Data Exchange

14 June 2018

Readiness Assessment Guide

SIA-2017-0195

New Zealand Government

Document control

Document information

Date:	14 June 2018
Owner:	Social Investment Agency

Revision history

Version	Key deliverables	Author	History
0.3	5 April 2017	Doug Lambert, Architect	Initial Draft
0.4	20 July 2017	Doug Lambert, Architect	Minor updates
1.0	21 July 2017	Tracey McFadyen	Update for rebranding to SIA
2.0	26 April 2018	Tracey McFadyen	Minor updates
3.0	14 June 2018	Amy Williams	Minor updates

Creative Commons Licence

Liability

While all care and diligence has been used in processing, analysing and extracting data and information in this publication, the Social Investment Agency gives no warranty it is error free and will not be liable for any loss or damage suffered by the use directly, or indirectly, of the information in this publication.

Citation

Social Investment Agency 2017. Data Exchange – Readiness Assessment Guide. Wellington, New Zealand.

Contents

Introduction

This Readiness Assessment Guide is structured into two major parts:

1. Readiness Assessment Guide

2. Readiness Assessment Checklists
    a. Initial Capability Checklist
    b. Final Capability Checklist

The Guide details the requirements for an organisation to connect to the Data Exchange, with explanatory notes. The Initial Capability Checklist and Final Capability Checklist are intended to be completed at the outset and completion of connecting to the Data Exchange, respectively.

Related documents are referenced throughout this guide and collectively in the References section.

Background/summary

Social Investment

Social investment is about improving the lives of New Zealanders by applying rigorous and evidence-based investment practices to social services. Social investment answers questions such as ‘what works, for whom, where and at what costs’. It’s called social *investment*, not spending, because it’s about investing resources upfront to enable people in need to thrive over the longer-term. Four elements of social investment:

- Use data smarter to better understand people's current and future needs
- Systematically measure the effectiveness of services in meeting people's needs
- Measure long-term outcomes for people over their lifetime and feeding back into decision-making
- Understand the fiscal implications of better outcomes and help to manage the long-term costs to government.

Social Investment Agency

The SIA will use data and analytics to provide evidence-based information, tools, guidance and products to social agencies to help inform their investment and decision-making and create improved outcomes for vulnerable New Zealanders.

An essential infrastructural requirement is the safe and secure sharing of data between social agencies, which is where the Data Exchange comes in.

Readiness Assessment Guide

The major considerations involved in connecting an organisation to the Data Exchange and transferring data have been organised into a few high level themes, below. Themes would generally be considered in the order presented.

Each theme:

- Starts with a key question intended to frame thinking.
- Is described with introductory detail.
- May contain references to related documents.

The framing questions are intended to gauge the current capability of the connecting organisation – answers to these questions are to be recorded in the Initial Capability Checklist at the outset of connecting, and again in the Final Capability Checklist at the completion of connecting and having transferred data.

Business

How well understood are the business benefits and obligations of using the Data Exchange?

The Data Exchange is fundamentally a secured data transfer channel. The technical requirements to connect to and use the Data Exchange are low and the economics are compelling. As more organisations connect and transfer data the value proposition increases: parties who have data you want may already be connected, perhaps even sharing the data you most need.

Where the counter-party required to transfer data is not already connected, both organisations should engage and agree how to proceed as early on as possible.

Justifying the effort and distraction of connecting to the Data Exchange, small as it is, can be alleviated by identifying a specific business case that would be advantaged through the use of a secured, easy to operate, and low cost data transfer channel. SIA recommends organisations frame up at least a light weight business case to understand the role and requirements of involving the Data Exchange in any initiative. SIA has developed a use case guide that organisations are welcome to take advantage of.

Refer to:

- Data Exchange Use Case Guide

Governance

How clear and explicit is the connecting organisation’s understanding and allocation of responsibilities about using the Data Exchange?

SIA, as the Data Exchange Operator, is responsible for:

- Governing the use of the Data Exchange
- Facilitating connectivity to the Data Exchange

An organisation sharing data using the Data Exchange is responsible for:

- Governance and security of data within and leaving their organisation
- Preparation of data to be shared, including the application of business rules to data
- Presentation of data to be shared to the Data Exchange Agent

An organisation receiving data using the Data Exchange is responsible for:

- Governance and security of data within their organisation
- Collection of data as it arrives from the Data Exchange Agent
- Use of data according to legal and agreed conditions

EightWire, as the provider of the Data Exchange, is responsible for:

- Secure transfer of data between Data Exchange Agents
- Availability of the Data Exchange
- Delivering training
- Support

Connectivity to the Data Exchange does not change or compromise existing accountabilities or responsibilities.

To support the use of the Data Exchange, each connected organisation must establish two roles:

- Data Exchange Agent Administrator, responsible for:
  - On-going management of the Data Exchange Agent
  - Managing security accounts for people permitted to use the Data Exchange

- Data Exchange Data Manager, responsible for:
  - On-going management of configuration that defines data to be shared or received

Legal

How well does the connecting organisation understand the variety of data sharing legal provisions that entitle them to share or receive data?

Legislation conveys clearly data collection and management responsibilities, particularly for data about people. Some organisations have legislation specific to their mandate (Inland Revenue, Statistics NZ) and others operate under more general legislation (Privacy Act 1993). It is essential that each data collecting and data sharing organisation robustly understand their legal obligations and work within these boundaries.

When legislation does not detail data sharing permissions, a collection of additional mechanisms are available:

- Agreed Information Sharing Arrangements (AISA): where legislation does not prohibit or does not make clear data and information sharing options an AISA can be drawn up between the parties involved in a particular scenario. AISAs are approved by Cabinet and approved by the Governor-General as an Order in Council.
- Contracts: legislation permitting, contracts may be drawn up between parties to make clear what data and information each party will pass to the other.
- Memorandum of Understanding (MoU): an MoU is evidence of consideration by data sharing parties that they are permitted to share cited data. MoUs do not extend law or any other permitting mechanism, they simply make clear under what provisions data sharing is taking place.

SIA has developed a Data Sharing MoU Template for connecting organisations to use as they see fit.

Refer to:

- Data Exchange Data Sharing MoU Template

Privacy

How well does the organisation understand the conditions of the Privacy Act 1993 which apply to their collection, storage and sharing of personal information?

The Privacy Act 1993 sets out a range of conditions which apply to the collection of personal information. Organisations are likely to have differing levels of understanding about their obligations under the Privacy Act 1993, and the conditions they need to meet to share data on the Data Exchange.

The SIA has developed a privacy screening template to help organisations assess their readiness to connect to the Data Exchange.

Refer to:

- Data Exchange Privacy Impact Assessment

Process

How developed is the data management practice of the connecting organisation?

For most organisations, using the Data Exchange is a straightforward extension to existing business processes. If data to be shared is already being extracted from operational systems and is being transferred using secured devices, email, optical storage, or otherwise, then the Data Exchange simply replaces these transfer mechanisms. Data must still be extracted and made available to the transfer mechanism.

The provider of the Data Exchange, EightWire, provide support and training for connecting organisations. SIA has developed in conjunction with EightWire a suite of support and training guides.

Refer to:

- Data Exchange User Guide

Data

How clear is the organisation in their understanding of the necessary treatments and management of data to be transferred?

The following points about data transfers using the Data Exchange are important to understand up front:

- Organisation transferring data using the Data Exchange always retains full control of the data and systems in their organisation.
- The Data Exchange transfers data contained in files and databases – it does not transfer the actual file or database containers, just the contents. The source and destination containers can be different and this is a feature of the Data Exchange: storage format conversion on the fly.
- Subsets of data can be transferred by specifying filtering criteria when configuring data sharing on the Data Exchange.

- Data can only be received by organisations connected to the Data Exchange that have been allowed to receive the data by the organisation sharing the data. Shared data is never available to "just anyone".
- Data is streamed from the data sharing organisation to the data receiving organisation via the Data Exchange. Once data arrives at the data receiving organisation it is no longer available on the Data Exchange.
- All transferred data remains within New Zealand.
- All transferred data is encrypted between Data Exchange Agents.

The general process involved in transferring data from one organisation to another is:

1. **Agreement**: The sharing organisation and the receiving organisation agree why data is to be shared between them, what data is to be shared, when data is to be shared, who is responsible for sharing and receiving data, and how shared data will be used. These considerations are usually detailed in business and legal documents such as contracts, legislation, AISAs, or MOUs.
2. **Preparation**: Data to be shared is formatted as agreed with the receiving organisation. This formatting is done prior to the data being made available to the Data Exchange. Organisations will often already have data extraction processes in place from their CMS and these can typically be duplicated.
3. **Presentation**: Once prepared, data is to be made available to the Data Exchange Agent. This will typically be a suitably secured Windows server that has the Data Exchange Agent installed. This secured staging location is referred to as the "data staging server". Data can be staged here in database tables, spreadsheets, or text files.
4. **Transfer**: The entirety of the retrieval of data by an Agent from the staging point, the data passaging the Data Exchange, the delivery of the data to the receiving staging point.
5. **Receipt**: Acceptance that all intended data to be transferred has been received.
6. **Consumption**: The use of the data beyond the receiving staging point. The use of the data must of course be in accordance with the Agreement established at the outset.

The Data Exchange does not remove shared data once it is transferred. Removal of data presented for sharing is the responsibility of the data sharing organisation.

Security

How well understood and implemented are security requirements?

Phase 1 of the Data Exchange was certified by the Ministry of Social Development to transfer data classified up to and including IN CONFIDENCE. In practice this means that data about people could only be transferred if it is anonymised.

In November 2017 certification was raised to SENSITIVE. This allows for the transfer of non-anonymised personal data.

The Data Exchange encrypts transferring data from Agent to Agent. This is done in three phases:

1. Data is encrypted by the sharing Agent before being sent across the internet to the Data Exchange.
2. Upon arriving at the Data Exchange the data is decrypted and then encrypted using a different cryptographic scheme before being stored on disk to await delivery the the receiving Agent.
3. Data is decrypted from disk and re-encrypted by the Data Exchange before it is delivered to the receiving Agent. Upon arrival at the receiving Agent the data is decrypted and written to a database or file.

The encryption used while data is in transit and on disk are different schemes. This is intended to result in illicit access to the data more difficult as two different cryptographic schemes rather than just one are in use.

Also, the Agent requires the Data Exchange to prove its identity as well as the Data Exchange requiring the Agent to prove its identity: mutual authentication. This lifts the robustness of the Data Exchange by reducing the likelihood of a successful security attack.

It is the responsibility of each connecting organisation to ensure two things:

1. They are satisfied with the security robustness of the Data Exchange for the type of data they are transferring.
2. They are satisfied their own connectivity to the Data Exchange is suitably secure.

SIA can provide security certification details of the Data Exchange to inform a connecting organisation of its robustness. SIA has also developed security primer tools to help an organisation meet their own security assessment requirements. These tools should significantly reduce the time and cost for an Agency to complete a Security Risk Assessment (SRA).

Refer to:

- Data Exchange Security Risk Assessment Tool

Systems and Infrastructure

How suitable is the organisation's current infrastructure, network configuration, and technical support to accommodate the Agent and data staging?

The Data Exchange comes in two major parts:

- The collection of cloud hosted services that manage data transfers and perform data transfers.

- Small software Agents that are installed at each connecting organisation and transfer data to and from the cloud services.

The cloud services are in two collections:

- The Management Service is responsible for managing data source definitions, job definitions, schedules, and auditing. This is hosted by Microsoft Azure in Australia. No data is transferred via this service.
- The Data Processing Service transfers data between Agents and is managed by the Management Service. This is hosted by Revera in New Zealand. Data is transferred only via this service.

Connecting to the Data Exchange involves the following technical requirements:

- A Windows server or desktop machine for installing the Agent on; this is typically a virtual machine. The hardware and software requirements of this machine are low. This machine does not have to be dedicated for the Agent but it is recommended that a dedicated machine is used to reduce security concerns. This machine should be in a secured part of an organisation's network such as a DMZ.
- Installation of the Agent. This is a straightforward task that takes about five minutes. The Agent installer is downloaded from the Data Exchange web site. Once installed the Agent can be configured to automatically update itself as new versions become available if this is the preference of an organisation. The security account under which the Agent executes must have access to the data that will be transferred.
- Configuration of network security controls such as firewalls and proxies to allow the Agent and the Data Exchange to communicate with each other.
- Presentation of the prepared data for sharing, or presentation of a secured staging area for data to be written to.
- Configuration to point the Agent to the data staging area and data to be transferred.

SIA has developed a Solution Design Guide to help organisations understand how to connect to and use the Data Exchange.

Refer to:

- Data Exchange Solution Design Primer

Delivery

How clearly understood, appropriate, and agreed is the approach to connecting the organisation and the Data Exchange?

Everything associated with the logistics of connecting an organisation to the Data Exchange and completing the first transfer. This is traditional project management.

Ideally, a single person at the connecting organisation would be the primary point of contact for the Data Exchange Operator, and the Data Exchange Operator would have a single point of contact for the connecting organisation. These people would often be project managers.

Between the two organisations a delivery approach needs to be agreed and communicated to all parties involved in delivering connectivity to the Data Exchange.

Refer to:

- Data Exchange Implementation Planning guide

Assessment Checklists

This Readiness Checklist is an abbreviated form of the Readiness Guide and can be used as an overview of readiness requirements and as a progressive checklist of activity completion as connectivity to the Data Exchange unfolds.
Initial Capability Checklist

This checklist is intended to be read and responded to at the outset of considering connecting to the Data Exchange. The same checklist of questions is intended to be asked and answered once an organisation is connected to the Data Exchange. Two swipes at the same checklist are used to understand the nature of change an organisation had to undertake to connect to the Data Exchange. This information is useful for the connecting organisation and for SIA.

Theme	Question	Response
Business	How well understood are the business benefits and obligations of using the Data Exchange?	
Governance	How clear and explicit is the connecting organisation's understanding and allocation of responsibilities in regard to using the Data Exchange?	
Legal	How well does the connecting organisation understand the variety of data sharing legal provisions that entitle them to share or receive data?	
Privacy	How well does the organisation understand the conditions of the Privacy Act 1993 which apply to their collection, storage and sharing of personal information?	
Process	How developed is the data management practice of the connecting organisation?	
Data	How clear is the organisation in their understanding of the necessary treatments and management of data to be transferred?	
Security	How well understood and implemented are security requirements?	
Systems and Infrastructure	How suitable is the organisation's current infrastructure, network configuration, and technical support to accommodate the Agent and data staging?	
Delivery	How clearly understood, appropriate, and agreed is the approach to connecting the organisation and the Data Exchange?	

Final Capability Checklist

This checklist is intended to be completed once an organisation has connected to the Data Exchange and transferred data. The answers to this checklist should be compared to the answers from the Initial Capability Checklist to understand any changes in capability required to use the Data Exchange.

Theme	Question	Response
Business	How well understood are the business benefits and obligations of using the Data Exchange?	
Governance	How clear and explicit is the connecting organisation's understanding and allocation of responsibilities in regard to using the Data Exchange?	
Legal	How well does the connecting organisation understand the variety of data sharing legal provisions that entitle them to share or receive data?	
Privacy	How well does the organisation understand the conditions of the Privacy Act 1993 which apply to their collection, storage and sharing of personal information?	
Process	How developed is the data management practice of the connecting organisation?	
Data	How clear is the organisation in their understanding of the necessary treatments and management of data to be transferred?	
Security	How well understood and implemented are security requirements?	
Systems and Infrastructure	How suitable is the organisation's current infrastructure, network configuration, and technical support to accommodate the Agent and data staging?	
Delivery	How clearly understood, appropriate, and agreed is the approach to connecting the organisation and the Data Exchange?	