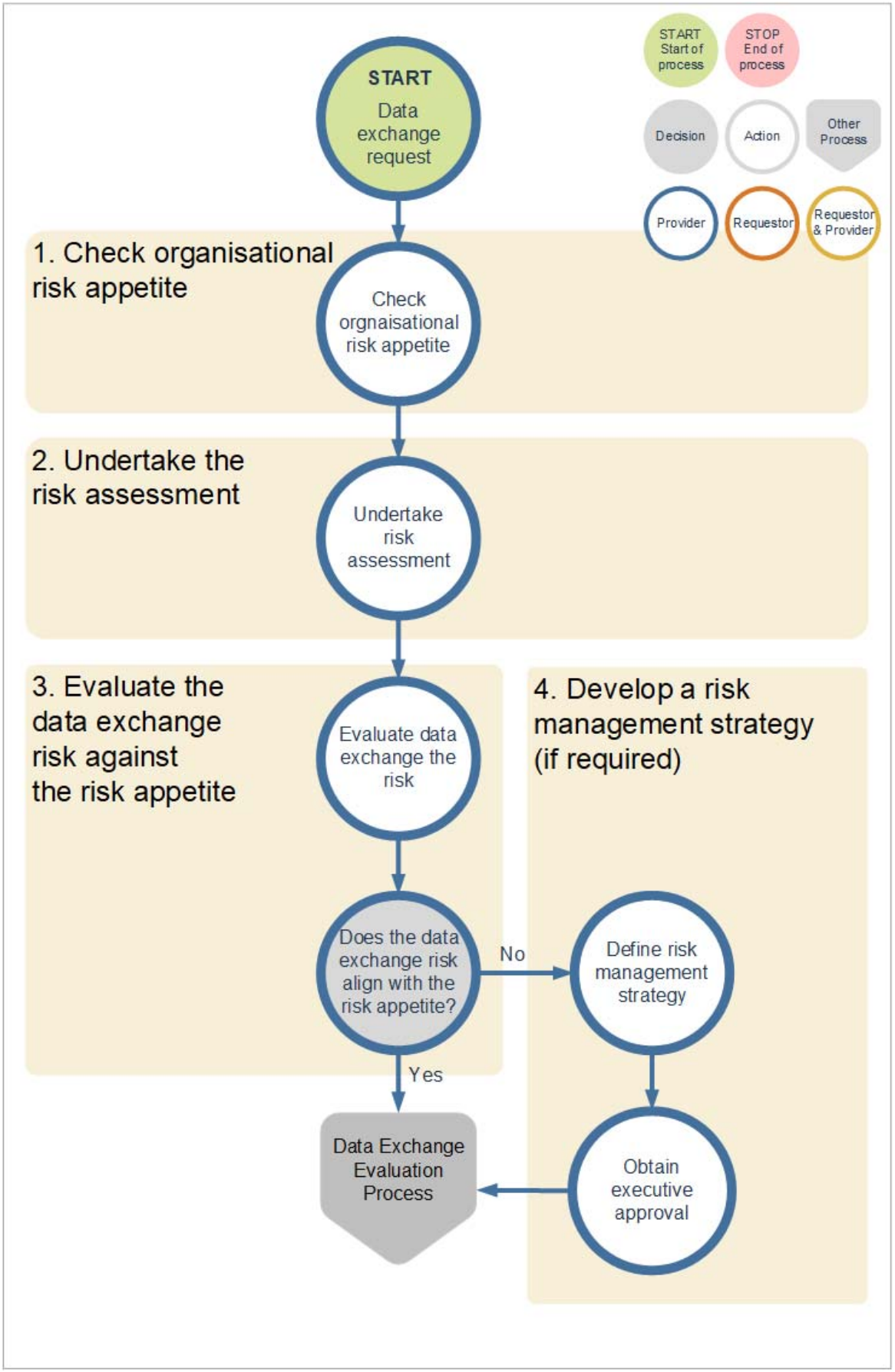
For further guidance on the Five Safes Framework and how it can be applied, refer to the Australian Bureau of Statistics' Managing the Risk of Disclosure: The Five Safes Framework or the Australian Computer Society's paper Data Sharing Framework.

Risk assessment for the data exchange should be assessed within the context of the overall risk appetite of the organisation. This should be part of the organisation's risk management framework. Refer to the VMIA's Risk Management Framework and Practice Guide for further guidance on risk management, risk terminology and risk appetite.

The general process that a Requestor should follow in assessing the risk of a data exchange is shown in Figure 5 - Risk assessment process. The process involves four key steps:

1. Check organisational risk appetite
2. Undertake the risk assessment
3. Evaluate the data exchange risk against the risk appetite
4. Develop a risk management strategy (if required).

Figure 5 - Risk assessment process



When assessing the risks of a data exchange, the following considerations (Table 4 – Risk assessment considerations) should be taken into account.

Table 4 – Risk assessment considerations

<table>
<tr><th>Area</th><th>Considerations</th></tr>
<tr><td>Organisational risk appetite</td><td>What is the organisational risk appetite for data exchange?
Prior to undertaking the risk assessment, a check needs to be made against the organisational risk appetite. The risk appetite is the level of risk (high, moderate or low) the organisation is willing to accept around all data exchanges and is the benchmark to compare the risk of the particular data exchange. Should a risk appetite not exist, assume a ‘moderate’ level.</td></tr>
<tr><td>Risk assessment</td><td>What are the data exchange risks?
Risk assessment entails reviewing each of the risk components (the Five Safes, reputational and public risk) in Table 3, and assessing the consequences and likelihood of each risk component (using
Table 5 – Consequence and Error! Reference source not found.)
The overall risk of the data exchange should be based on the risk component with the highest risk rating.</td></tr>
<tr><td>Risk evaluation</td><td>How does the overall data exchange risk compare to the organisational risk appetite?
Risk evaluation involves comparing the data exchange risk rating against the organisational risk appetite. The risk appetite can be determined by reviewing your organisation’s risk management framework for data exchange focused risks. If a risk appetite for data exchange cannot be determined, you can assume a ‘moderate’ risk appetite.
The process of evaluating risk is:
Compare the overall data exchange risk against the organisation’s risk appetite. The mapping below shows the relationship between the organisational risk appetite and corresponding maximum level of data exchange risk:
<table>
<tr><th>Organisational risk appetite</th><th>Data Exchange risk rating</th></tr>
<tr><td>Low</td><td>Significant or High</td></tr>
<tr><td>Moderate</td><td>Moderate</td></tr>
<tr><td>High</td><td>Low</td></tr>
</table>
If the data exchange risk is Significant or High and your risk appetite is Moderate or Low, then a risk management strategy needs to be completed and approved by the appropriate level of authority as defined in your organisational risk management framework</td></tr>
<tr><td>Risk management strategy</td><td>Where a risk management strategy is required, it must contain risk mitigation treatments to either avoid or reduce the risk to an acceptable level.
The risk management strategy should contain:
The risk and the risk level
The risk control and treatments to reduce the risk, including timelines
The people responsible for executing the actions
The owner of the risk and the risk management strategy</td></tr>
</table>

Area	Considerations
	▪ Monitoring requirements for the risk ▪ Applicable reviews of the risk and risk management strategy. Guidance on developing a risk strategy and a template can be found in the VMIA's Risk Management Framework Practice Guide.
Executive approval	The final risk management strategy must be approved by an executive within the Provider organisation.

Risk assessment is composed of two parts:

- **Assessing the risk consequence** – identifying the consequence (impact) of the data exchange against seven risk components
- **Assessing the risk likelihood** – assessing each risk component and consequence for the likelihood (probability) of the risk occurring.

Using the review of the risk components done under Table 3:

- Assess the potential consequences and likelihood of each component using the risk consequence table (Figure 5) and the risk rating matrix (Figure 6) to determine the risk rating
- Identify the component(s) with the highest risk rating. This will be used to represent the overall risk rating for the data exchange in the risk evaluation stage of the risk assessment (refer to the risk evaluation section in Table 4).

Figure 6 - Consequence versus likelihood

Risk Rating

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood ▼	Rating	1	2	3	4	5
Almost Certain	5	Medium	Medium	Significant	High	High
Likely	4	Low	Medium	Significant	Significant	High
Neutral	3	Low	Medium	Medium	Significant	Significant
Unlikely	2	Low	Low	Medium	Medium	Medium
Rare	1	Low	Low	Low	Low	Medium

Table 5 – Consequence

Consequence rating				
Insignificant – 1	**Minor – 2**	**Moderate – 3**	**Major – 4**	**Catastrophic – 5**
Safe Projects				
No identified ethical aspects or not using data involving people	Having minor ethical risks which can be mitigated, or using highly aggregated or obfuscated data which has no residual personal information	Having ethical risks which require monitoring, or using lightly aggregated or obfuscated data with a possible risk of re-identification of individual information	Having identifiable ethical risks which require significant attention, or using lightly aggregated or obfuscated data with a plausible risk of re-identification of individual information	Clear ethical risks, or using personal information without appropriate de-identification or security controls
Safe People				
Authorised people interacting with the data have the knowledge and skills for required management and use of the data	Authorised people interacting with the data have reasonable knowledge and skills for required management and use of the data	Authorised people interacting with the data have minimal knowledge and skills for required management and use of the data	Authorised people interacting with the data have little to no knowledge and skills for required management and use of the data	Unauthorised management or use of the data
Safe Data				
No sensitive data requiring treatment	Unauthorised disclosure of sensitive data to an internal party	Unauthorised disclosure of sensitive data to a single external party (not including the general public)	Unauthorised disclosure of sensitive data to multiple external parties (not including the general public)	Unauthorised disclosure of sensitive data to the general public
Safe Settings				
System accessed with multi-factor user authentication, active action logging, full audit trail of data lifecycle, anomaly detection, prevention of on-sharing	System accessed with multi-factor user authentication, user action logging, prevention of on-sharing	System accessed with multi-factor user authentication, no ability to readily on-share	System accessed with named user login authentication, limited ability to on-share	System accessed with no restriction on who can access data with ability to on-share
Safe Outputs				
Projects based on open data or projects considered to be Highly Safe.	Projects based on low value data or projects which are considered to be Safe	Projects based on moderate value data or projects which are considered to have a Moderate Level of Safety	Projects based on high value data or projects which are considered to have a Low Level of Safety	Projects based on very high value data or projects which are considered Not Safe

Consequence rating				
Insignificant – 1	**Minor – 2**	**Moderate – 3**	**Major – 4**	**Catastrophic – 5**
Reputational risk				
Minor, adverse local public or media attention or complaints	Media attention of local concern	Significant adverse attention by media and or public	Serious public or media outcry (State coverage)	Serious public or media outcry (National coverage)
Public risk				
No public risk to wellbeing or safety or members of the public identified	Minor public risk to wellbeing or safety. Potential for a person to be identified	Significant public risk to wellbeing or safety. Potential for a person to be identified	Major public risk to wellbeing or safety or members of the public identified	Serious public risk to wellbeing or safety or members of the public identified

Step 2 - Applying the business rules

Data exchange arrangement (Requestor and Provider)

The applicable requirements in the standard are:

6. Ensure that all data exchanges are accompanied by a data exchange arrangement - legally binding, non-legally binding or Creative Commons licence. The type of arrangement used should be based on who the department is exchanging data with, the level of data protection required and the level of risk associated with the data and the data exchange (see Table 6).
7. Ensure all legally binding and non-legally binding data exchange arrangements include the minimum requirements outlined in Table 2 in the Supporting Information section of the standard.
8. Exchange data to the maximum extent possible under a Creative Commons licence and release via data.vic.gov.au as open data unless restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law[6].
12. Ensure all data exchanges are authorised by an officer of the organisation at a level commensurate to the risk associated with the data and in accordance with the government's Information Management Framework and Information Management Governance Standards.

When exchanging data, it is important that the parties involved enter into an arrangement which outlines the definition of the data exchanged and the roles and responsibilities by each party on how the data will be provided, used, secured and managed. A data exchange arrangement will protect the rights and interests not only of the Provider and Requestor but also the wider government, community and individuals.

It is not sufficient for the Provider to 'just trust' the Requestor.

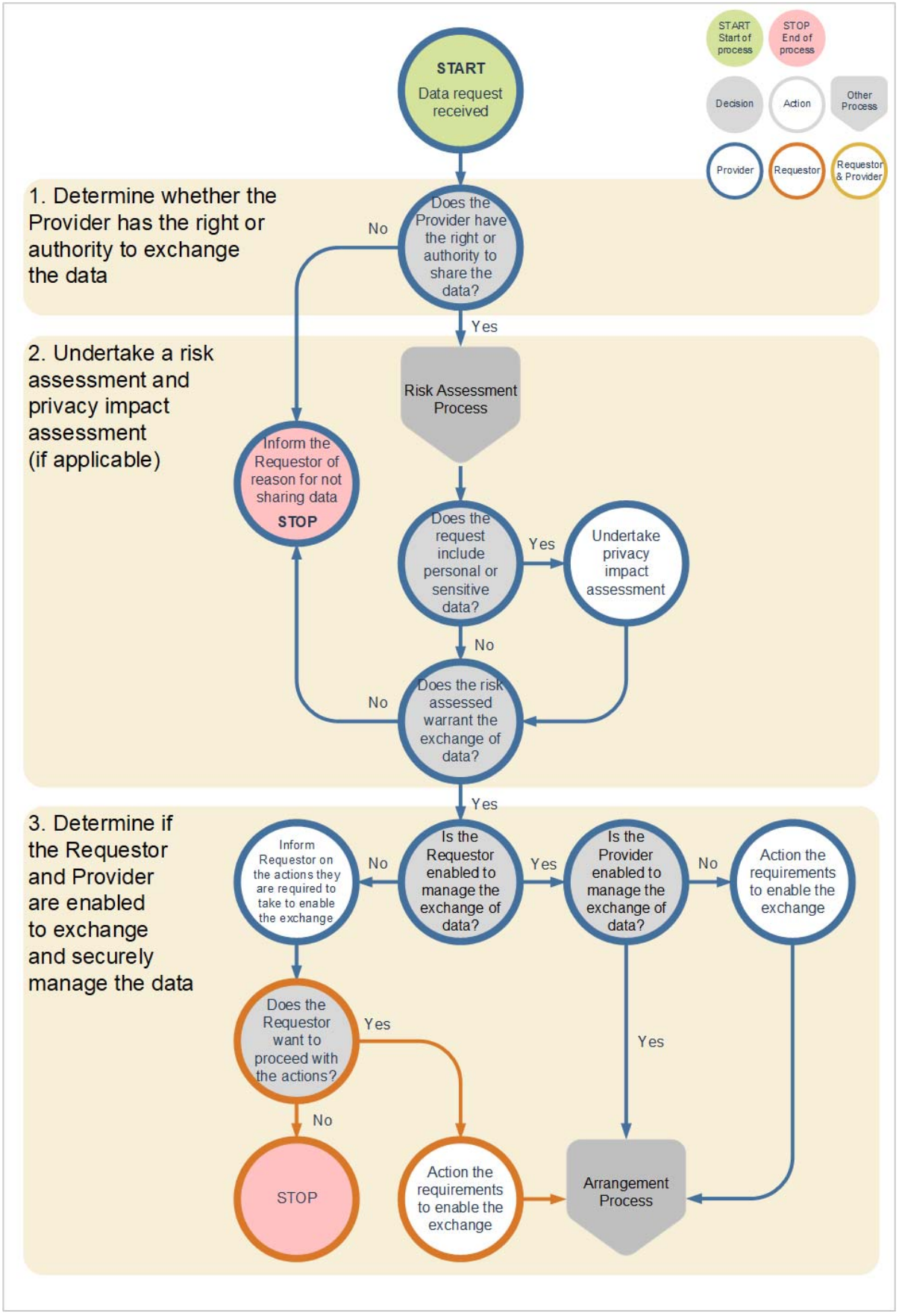
The general process that a Provider and Requestor should follow to negotiate and agree on a data exchange arrangement is shown in Figure 7 - Entering into a data exchange arrangement.

The process involves three key steps:

1. Select an appropriate arrangement tool
2. Negotiate the terms and conditions of the arrangement
3. Obtain approval and sign off for the arrangement.

[6] As per Principle 4 of the Information Management Policy and Principle 1 of the Datavic Access Policy Guidelines For The Victorian Public Sector. Refer to this guideline for information on what data should and should not be made available.

Figure 7 - Entering into a data exchange arrangement



Arrangements come in many variations and range by type (legally or non-legally binding) and by format (informal or formal). The selection of arrangement should follow the rules set out in Table 6 – Criteria determining the use of arrangement types.

Table 6 – Criteria determining the use of arrangement types

Requestor →	**Internal**	**External**				
		Victorian Government			**Non-Victorian Government**	
	Refers to requestors that are internal to the provider department (3)	**Refers to Victorian Government departments and agencies. Note, while statutory bodies are part of the government, they are legal entities in their own right. A legally binding agreement should be entered into with a statutory body when warranted by the associated level of risk**			**Refers to all other entities including government funded entities outside of government, local government, federal government, governments in other jurisdictions and any non-government entities**	
Data risk	All levels (1)	Not sensitive (1)		Sensitive	Not sensitive (1)	Sensitive
Arrangement type	Non-legally binding	Non-legally binding	Legally binding	Non-legally binding	Legally binding	
Format	Informal	Informal	Formal	Formal	Formal	Formal
Example arrangement	Email	Email	Licence such as creative commons (2)	Memorandum or letter of understanding (or other formal non-legally binding mechanism)	Licence such as creative commons (2)	Legal Agreement

(1) If data is not 'sensitive', the Provider should consider releasing it as open data, as per Principle 4 of the Information Management Policy and Principle 1 of the DataVic Access Policy Guidelines for The Victorian Public Sector. Refer to the DataVic Access Policy Guideline for information on what data should and should not be made available.

(2) Refer to Creative Commons Australia (who provide copyright licences to facilitate sharing and reuse of creative content) and DTF's Intellectual Property Guidelines for the Victorian Public Sector for further guidance.

(3) For example, a requestor internal to the organisation Department of Health and Human Services (DHHS) is a person within a branch, division or business unit of DHHS. Other 'bodies' (agencies, statutory bodies, etc.) related to DHHS, such as Family Safety Victoria (FSV) and the Victorian Agency for Health Information (VAHI) are considered external to the organisation of DHHS.

When entering into a data exchange arrangement, the Provider and Requestor should take into consideration all the elements outlined in Table 7 – Data arrangement considerations below, as well as Table 2 in the Supporting Information section of the standard.

Data arrangements do not always have to exist in a standalone state. They can sometimes form part of a broader agreement. Contracts often contain obligations around providing data and reporting. In these instances, it is important that these considerations be taken into account.

Where more than one dataset is to be exchanged, the structure of the arrangement should have a master arrangement detailing the general terms and conditions and separate schedules for each dataset exchanged. Each schedule should include the dataset name, description, data owner (or custodian), data fields, data definitions, data quality statement, data security classification and any other terms and conditions specific to the dataset.

Table 7 – Data arrangement considerations

Area	Considerations
Arrangement selection	In following the principles underpinning the WOVG Information Management Policy and DataVic Access Policy[6], data should be made available under a Creative Commons licence to the maximum extent possible, unless restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law.
	The main considerations in selecting the appropriate type of arrangement are: ▪ Whether the Requestor is internal or external to the department ▪ The risk associated with the data, as determined via the risk assessment. The higher the risk the more formal the data exchange arrangement should be.
	The various types and formats of arrangements and rules on how to select the appropriate one have been discussed above in Table 6.
Negotiate the arrangement	Table 2 in the standard (Supporting Information section) outlines the minimum requirements for a legally or non-legally binding arrangement (excluding Creative Commons license), depending on whether the request is internal or external to the department. Most of the requirements are self-explanatory, however further notes have been provided below on certain requirements.
	Obligations of parties The arrangement should outline the responsibilities of each party as well as any governance or oversight body (e.g. steering committee) created as part of the arrangement.
	Data description The data description should include: ▪ Types of data - dimensions (e.g. dates, locations, age groups, other subject-specific categories) and measures (e.g. count of people, amount of expenditure, average age, expenditure) ▪ Timeframe of the data (e.g. data from 2010 – 2018, broken down by month) ▪ Data-related standards used (e.g. metadata standard, GIS standard) ▪ Data security classification applied (refer to VPDSF guidance around Business Level Impact and Protective Markings) ▪ If data has been de-identified, what method was used? ▪ Refer to the Data Exchange Technical Considerations section and Data Exchange Technical Specification Template.
	Terms of use and disclosure ▪ For what purpose(s) can the data be used? ▪ Is Requestor permitted to join or integrate the data with other datasets? If so, which datasets and their sources? ▪ Is the Requestor required to de-identify the data? ▪ Is the Requestor permitted to reproduce, distribute or published the data or outputs of the initiative internally or externally? If so, to whom and under what conditions? ▪ Does the Provider want the right to review the outputs before it is published? ▪ Is the Requestor permitted to commercialise the data?
	Intellectual Property (IP) and licencing Who will own any new IP developed? It is quite common for Requestors to join or integrate the data provided with data from other sources and create new datasets. The arrangement should address the ownership of the new datasets.

Area	Considerations
	▪ Does the Requestor require consent from the Provider on how, when and who can use this new data set? ▪ Does the Provider want the right to review the output before it is published by the Requestor?
	Data exchange and management This section should cover: ▪ How the data will be transmitted by the Provider to the Requestor ▪ How the data will be managed by the Requestor. <u>Data transmission (Provider)</u> ▪ Format of the exchange - the format in which the data will be provided (e.g. csv, xlsx, db, API) ▪ Frequency of transmission – one-off, recurring (how frequently?) ▪ What method of transmission will be used (e.g. system-to-system, bulk upload, web portal transfer, via email, via encrypted flash drive) ▪ Whether encryption of the data is required ▪ Refer to the Data exchange technical considerations section and Data Exchange Technical Specification Template. <u>Data management (Requestor)</u> ▪ Where the data will be stored ▪ Who will have access to the data? ▪ If required, how will data de-identification and confidentiality be maintained ▪ How the data security will be maintained over access and use of the data ▪ Whether the data will need to be disposed of or returned to the Provider after the term of use ▪ Refer to the Data Exchange Technical Considerations section and Data Exchange Technical Specification Template.
	Service levels This section outlines the Provider's responsibilities in providing the data: ▪ When the data will be provided (e.g. within 3 days after month end) ▪ If the data transmitted via an automated mechanism (e.g. system-to-system, bulk upload, API), the level of reliability and availability of the mechanism Refer to the Data Exchange Technical Considerations section and Data Exchange Technical Specification Template ▪ Maintenance of data quality to the level specified in the data quality statement ▪ Provision and maintenance of metadata ▪ What are the consequences if there is a failure of service ▪ Complaint handling ▪ Resolution timeframes.
	Change management The Provider's responsibility to notify the Requestor if: ▪ changes occur that impact data quality or format. The elements of data quality are described in the WOVG Data Quality Guideline ▪ changes occur to the metadata. When and how will the notification occur? When will the updated data quality statement or metadata be provided?
Obtain sign off	The arrangement should be approved or signed off by an officer from each party with the appropriate level of authority in accordance with their respective information governance, delegation of authority or security policy.

Area	Considerations
	If there are no such policies, then this should be done in accordance with the WOVG Information Management Framework and Information Management Governance Standard.

Data exchange technical considerations

When exchanging data, the Provider and Requestor will need to take into account technical considerations around the data, its transmission and management, as described in Table 8 – Technical considerations.

A Data Exchange Technical Specification Template has been provided as an example of what technical details should be supplied to the Requestor when the data is exchanged, in addition to the data quality statement and the metadata document.

It is recommended that this document be completed by both the Provider and Requestor (in the relevant sections indicated in the template) in consultation with each organisation's Information Technology and Information Management subject matter experts.

Table 8 – Technical considerations

Area	Considerations
Data (Provider, unless stated otherwise)	Document the data schema and model (structure of the data, variables, data types, interdependencies, mappings and process flows)
	Definitions of the data (data dictionary) to aid interpretation and understanding of the data. e.g. Region is a geographical area in Victoria where services are provided (definition). Regions comprise four areas: North (define boundary), South (define boundary), East (define boundary) and West (define boundary).
	Metadata standard used in providing the metadata document. For guidance on metadata standards, refer to Australian Government Locator Service (AGLS) Metadata Standard. Refer to your IT specialists for further guidance on the appropriate metadata standard that should be used for the particular data being exchanged.
	What is the data security classification of the data? Data must be classified to ensure appropriate security is applied during the exchange. Data should be classified accordance with the department's security policy or OVIC's guidance around Business Level Impact and Protective Markings.
Transmission (Provider, unless stated otherwise)	Will the data be exchanged once, or will there be on ongoing process? Where there is an ongoing process, how frequently will the exchange occur? The frequency of the exchange should be an input into the technical design of the exchange. ▪ For more frequent exchanges, there is likely to be value in developing an automated process for the exchange ▪ Non-recurring exchange or less frequent exchanges, the development overhead required for automation may not provide value.

Area	Considerations
	What is the size or volume of the dataset to be exchanged? If the exchange is recurring, how will the size or volume of data change over time? Will the dataset be exchanged as a batch or incrementally as it is generated? The size of the dataset and batch vs. incremental transmission should be an input into the technical design of the exchange. For example, a large dataset that is to be transferred as a batch may not be suited to an API or messaging style of transfer. Consideration should be given to reliable file transmission methods such as SFTP.
	The transmission method used should be appropriate for: ▪ The frequency of the exchange ▪ The size or volume of the data that will be exchanged during each exchange instance ▪ Whether the exchange will be batch or incremental ▪ The security classification and level of risk of the data. The higher the risk, the more secure the method required. Example transmission methods include: ▪ Secure file transfer using protocols such as Secure File Transfer Protocol (SFTP), File Transfer Protocol Secure (FTPS) or Hypertext Transfer Protocol Secure (HTTPS) ▪ Application programming interface (API) such as the government's API Gateway (see Understand the API design principles – Digital Standards) ▪ System-to-system ▪ System to location ▪ Messaging ▪ Bulk uploads ▪ Email ▪ External storage media such as flash drives, CD or DVD. While there is no definitive guide for when a particular transmission method should be used, the following rules should typically apply: ▪ Frequent exchanges with smaller data volumes may be more suited to automated, machine methods such as APIs ▪ Large data volumes may be more suited to file transfer mechanisms such as SFTP ▪ Sensitive data should never be transmitted via email or external storage devices.
	The format or language that will be used to transfer the data, such as: ▪ CSV, comma separated file ▪ TXT, plain text file ▪ XML, type of open data format ▪ JSON, JavaScript Object Notation ▪ Standard Interchange Format ▪ Data Interchange Format ▪ Open Document Format.
	Will encryption be required? If so, what encryption method will be used? Any encryption applied must be done so using an appropriate method. The Australian Government Information Security Manual provides guidance on appropriate encryption methods based on the security classification of the data.

Area	Considerations
	Both the Provider and Requestor need to ensure that the data: ▪ Can be provided via the agreed transmission method ▪ Can be received via the agreed transmission method ▪ Can be read in order to extract the data for use.
Management (Provider and Requestor)	(Provider) Will there be a performance impact to the source system due to the extraction and or transmission of the data? (Requestor) Will there be a performance impact to the target system due to the receipt and or transmission of the data? Has adequate testing be carried out to understand the impact? If there is a potential impact, how will this impact be mitigated? (e.g. transfer outside of business hours)
	(Requestor) How and where will data be stored once it is received? ▪ Is there sufficient storage capacity to store the data files, especially when the data exchange is ongoing and involves large data files? ▪ Will the data be encrypted where it is stored? ▪ How will the data be disposed of if the Requestor will only retain it for a limited time?
	(Requestor) How will data be secured once it is received? ▪ Are there adequate security controls in place to ensure it is protected from unauthorised access, modification and loss? ▪ How will access to the data be restricted? ▪ What level of access (read or write) will the permitted users (or groups) be given?
	What is the technical process where there is an interruption or fault within the data exchange? The process should consider: ▪ Monitoring for errors and faults ▪ Ability to restart the process while ensuring no data is lost and no duplicates are produced.

Step 3 – Identifying mechanisms and tools

Throughout this guideline, references have been made to various mechanisms and tools that will help support a streamlined, safe and authorised data exchange. These are listed in Table 9 – Data exchange mechanisms and tools.

Table 9 – Data exchange mechanisms and tools

Area	Mechanism or tool
Data request	**Data Request Template** An example of the minimum considerations that should be addressed in a data request. Providers and Requestors can use this template as it is or as a basis for developing your own template.
Data request evaluation	**Data Exchange Request Evaluation Checklist** An example of the key considerations that should be addressed when evaluating a data request.
	Risk Assessment Model (in this document) Helps to assess the risk and apply appropriate controls to data exchange. This model will help data owners to assess if the data exchange is in the best interest of the either the Provider or Requestor departments, the wider government or of the Victorian people.
Data exchange	**Data Exchange Technical Specification Template** An example of the key technical details that should supplied to the Requestor when the data is exchanged. Providers can use this template as it is or as a basis for developing your own template.
	Data Quality Statement Template An example of the key information about data quality that should be supplied to the Requestor when exchanging data. (Refer to Policies and standards for government IT)

Step 4 – Exchanging the data

The applicable requirements in the standard are:

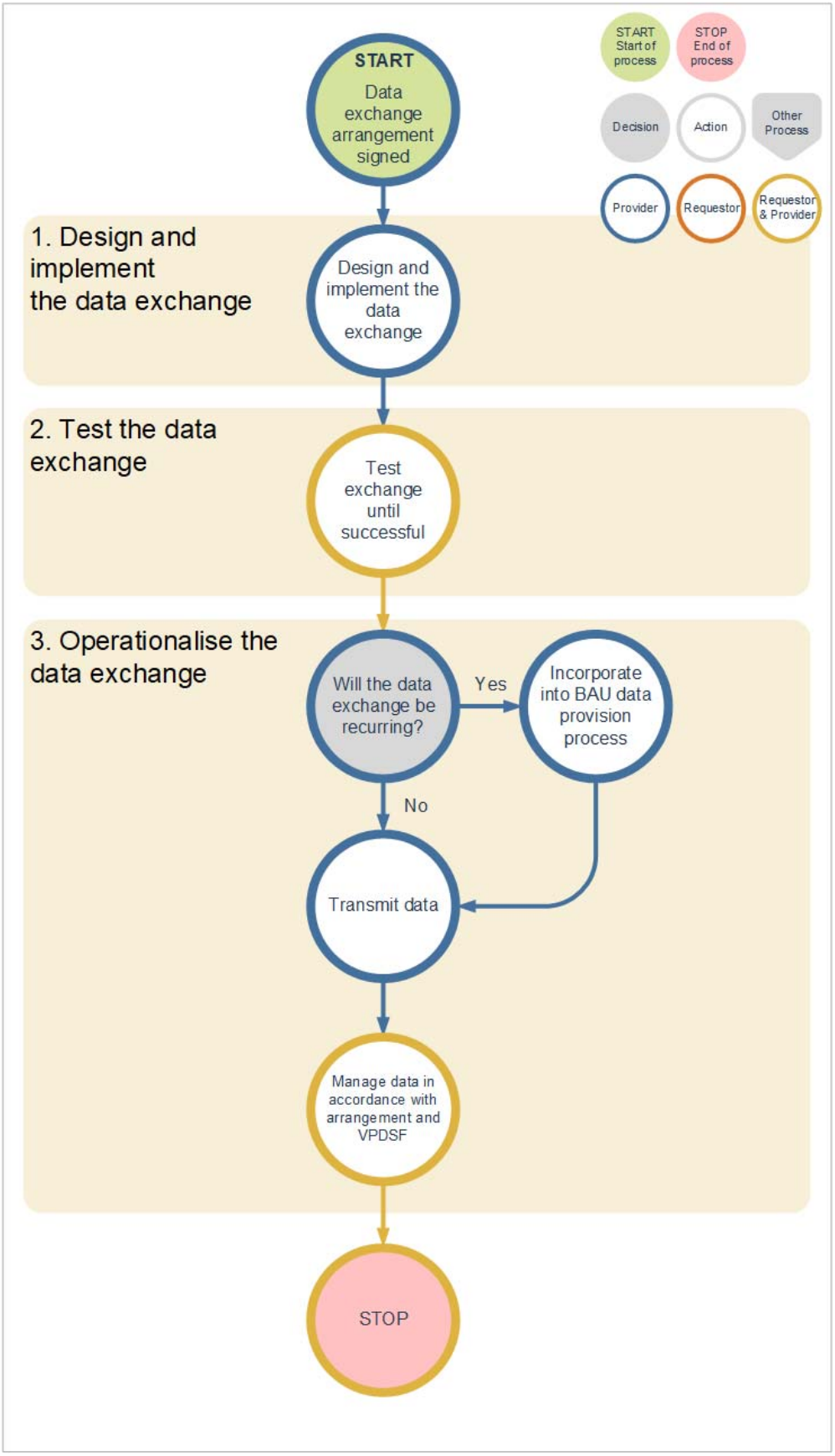
9. Record all requests and data sharing arrangements into a register of data exchange initiatives for government probity and transparency and in accordance with the Victorian Protective Data Security Framework and Standards.
10. Ensure compliance with the requirements for managing public sector data under the Victorian Protective Data Security Framework and Standards.
11. Incorporate data exchange policy and associated processes into department-wide data or information management strategy, policies and processes. Key considerations include data governance and authority, roles and responsibilities, data definitions, data security classifications, risk assessment, data exchange arrangement tools, data transmission methods and issue management.
13. Appoint an owner in each of the Requestor and Provider organisations who will be responsible for the data exchange arrangement.

The general process that a Provider should follow to undertake a data exchange arrangement is shown in Figure 8 - Data exchange process.

The process involves three key steps:

1. Design and implement the data exchange
2. Test the data exchange
3. Operationalise the data exchange.

Figure 8 - Data exchange process



Data exchange design and implementation

Many of the design and implementation considerations have already been discussed in the evaluation (Table 2 and Table 4), arrangement (Table 7) and technical considerations (Table 8). These will be referenced accordingly in addition to an outline of other considerations, in Table 10 – Design and implementation considerations.

The Provider and Requestor columns indicate which considerations are relevant to each party.

Table 10 – Design and implementation considerations

Area	Considerations	Provider	Requestor
Data exchange governance and authorisation	Identify the data exchange owner and custodian for the data exchange transaction. ▪ The owner will be accountable and have the power to authorise the exchange ▪ The custodian will be the contract manager and the main operational point of contact for the exchange.	Yes	Yes
	Organisations quite often do not share their data for various reasons that usually stem from actual or perceived risk of negative consequences. It is important to remember that the government endorses an open data policy on public data wherever possible (refer to DataVic Access Policy and Guidelines). Undertaking a risk assessment and identifying and mitigating risk gaps may help to alleviate the concerns for exchanging data.	Yes	N/A
Enable the exchange	Do both the Provider and Requestor have the appropriate technology, infrastructure, policies and processes to undertake the exchange and securely manage the data? This is discussed in greater detail in: ▪ Enable Exchange section of Table 2 – Access to the source data – Data de-identification – Processes – Data quality – Metadata – Capacity and resources ▪ Safe People, Safe Settings and Safe Data sections of the risk assessment in Table 3 ▪ Technical considerations in Table 8 – Data models, schemas, dictionaries, metadata – De-identification methodology – Transmission method and format – Data management including storage, retention and disposal – Security and confidentiality	Yes	Yes

Area	Considerations	Provider	Requestor
	Artefacts that document the data exchange should be maintained and shared with the Requestor to help aid understanding of the data. These artefacts should include:		
	▪ Data Quality statement	Yes	N/A
	▪ Metadata document	Yes	N/A
	▪ Technical specification document.	Yes	Yes
	Internal artefacts that document the exchange should be maintained include:		
	▪ Data exchange register[7]	Yes	Yes
	▪ Data exchange policies, data models, schemas and process flows	Yes	Yes
	▪ Risk register (in relation to data-related risks).	Yes	Yes
Agree on an arrangement	The terms and conditions for the data exchange should be captured in a data exchange arrangement. Both parties will have responsibilities around how the data is transmitted, managed and used. The considerations outlined in Table 7 of the guideline and Table 2 of the standard should be addressed.	Yes	Yes
Operationalise the exchange	What are the service levels required to be maintained in providing the data? This will inform the development of the arrangement. Refer to the service levels section of Table 7.	Yes	N/A
	What is the process to manage changes to the data that impact data quality and metadata? Refer to the change management section of Table 7.	Yes	N/A
	How will the Provider monitor that the Requestor is complying with the conditions of the arrangement, especially with regard to how they manage and use the data?	Yes	N/A
	How will the Requestor demonstrate to the Provider that they are in compliance with the conditions of the arrangement?	N/A	Yes

Data exchange testing

Testing is an essential part of the data exchange process. It will highlight any issues in the data, process or systems (for both the Provider and Requestor) that need to be addressed and potentially altered in order to ensure a successful operational data exchange.

Testing should be designed and implemented in consultation with IT technical specialists from each of the Provider and Requestor parties to ensure it is carried out correctly.

The key considerations when testing a data exchange are outlined below:

[7] In accordance with the Victorian Protective Data Security Framework and Standards

Table 11 – Testing considerations

Area	Considerations
Designing the testing process	When designing the testing process, all parts of the exchange should be considered including the business process, system and data components. It may be appropriate to conduct testing within a dedicated testing environment where: ▪ The complexity of the exchange is high or ▪ There is an impact to current production systems. The test environment should be an exact replica of the production environment, ensuring issues that would appear in production will be visible in the test environment. Testing may not be required for all components and should be performed to an appropriate level. ▪ What is considered 'appropriate' will depend on multiple factors that include but are not limited to: – The complexity of the exchange – The frequency of the exchange – The level of automation involved in the exchange – The risk associated with the exchange e.g. the higher the risk the more testing required – The security classification and sensitivity of the data. ▪ For example, a frequently occurring, fully automated exchange will require comprehensive testing of all components of the process. One off transfers of a single file, however, may not require detailed testing of the technical exchange component however: – Validation of the data may still need to occur to ensure that it is of the agreed structure and format and of an appropriate level of data quality. – The supporting business process should still be considered and tested.
	The test process should have a clearly documented test plan that defines what testing will be performed, how, when and by whom. The test plan should also document how defects or issues will be documented, tracked, managed and resolved. Where detailed testing of the technical process and or validation of the data is required, it may be necessary to define and document the individual test cases that are to be carried out.
	A range of tests should be considered when designing the testing process. While the tests that are appropriate is highly dependent on the scenario and risk, some example tests that may be carried out include: ▪ End-to-end testing – Does executing the end-to-end exchange process produce the expected result? – Has the data been delivered to the specified location? – Does executing the end-to-end exchange process complete without errors? – Is the supporting business process robust? ▪ Data protection / security – Has the data been de-identified where required? – Has the data been encrypted during transmission if required? ▪ Validation of data – Is data being received as per the agreed schema and format?

	– Is all data present? – Does all data conform to any agreed business rules and required transformation? ▪ Performance testing – Does the data exchange occur within acceptable performance limits? – Is the time to transmit the data acceptable? – Is the load placed on the source system acceptable? – Is the load placed on the receiving system acceptable? ▪ Access – Is access allowed to the data for those with the appropriate privileges and blocked for those without at the receiver end? ▪ Fault tolerance and resiliency – Can mid-exchange failures be recovered from? – Is appropriate logging in place so a failure can be investigated? – What notification process is in place to notify relevant stakeholders?
Executing the testing process	Testing should be conducted until all defects or issues have been resolved, or there is agreement between both the Provider and Requestor that a defect can remain (i.e. the impact of the defect is low). As testing is cyclical and will require input from both the Provider and Requestor, it is important that agreement is reached on resourcing and scheduling from both parties.
	It is generally preferable to conduct testing with both synthetic data (made up to test the known boundaries of the process) and actual data. Whether it is necessary to use synthetic data in the testing process should be considered as part of design. Where the actual data to be transferred has a high security classification or is considered 'sensitive', it may be necessary to conduct testing with purely synthetic data. In this situation, it is extremely important that the synthetic data is representative of the actual data that will be transferred in the exchange.
	The use of automated testing tools and utilities should be considered for more complex data exchanges. Automated testing can help reduce testing timeframes in certain scenarios such as: ▪ Where test cases need to be executed a large number of times ▪ Where changes are expected to be made to the data exchange process over its lifetime and ongoing, repeatable testing is required after each release. Automated testing is not appropriate for all data exchange scenarios and the following should be considered: ▪ An initial development overhead is required to set up automated testing ▪ Automated testing usually requires specialised development resources.
Managing the testing process	Tracking and managing issues and defects Defects and issues should be logged in a register that is accessible by all parties involved in the testing process. It is recommended that a specialised defect or issue management tool is used for this register where one is available.
	Any actual (real) data used during the testing process should be handled according to the agreed access constraints and secured using approved security controls. This may include: ▪ Encrypting data at rest and in transit where required ▪ Restricting access to data from unauthorised individuals ▪ Permanently deleting data at the conclusion of testing.

Operationalise the data exchange

Operationalising a data exchange (where it becomes part of a business-as-usual process) occurs when the exchange of the actual (real, not test) data occurs. This may occur as a one-off or recurring process.

The key considerations when operationalising a data exchange are outlined in Table 12 – Operationalisation considerations. Unless otherwise stated, these considerations apply to both one-off as well as recurring data exchanges.

Table 12 – Operationalisation considerations

Area	Considerations	Provider	Requestor
Change management (only applicable to recurring data exchanges)	Changes may occur from time to time that impact data quality (such as the way data is collected, how dimensions are defined, how measures are calculated, data stops being collected) or impact the format or method of the exchange. ▪ If the changes impact data quality, the Provider should update and reissue the data quality statement to inform the Requestor of the changes ▪ If the changes impact metadata, the Provider should update the metadata and inform the Requestor of the update ▪ If changes impact the format or method of the exchange, the Provider should work with the Requestor to test the new format or method ▪ Change management should be addressed as part of the data agreement arrangement ▪ Notification of changes should be within the timeframe set out in the arrangement or at least when the next tranche of data is provided.	Yes	N/A
Exception handling	Exception handling is required when there is a failure in the data exchange process. This can happen at any point of the process, from data collation to transmission. An example is when system outages (such as source systems of the data, data distribution portals) occur that delay the provision of the data: ▪ The Provider should consider how the failure is going to be remediated ▪ Exception handling (including complaints handling) should be addressed as part of the arrangement in the service levels section.	Yes	N/A
Contract management (including service levels)	As part of the arrangement, both parties should appoint a data exchange owner and custodian. ▪ The owner will be accountable and have the power to authorise or stop the exchange, if required ▪ The custodian will be the contract manager and the main operational point of contact for the exchange. The custodian should monitor each party's obligations as set out in the arrangement and manage issues if they arise. This may include: ▪ Monitoring and reporting performance against the obligations (such as service levels)	Yes	Yes

Area	Considerations	Provider	Requestor
	▪ Ensuring changes and exceptions (see above) are managed ▪ Liaising with the other party to resolve any issues ▪ Monitoring changes to the terms and conditions of the arrangement and amending the arrangement where necessary ▪ Renegotiating or extending the contract, if required Complex, high risk data exchanges may need a regular face to face status meeting.		
Monitoring and reporting	As part of contract management, custodians will need to be able to monitor each party's obligations of the arrangement. This may require reviewing or updating various reports such as:		
	▪ Monitoring log reports of when data is provided to ensure data is provided within the timeframe set out in the arrangement	N/A	Yes
	▪ Monitoring log reports of when data is accessed and by whom to ensure data is only accessed by permitted users	N/A	Yes
	▪ Monitoring system error log reports to identifying system failures	Yes	Yes
	▪ Updating the data exchange register for the data exchange(s)	Yes	Yes
	▪ Monitoring data exchange risks and updating the risk register	Yes	Yes
	▪ Monitoring the sharing, management and security of the data in accordance with the VPDSF and Standards	Yes	Yes
	▪ Where applicable, reviewing the output to ensure de-identification has occurred	Yes	Yes
	▪ If and when required, ensuring the data is returned to the Provider or disposed of in an appropriate manner in accordance with the arrangement.	Yes	Yes
Resourcing	Do all the people involved in the data exchange understand their roles and responsibilities? ▪ The roles that may be involved in an exchange are listed below. The roles do not always have to be held by different people. An individual may sometimes have multiple roles. – Data exchange owner – Data exchange custodian – Information management specialists – Information technology specialists (security, ETL, data warehousing, testing) – Data analysts (analysts, researchers) – Data consumers (internal: business managers, general staff, external: other public sector, private sector, special interest groups, general public)	Yes	Yes

Area	Considerations	Provider	Requestor
	Do all the people involved in the data exchange have sufficient knowledge and skills to manage and or use the data for its intended purpose? If not, education and training may be required to be provided	Yes	Yes

Further information

For further information regarding this standard, please contact Enterprise Solutions, Department of Premier and Cabinet, at: enterprisesolutions@dpc.vic.gov.au.