COMMONWEALTH OMBUDSMAN

Power BI Solution
Privacy Impact Assessment

V 1.0

July 2018

Privacy Impact Assessment Report – Contents

PRIVACY IMPACT ASSESSMENT

Role of OAIC

Note: The Privacy Act gives the Information Commissioner (IC) a power to direct an agency to provide a PIA to the OAIC, if the Commissioner considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals. (s33D Privacy Act) This includes when the agency proposes to engage in a new activity or function, or substantively change an existing activity or function e.g., a substantive change to the system that delivers an existing function or activity.

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is a systemic assessment of a project that may have privacy implications. The term project includes:

- policy proposal
- new or amended legislation
- new or amended program. system or database
- new methods or procedures for service delivery or information handing
- changes to how information is stored

The PIA identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating adverse impacts. It will go beyond assessing the project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk.

This PIA will also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

This PIA should be prepared with reference to the Commonwealth Ombudsman's Privacy Impact Assessment Guidelines

Power BI Solution

The Information and Communication Technology Section is commencing the development of a new Business Intelligence & Reporting capability for the Office of the Commonwealth Ombudsman (OCO). The capability will utilise existing OCO system data, from Resolve and Zeacom (Phone system).

The solution will utilise Microsoft Power BI, and is likely to include a cloud based Software as a Service (SaaS), known as the Power BI Service.

1. Threshold Assessment

Will any personal information be collected? If yes, record a brief description of the personal information that will be collected, used or disclosed (such as name, address, date of birth, health information etc.).

The Business Intelligence solution harvests data from existing data holdings within the OCO. As such no new information is collected, instead data is consumed and stored separately in a format suitable for reporting.

The scope of the Privacy Impact Assessment is the Power BI Reporting system and the data that it utilises. The Resolve system and associated data, and the Zeacom system and associated data are outside of the scope of this Privacy Impact Assessment.

Private data has been explicitly excluded from the Power BI Solution as detailed in the Power BI Architecture (See the attached – ICT Business Intelligence Capability Development Architecture, Page 4 - Architectural Principles, which states:

"AP1.2 - The BI Solution will not consume, host or display private data. The data is de-identified." [1]

The above principle is implemented via the following:

- The On-Premises Gateway

[1] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#meaning-of-reasonably-identifiable

Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:[28]

- *the nature and amount of information*
- *the circumstances of its receipt*
- *who will have access to the information*
- *other information either held by or available to the APP entity that holds the information*
- *whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'[29]*
- *if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual.*

- The Reporting Data Interface
- The Power BI Change Process

The components mentioned above are all designed to mitigate the risk of access and publishing of private or sensitive data. The technical components of the Reporting Data Interface mitigate the risk of unauthorised access to data (e.g. system compromise). The Change process mitigates the risk of unintended/inadvertent or un-approved publishing of private data to the Power BI reporting system.

Data that could reasonably identify an individual (as per the definition in footnote 1) is not consumed, stored or reported on by the power BI system.

Azure On-Premises Gateway

The Microsoft On-Premises Data Gateway (Data Gateway) is a service used to broker connections between the on-premises data source (e.g. SQL Server database) and the relevant Azure service; in this case Power BI.

The Data Gateway is implemented on premises and used to load, and subsequently periodically refresh data held in a cache in the Power BI Service for reporting and analytics.

The Data Gateway Service polls the Azure Service Bus checking for requests in the queue from the Power BI Service to the relevant data source. If a request is waiting in the in the queue, the Service bus receives the encrypted connection credentials in the request, and applies them in a connection request. If successful the Data Gateway completes the connection to the Service bus, and the results are passed back to the Power BI Service via the Azure Service Gateway and the Azure Service Bus.

All connections from the Data Gateway are Outbound and are encrypted using TLS/IP (1.2).

Reporting Data Interface

The reporting data interface (RDI) is a set of gateway layers that limit and control the access to the underlying data holdings with the following objectives:

- Implement a consistent interface for accessing underlying data for the purposes of reporting
- Implement controls over data access, excluding private data
- Provide limited filtering to avoid verbose data being exposed and uploaded to the BI Layer

Creation or modification of RDI views is limited to administrative users, and is controlled in the Power BI Change Process. See the section: Power BI Change Control Process for details.

This approach implements another level of control mechanism over access to OCO data, further mitigating the risk of the system being compromised.

Power BI Change Control Process

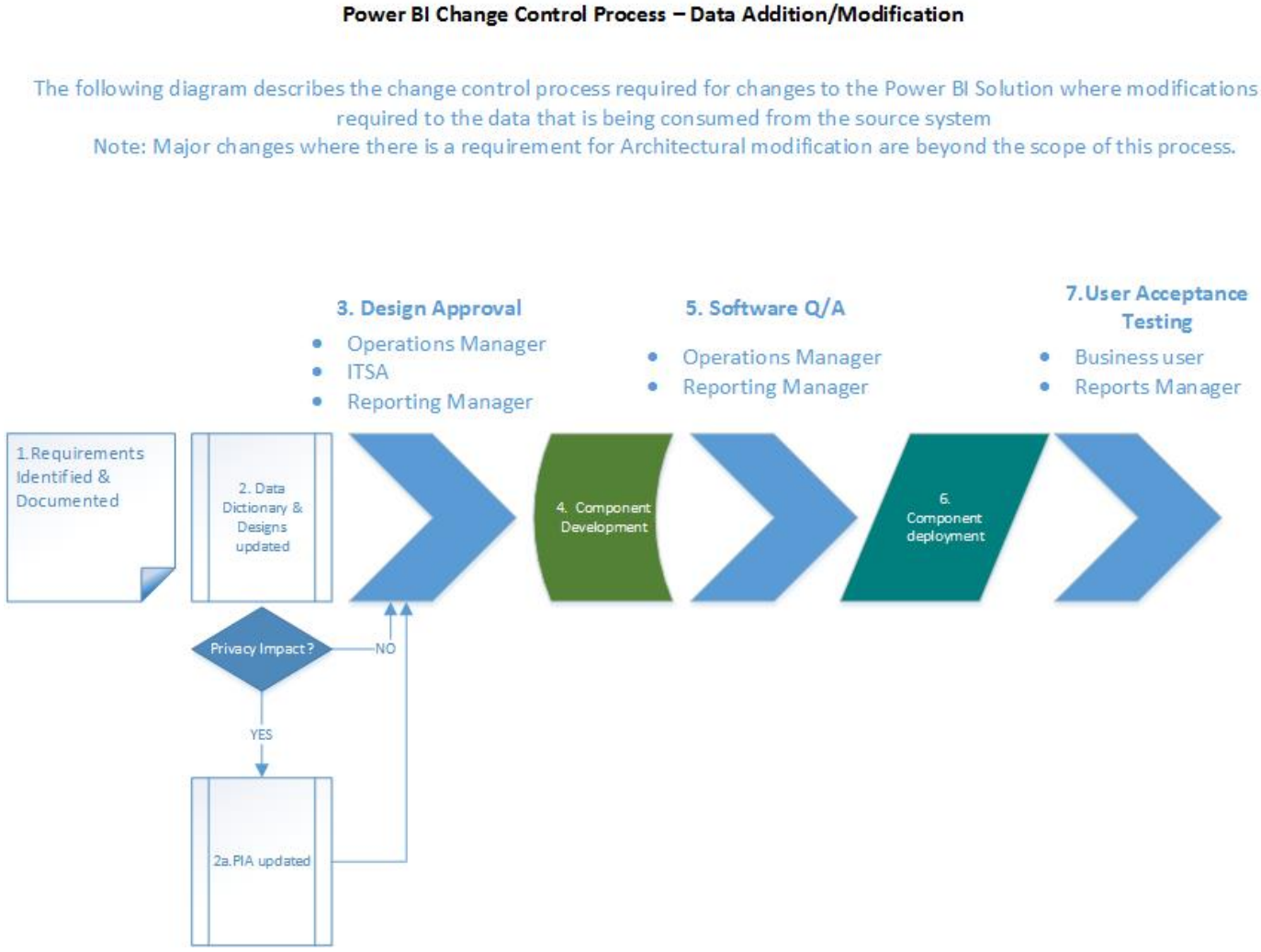

Figure 1- Power BI Change Control Process

The Power BI Change control process is applied where there are changes to the data being consumed by the Power BI Service. Additional Reports or dashboards that utilise existing reporting data (data already available in the Power BI Data Model) are not required to follow this process.

The Power BI Change control process contains the Following steps:

1. Requirements Identified & Documented
   The reporting requirement is relayed to the IT team and documented.

2. Data Dictionary and other Designs updated.
   The designs and / or Data Dictionary are updated where required. At this point a decision is made whether there is a Privacy Impact, and if so the Privacy Impact Assessment is updated and the review approval process is applied.

3. Design Approval.
   The updated designs mentioned in Step 2 are reviewed and approved (or amended as required). Approval is sought from the Operations Manager, The ITSA (IT Security Advisor) and the Reporting Manager.

4. Component Development.
   The new or changed components are developed locally within the office's network (ie. Not the Power BI Production cloud environment).

5. Software QA (Quality Assurance).
   The Changes are Quality assured for accuracy, performance etc. against the requirements and designs.

6. Component Deployment.
   The developed Components are deployed to the required servers (SQL server, Power BI Service etc.).

7. User Acceptance Testing.
   The Business Manager /Stakeholder and reports manager exercise the functionality implemented and accept the changes (or highlight issues and rework as required).

2. Plan the PIA.

General Description

Name of Program: Power BI Solution Implementation
Date:05/06/2018
Name of Section/Branch: Information and Communication Technology Section/ Operations Branch
PIA Drafter: James Marshall
Email: James.Marshall@ombudsman.gov.au Phone: #464
Program Manager: Paul McInerney
Email paul.Mcinerney@ombudsman.gov.au Phone: # 0110

Definition – Project: For the purpose of this document, the term project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals,
- new or amened legislation, programs, activities, systems or databases,
- new methods or procedures for service delivery or information handling
- changes to how information is stored

3. Describe the Project

The ICT Section, in the Corporate Branch of the OCO is implementing a business intelligence and reporting capability.

This will enable analytics capability for staff who require reporting and decision support functions in their work. The new capability will facilitate timely and evidence based decision making, enabling the office to predict and plan for the changing nature of work undertaken.

The solution will use Microsoft Power BI (http://www.powerbi.com) and will leverage data from the Resolve case management system and from the Zeacom phone logging system.

Reporting functional requirements range from statistical analysis of Resolve Cases (e.g. totals by case type, Team, Agency of approach etc.), to operational reporting (e.g. elapsed time taken to resolve cases etc.).

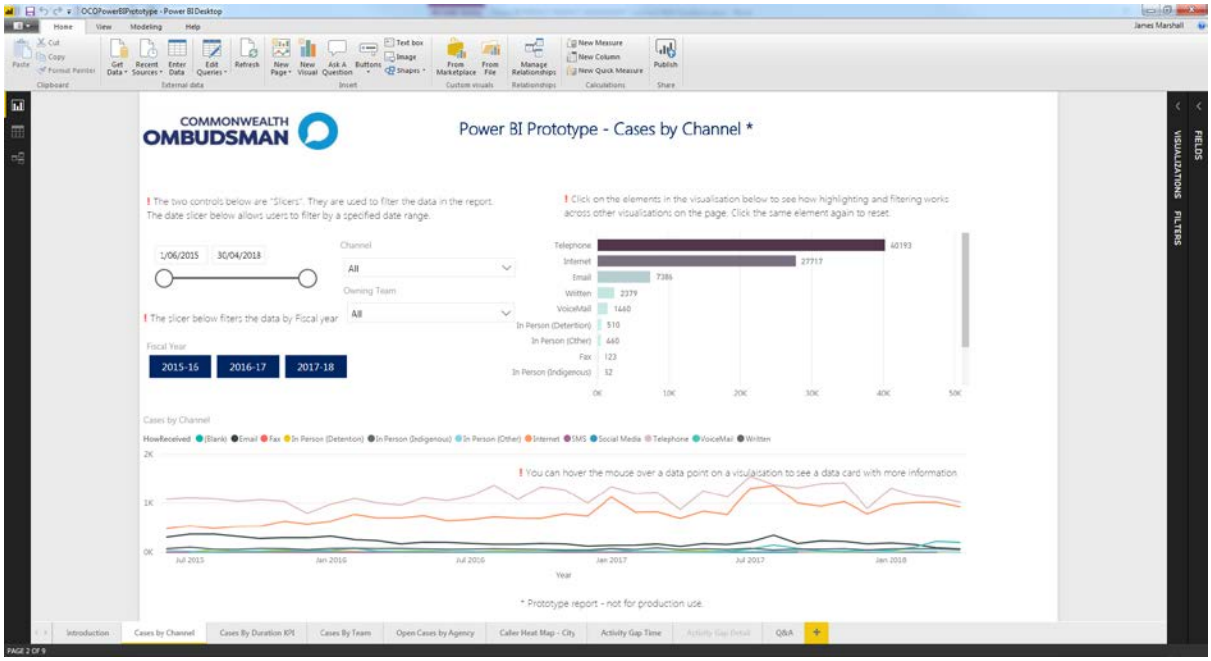

Figure 2- Power BI Prototype statistcal report

The project has been underway since mid-February, and Privacy and Security have been at the centre of the architectural design focus for the solution. An Initial on-premises only (no cloud component) prototype has been completed and is in use by project stakeholders, providing a vehicle for forming ideas and requirements.

The solution design is complete, with an initial tranche of reports in development, along with data access components (Databases, Schemas, Views etc.).

Private and identifying data has been explicitly excluded from the solution (please see the section Reporting Data Interface for details on how this is achieved).

4. Identify and consult with stakeholders

In order to provide an understanding of the system capability and capacity the following activities have been undertaken:

- Demonstrations of the prototype system were provided to stakeholders, including a discussion on Architectural Principles on Privacy and de-identified data.
- The working prototype has been deployed to the stakeholders for familiarisation and experimentation, and requirements discovery.
- Extensive project and architectural documentation has been provided and distributed to relevant audiences.

The list of stakeholders engaged includes (but is not limited to);

- Senior Assistant Ombudsman (Office senior executives)
- IT team
- Project stakeholders
- Information Technology Security Advisor (ITSA)
- Legal and Information section

Private and identifying data has been explicitly excluded from the solution (please see Reporting Data Interface for details on how this is achieved).

5. Map Information Flows

Describe and map the project's personal information flows.

VERIFICATION

There is no personal information included in the design for the Power BI Solution. Personal and identifying data is explicitly excluded from the Reporting Data Interface (the "pipeline" that the data flows through). Please see Reporting Data Interface for details on how this is achieved and APPENDIX A - Power BI Solution Iteration 1 Data Dictionary for the list of data elements that are included.

COLLECTION

There is no personal information included in the design for the Power BI Solution. Personal and identifying data is explicitly excluded from the Reporting Data Interface and is not passed to power BI from the underlying solution. Please see Reporting Data Interface for details on how this is achieved and APPENDIX A - Power BI Solution Iteration 1 Data Dictionary for the list of data elements that are included.

Please see APPENDIX A - Power BI Solution Iteration 1 Data Dictionary for a list of data elements that are consumed by the Power BI solution.

USE

There is no personal information included in the design for the Power BI Solution. Personal and identifying data is explicitly excluded from the Reporting Data Interface and is not passed to power BI. Private and identifying data has been explicitly excluded from the solution . Please see Reporting Data Interface for details on how this is achieved and APPENDIX A - Power BI Solution Iteration 1 Data Dictionary for the list of data elements that are included.

INFORMATION QUALITY

Information is queried directly from the source database with minimal transformation. The data is a largely a reflection of that which is contained in the source database (i.e. Resolve), and as such the quality of the data contained in the reporting solution relies on the quality of the data in the source database. Where calculations are required in the solution to generate reportable values, the calculations are quality assured as part of the defined change control process. Please see the section Power BI Change Control Process for details.

The data elements that are included in the BI solution are first detailed in design documents (please see APPENDIX A - Power BI Solution Iteration 1 Data Dictionary), evaluated via the ICT change control process, including assessment by the IT Operations Manager, the IT Security Adviser and system stakeholders. Please see Power BI Change Control Process for the details of the process change.

SECURITY

The architecture for the solution has been designed to secure the underlying source databases and ensure that only authenticated and authorised access is possible via the BI data refresh channel. In Addition to the standard recommended "Microsoft On-Premises Gateway[2]" configuration in the solution architecture, additional controls have been designed to protect private and sensitive data in the underlying source systems ie. Resolve).

Several security additional database gateways have been included in the solution to further reduce the risks of unauthorised or accidental access to data that has not been approved for reporting use.

The power BI Solution will utilise Azure Active Directory for user authentication and authorisation, which offers seamless integration with Power BI and the OCO's on-site Active Directory implementation.

RETENTION AND DESTRUCTION

Reporting data is stored in a cache in Microsoft Power BI's back end encrypted data stores. Being a Software as a Service (SaaS) this data is not accessible via any other channel than the Power BI Service, using the inbuilt Authentication and authorisation mechanisms.

[2]Microsoft On-Premises Data Gateway documentation : https://docs.microsoft.com/en-us/power-bi/service-gateway-onprem-faq

In general the cache of data in Power BI will be updated every 24 hours, and can be cleared / deleted by an administrator on demand via the provided tools.

6. Privacy Impact Analysis and Compliance Check

PRIVACY IMPACT ANALYSIS

The privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

ENSURING COMPLIANCE

You will need to consider whether your project complies with each of the Australian Privacy Principles (APPs).

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	Principle 1 – Open and transparent management of personal information The agency must have a clearly expressed and up to date APP privacy policy about the management of personal information by the agency.	*No Personal or identifying Information collected or used in this solution. A Case Number can be related back to the Caller involved, but not by a reasonable member of the public and not without access to the internal Resolve data or system. Within the definitions provided by the Office of the Australian Information Commissioner (1, [3]) the data contained in the reporting solution would not be classified as identifying or personal.*	*Complies*	

[3] https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information : When is an individual 'reasonably identifiable'? "The inclusion of the term 'reasonably' in the definition of personal information means that where it is possible to identify an individual from available information, the next consideration is whether the process of identification is reasonable to achieve. This is determined by asking whether, objectively speaking, it is reasonable to expect that the subject of the information could be identified. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as 'personal information'."

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
2	Principle 2 – Anonymity and pseudonymity Individuals must have the option of not identifying themselves, or of using a pseudonym, note exceptions.to this rule apply.	*All references to individuals are provided in a non-identifying context. The Caller entity makes reference to the approximate location (Postcode/Suburb) that a caller has provided in Resolve, however no identifying information that would uniquely identify a person is included.*	*Complies*	
3	Principle 3 – Collection of solicited personal information Limits apply to only collect information where the information is reasonably necessary for or directly related to one or more of the agency's functions or activities.	*No Personal or identifying Information collected or used in this solution. Please see the data dictionary in* APPENDIX A - Power BI Solution Iteration 1 Data Dictionary *for the data elements consumed.*	*Complies*	
4	Principle 4 – Dealing with unsolicited personal information Determine whether or not the agency could have collected the information under APP 3. If not, where it is lawful and reasonable to do so destroy or de-identify the information.	*No unsolicited personal information is included in the solution.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
5	Principle 5 – Notification of the collection of personal information Inform the person what information you are collecting, the purpose or use of the information and how they may access or complain about the use of the information. Also inform them if the agency is likely to disclose the information to overseas recipients.	*OCO publishes an APP 5 Privacy statement notifying the public of its collection, purpose and use of personal information.*	*Complies*	
6	Principle 6 – Use or disclosure of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	*Data is provided by callers to allow the OCO to investigate complaints on their behalf. The reporting solution is used to provide information and decision support to supply this service more effectively and efficiently.*	*Complies*	
7	Principle 7 – Direct marketing Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.	*No information will be used for direct marketing, personal or other.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 8 – Cross-border disclosure of personal information. Requirement to ensure overseas recipient does not breach APPs note exceptions apply e.g., information is subject to a law similar to APP's.	*No data will be available to overseas recipients (other than OCO staff members abroad, should that scenario arise). The reporting solution is only available through authorised access.*	*Complies*	
9	Principle 9 – Adoption, use or disclosure of government related identifiers. Only assign unique identifiers where permitted. Agency should not disclose identifiers unless permitted.	*Identifiers for public callers / Complainants will not be applied.*	*Complies*	
10	Principle 10 – Quality of personal information. Ensure information is accurate, up to date, complete and relevant prior to using it.	*No Personal or identifying Information collected or used in this solution.* *Other reporting information will be uploaded from the source daily.*	*Complies*	
11	Principle 11 – Security of personal information. Take care of the information and protect it against loss, modification, or unauthorised disclosure and other misuse. When no longer required either destroy or de-identify it.	*No Personal or identifying Information collected or used in this solution. For details on the security Please refer to the sectio on security; ICT_Business_Intelligence_Capability_Architecture , P12 "Security" for details.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
12	Principle 12 – Access to personal information People have a right to see their personal information noting exceptions apply, eg., FOI exemptions.	*No Personal or identifying Information collected or used in this solution. Additionally, callers (Complainants) will not have access to the Power BI Solution. This is an internal OCO system.*	*Complies*	
13	Principle 13 – Correction of personal information Agency must take steps to correct personal information held, ensure information is up to date, accurate, complete and not misleading.	*No Personal or identifying Information collected or used in this solution. The data that is stored in Power BI data sets will generally be updated every 24 hours.*	*Complies*	

7. Privacy Management – Addressing Risks

A risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating
R1	As private data is explicitly excluded from the solution, the only residual risk is that in a potential future development iteration of the system, private data is inadvertently consumed by the system and exposed by the system from the source database. Note that in this scenario the data would still only be available to authenticated OCO staff. This would still not represent a "Data Breach[4]".	1. Implement change control process with multiple quality gates required for changes to be deployed. 2. Implement Technical constraints such that several steps across multiple solution nodes are required to add any data elements.	Low	Minor	Low

Please see the attached Power BI IT Security Risk Management Plan which contains a full set of system & security risks.

[4] "A data breach happens when personal information is accessed or released without authorisation, or is lost." AOIC Definition https://www.oaic.gov.au/individuals/data-breach-guidance

Recommendations

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

Ref	Recommendation	Agreed Y/N
R- 01	Continue with the implementation of the system as designed, given the solution architecture has excluded the private data and identifying data from the product.	
R- 02	Report to the privacy delegate if the privacy status/ risk profile of the solution should change.	

Signatures

_____ _____

Name of Senior Assistant Ombudsman responsible Signature

_____

Date

Rodney Lee Walsh, Privacy Delegate _____ _____

Signature

APPENDIX A - Power BI Solution Iteration 1 Data Dictionary

The data dictionary below details the data elements utilised in the solution;

OCO Power BI Resolve data model

Version 1.1

This workbook is a data dictionary for the OCO BI development project.
All of the data elements consumed by Power BI should be defined in this workbook.

The properties of each attribute contained are as follows:

Attribute Name – The user friendly name used in the data model in Power BI
Field Name – The database field name where the attribute originates (where applicable)
Table Name - The database Table name where the attribute originates (where applicable)
Data Type – The type of data the attribute holds
Description – Description of the Attribute
Identifying Category – The category of identifier that the attribute has, within the context of personal Identifiers / de-identification.
Remarks – Remarks on the attributes identifying category
Attribute Source – Where the values contained in the Attribute are sourced from

Please note the following:

This is a living document, it will change as new reporting capability is developed.
Data attributes should be defined in this document and approved by the Director of IT and the ITSA (or delegate) prior to implementation

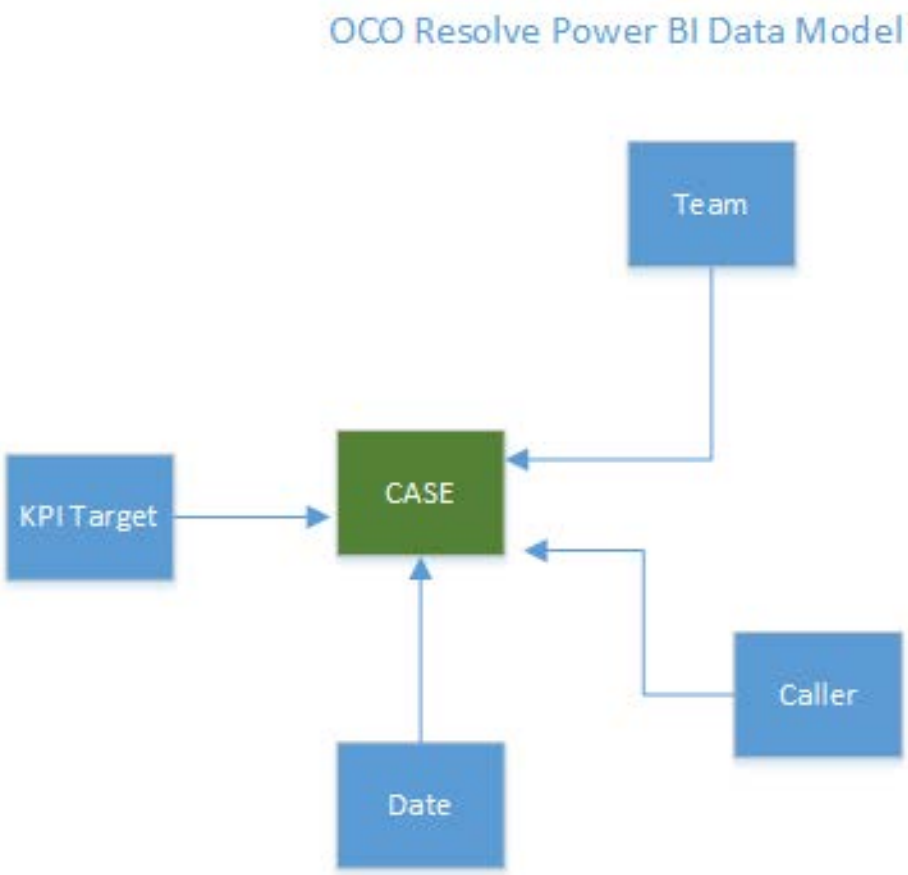

Figure 3- Power BI Resolve Data Model

Case							
The primary table for the Resolve reporting capability. Contains attributes relating to a Case in Resolve.							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
Number	CaseNumber	dbo.tblCase	Varchar	The Business key value for a Case	Non-Identifying		Resolve Database
CaseId	CaseId	dbo.tblCase	UniqueIdentifier	The System Unique key for a Case	Non-Identifying		Resolve Database
Agency of Approach	DisplayName	dbo.tblCase	Varchar	The name of the Agency of Approach	Non-Identifying		Resolve Database
Abbreviated Agency Name	SerialNo	dbo.tblCase	Varchar	The abbreviated name of the Agency of approach	Non-Identifying		Resolve Database
RespondentOrg of PHIO	DisplayName	dbo.tblCase	Varchar	The name of the PHIO Agency of approach	Non-Identifying		Resolve Database
Cases Priority	Description	dbo.tblPriority	Varchar	The Priority (for Approaches), or Level (for PHIO Cases)	Non-Identifying		Resolve Database
Owning Team	Description	dbo.tblGroup	Varchar	The name of the Owning Team for a Case	Non-Identifying		Resolve Database
Owning Team Group ID	Owning Team GroupId	dbo.tblCase	Int	The ID (Group ID) of the Owning team	Non-Identifying		Resolve Database
Jurisdiction - Case	Levels	dbo.UDFElement	Varchar	The Jurisdiction			Resolve Database
Case Type	DisplayName	dbo.CaseEntityType	Varchar	The type of case (e.g. Approach)	Non-Identifying		Resolve Database
ReceivedDate	Received Date	dbo.tblCase	DateTime	The Date and Time a case was received by the OCO	Non-Identifying		Resolve Database

ClosedDate	Closed Date	dbo.tblCase	DateTime	The data and time a case was closed	Non-Identifying		Resolve Database
HowReceived	Description	dbo.tblHowReceived	Varchar	The channel used to receive the Case (e.g. Phone , Web)	Non-Identifying		Resolve Database
Elapsed Time	N/A	dbo.tblCase	Int	The elapsed time in days between Received date and Closed Date	Non-Identifying		Calculated
ReceivedDateKey	RecievedDate	dbo.tblCase	Varchar	ReceivedDate : formatted as a Datekey for relating to the Date Dimension ; Convert(Varchar(8),ReceivedDate,112)	Non-Identifying		Resolve Database
ClosedDateKey	ClosedDate	dbo.tblCase	Varchar	ClosedDate formatted as a Datekey for relating to the Date Dimension ; Convert(Varchar(8), ClosedDate,112)	Non-Identifying		Resolve Database
LastCaseActionId	LastCaseActionid	dbo.tblCaseAction	Int	The CaseActionId for the recent CaseAction record for a case	Non-Identifying		Resolve Database
LastActionId	LastActionId	dbo.Action	Int	The ActionId for the recent CaseAction record for a case	Non-Identifying		Resolve Database
LastActionAssignedDate	AssignedDate	dbo.CaseAction	DateTime	The AssignedDate for the most recent CaseAction for a case	Non-Identifying		Resolve Database
LastActionCompletedDate	LastActionCompletedDate	dbo.CaseAction	DateTime	The CompletedDate for the most recent CaseAction for a case	Non-Identifying		Resolve Database

KPI Target							
A table to hold the KPI target values for each category/Level in Resolve.							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
Category	N/A	KPI Target	Varchar	The category for the KPI Target	Non-Identifying	This value is hard coded in a table in the Reporting Data Interface database	Resolve Database
Level	N/A	KPI Target	Varchar	The Level for the KPI Target	Non-Identifying	This value is hard coded in a table in the Reporting Data Interface database	Resolve Database
Priority Reporting Label	N/A	KPI Target	Varchar	The Label for the KPI Reporting Target	Non-Identifying	This value is hard coded in a table in the Reporting Data Interface database	Resolve Database
Standard Service Time	N/A	KPI Target	Int	The Target value for the KPI	Non-Identifying	This value is hard coded in a table in the Reporting Data Interface database	Resolve Database

Team							
A table holding the list of teams as associated in the Case OwningTeam							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
GroupId	GroupID	tblGroup	Int	The key for a Group record	Non-Identifying		Resolve Database
TeamName	Description	tblGroup	Varchar	The name of the Team as assigned to a Case	Non-Identifying	Within the scope of Resolve a "Group" is a "Team"	Resolve Database

Team							
A table holding the list of teams as associated in the Case OwningTeam							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
GroupId	GroupID	tblGroup	Int	The key for a Group record	Non-Identifying		Resolve Database
TeamName	Description	tblGroup	Varchar	The name of the Team as	Non-Identifying	Within the scope of Resolve a	Resolve Database

				assigned to a Case		"Group" is a "Team"	

Caller							
A table holding the required properties of a Caller (De-Identified)							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
CaseId	CaseId	tblCase	Int	The key used to relate the location to the case	Non-Identifying		Resolve Database
City	City	tblPersonAddress	Varchar	The name of the suburb / city where a Caller is located	Non-Identifying	The City field is part of a composite address of a caller. However, the other elements of an address are explicitly not available in the solution. (eg. Street address, Street Number etc.) Refer to the ICT Business Intelligence Capability Architecture for details.	Resolve Database
Postcode	Postcode	tblPersonAddress	Varchar	The postcode where the Caller is located	Non-Identifying	The Postcode field is part of a composite address of a caller. However, the other elements of an address are explicitly not available in the solution. (eg. Street address, Street Number etc.) Refer to the ICT Business Intelligence Capability Architecture for details.	Resolve Database

State	State	tblPersonAddress	Varchar	The State where the Caller is located	Non-Identifying	The State field is part of a composite address of a caller. However, the other elements of an address are explicitly not available in the solution. (eg. Street address, Street Number etc.) Refer to the ICT Business Intelligence Capability Architecture for details.	Resolve Database
Country	N/A	N/A	Varchar	The Country where the Caller is location	Non-Identifying	The Country field is part of a composite address of a caller. However, the other elements of an address are explicitly not available in the solution. (eg. Street address, Street Number etc.) Refer to the ICT Business Intelligence Capability Architecture for details. The majority of complainants are located in Australia, however roughly 1.2 % are located outside Australia.	Resolve Database
ATSI	ATSI	tblUDFValue	Varchar	The Aboriginal Torres Strait Islander value for the Caller	Non-Identifying	ATSI (Aboriginal Torres Strait Islander)	Resolve Database

Date							

A table holding various date related values for reporting purposes							
Attribute Name	**Field Name**	**Table Name**	**Data type**	**Description**	**Identifying Category**	**Remarks**	**Attribute Source**
DateKey	N/A	N/A	VarChar		Non-Identifying		Resolve Database
DayDate	DayDate	tblDates	DateTime	Natural Key value for the Table. Datetime with Time component set to 00:00 (Midnight)	Non-Identifying		Resolve Database
MonthDay	MonthDay	tblDates	Int	The numerical day of the month for the date	Non-Identifying		Resolve Database
MonthName	MonthName	tblDates	VarChar	The name of the month of the date	Non-Identifying		Resolve Database
MonthShortName	MonthShortName	tblDates	VarChar	The Short name of the month of the date	Non-Identifying		Resolve Database
CalendarYear	CalendarYear	tblDates	Int	The Year of the Date	Non-Identifying		Resolve Database
CalendarMonth	CalendarMonth	tblDates	Int	The numerical month number of the date	Non-Identifying		Resolve Database
CalendarQuarter	CalendarQuarter	tblDates	int	The numerical quarter number of the date	Non-Identifying		Resolve Database
MonthDate	MonthDate	tblDates	DateTime	The first date of the month in which the date falls	Non-Identifying		Resolve Database
QuarterDate	QuarterDate	tblDates	DateTime	The first date of the quarter in which the date falls	Non-Identifying		Resolve Database
DatesId	DatesId	tblDates	Int	The surrogate key for the date	Non-Identifying		Resolve Database
FiscalYear	N/A	N/A	VarChar	The fiscal year in which the date falls	Non-Identifying		Calculated
DayofWeek	N/A	N/A	Varchar	The name of the day of the week of the date	Non-Identifying		Calculated