

5.1 Business motivation model

The business motivation for identity management is clearly articulated in the *Strategic Plan for Identity Management in DIAC 2007–2010*, which describes the reasons why we need to change the way identity is managed in the department.

The **business motivation model*** validates the vision and goals specified in the *Strategic Plan for Identity Management in DIAC 2007–2010* by aligning external drivers and key business problems and opportunities to business strategies, tactics, goals and objectives. The business motivation model defines explicit linkages between the strategies, goals and objectives to the various components and aspects of the IBRM.

Tactics and projects are then developed and initiated to incrementally introduce improved identity management practices that are aligned with the IBRM. This approach ensures the effective prioritisation of resources and that Identity Branch projects and other initiatives are contributing towards the realisation of the key outcomes expressed in the strategic plan.

Figure 3 provides one view of the IBRM business motivation model. It illustrates how specific tactics stated in the strategic plan relate to the IBRM business processes.

Figure 4 illustrates another view, which shows how the business motivation model provides the linkages from the 'receipt stated identity' process all the way through to the vision for identity management in DIAC.

The motivation model is a key element of the IBRM and it is used as follows:

- to develop other elements of the IBRM
- to provide traceability back to the business benefits that are anticipated from implementation of the IBRM.

* Based upon the Business Rules Group (2007) *The Business Motivation Model release 1.3* (online) <http://www.businessrulesgroup.org>

Figure 3 - Identity management tactics mapped to the IBRM business processes

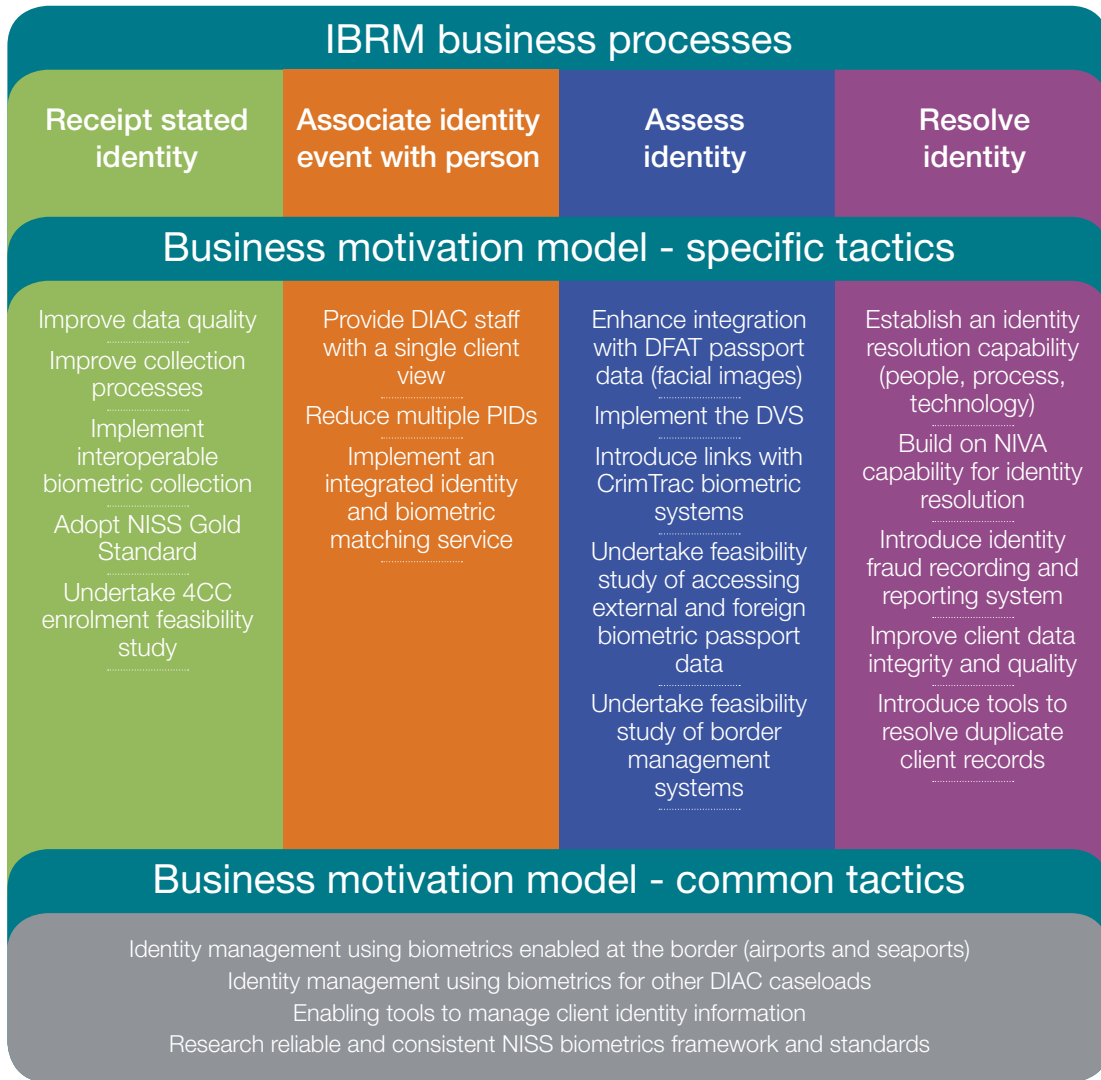
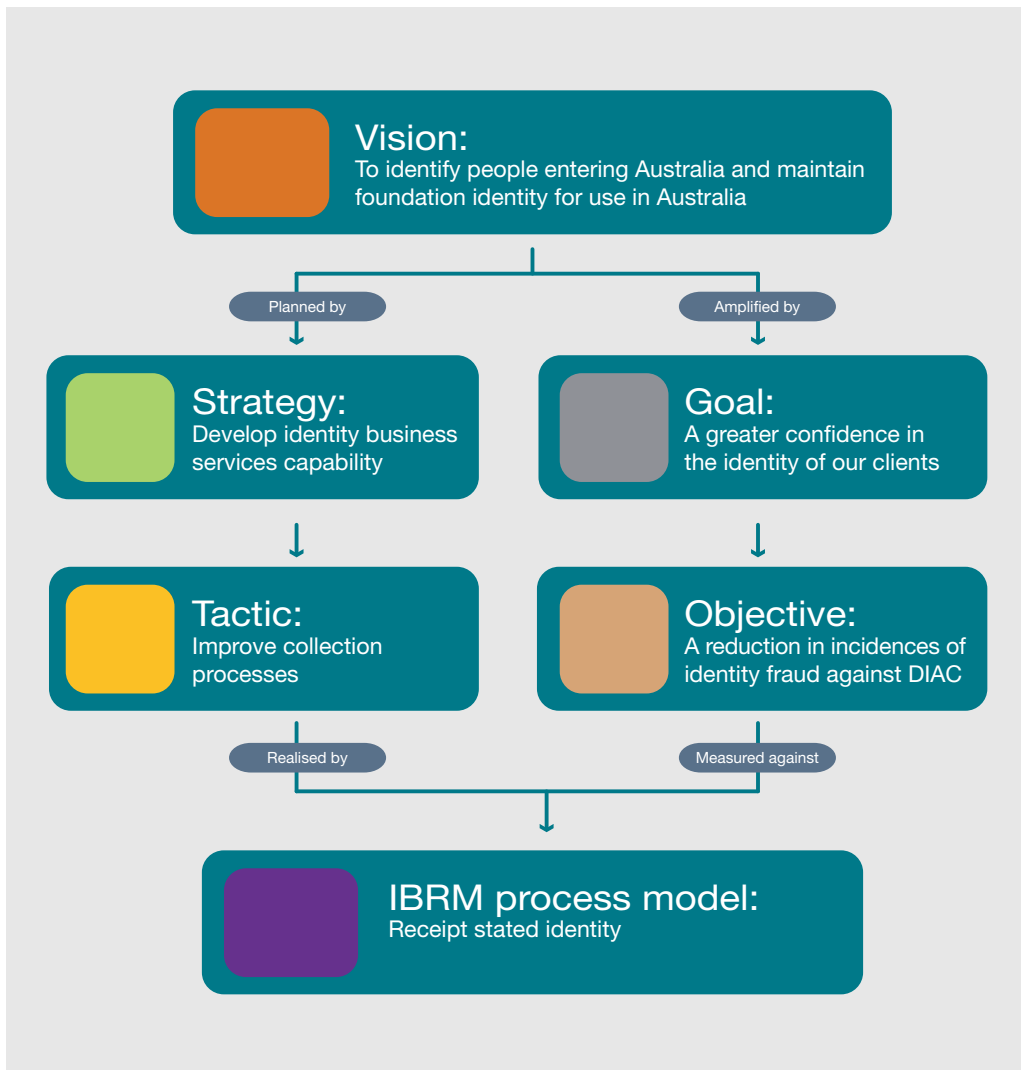


Figure 4 - Example of motivation model mapping to the 'receipt stated identity process'



5.2 Business process model

The **business process model** describes business processes specific to identity management and how they fit within the broader departmental business processes. It aims to create a standardised approach to identity management across the department.

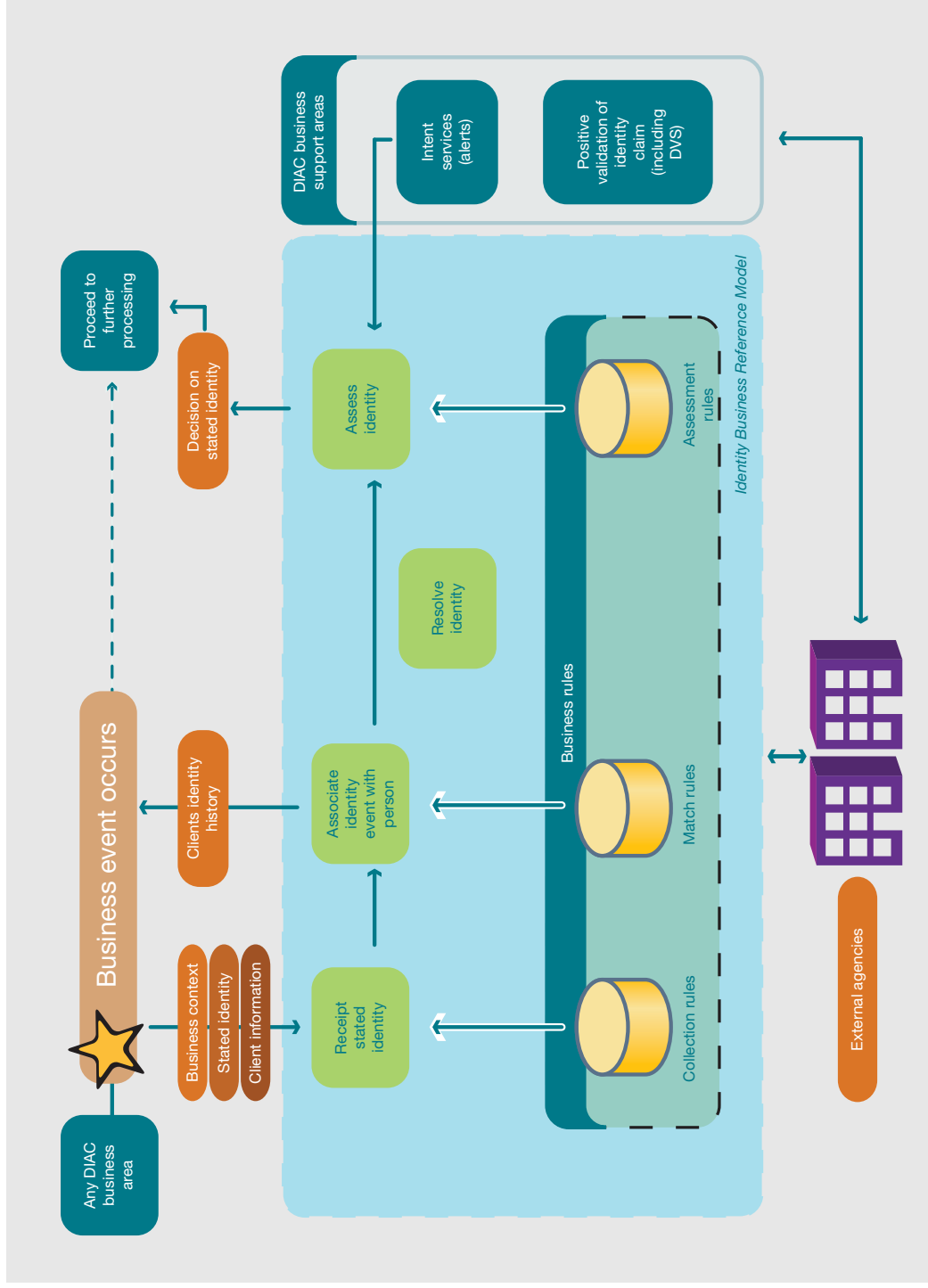
The model provides for a clear separation of identity management processes from other business processes, which differs significantly to the existing situation. At present, the recording of a client's identity information is piecemeal and interspersed throughout other processes, such as assessing a visa application.

Separating identity management processes from other business processes enables assessment of a client's stated identity to be undertaken as early as possible in a client's interactions with the department, which provides the potential to reduce costs to the department and improve client service. If a client's identity can be assessed up front and an earlier decision made on their identity, this could lead to an early decision that further resource intensive processes do not need to be undertaken.

Notwithstanding the above, the business process model allows for the flexibility to incrementally complete the identity management processes over an extended time period where necessary, for example in the business context of compliance and detention services.

The IBRM is predominantly presented in the context of the business process model. That is, a document has been produced for each identity management business process illustrated in Figure 5. Each document describes the business process along with events, locations, organisation aspects and roles specific to that process.

Figure 5 – Identity management business processes



Receipt stated identity

The **receipt stated identity** process involves recording the information and undertaking preliminary checks to ensure the information is complete, accurate and conforms to the department's identity and information management policies and associated standards.

The amount of information receipted at each identity event will vary depending on the business context and the associated risks.

The business rules for the collection of identity information will ensure the consistency of what is collected within specific business contexts, as well as across other departmental programs. They will also make sure that the information elements are captured and stored using consistent formats and are of an appropriate quality.

The IBRM **information model** illustrates and defines the full set of information that can be collected during the 'receipt stated identity' process. The business context is used to determine which of these information elements are collected during a business transaction. These include:

- stated identity
 - * biographical information
 - * proof-of-identity documents – eg passports and national identity cards
 - * physical features and characteristics
 - * biometric identifiers
 - » signature images
 - » fingerprint images
 - » facial images
 - * relationships between the person who is the subject of the stated identity and other people, for example mother, spouse, or travel companion
- client information
 - * statement on previous visits to Australia and other transactions with the department
 - * contact details – this can include phone numbers, email addresses, physical addresses and postal addresses
 - * evidence of social footprint – documents that confirm a client's contact details, for example phone bills, electricity bills and rates notices
 - * client knowledge – a series of questions and the answers provided by the client.

Associate identity event with person

The **associate identity event with person** process involves:

- Checking existing client records against the information provided during the **receipt stated identity** process and, if matches with existing client records are found, deciding which client record to associate with the **identity event**. These additional checks will be undertaken regardless of searches that might have been carried out prior to the invocation of the identity management business process. The checks will be mandatory and automated, therefore removing the reliance on end-users to initiate consistent and thorough checks of existing records before creating a new client record. Pre-defined match rules will determine what constitutes a confirmed match, a potential match, or a non match. The rules may also determine when an information notification or action referral needs to be passed to interested parties, such as the Identity Resolution Centre.
- Determining whether or not a new client record needs to be created. In some business transactions, this process might require the involvement of end-users in order to make a determination, especially where the result is more than one potential match. Where the end-user cannot determine which is a confirmed match, the identity event may be escalated to the Identity Resolution Centre (IRC). In the case of an Electronic Travel Authority (ETA) this process might be fully automated, based on rules specific to the ETA business context.
- Adding the **identity event** to a particular client's **identity history**. A client's identity history is made up of a collection of identity events as described in section 4.3.

Assess identity

The **assess identity** process is driven by predefined business rules that determine the identity assessment activities that will apply for a given business transaction. This rules-driven approach provides the flexibility to change the way a stated identity is assessed, depending on the business context, or as new identity risks are identified and as additional identity assessment activities are developed. Activities undertaken as part of assessing a stated identity could include:

- positive validation of elements of the stated identity or client information, for example, checking that a proof-of-identity document is genuine, or checking that an address is a valid address
- checks against identity related alerts, for example, checking to see whether or not a passport is on a lost and stolen passports list
- collection of additional information, in which case the process becomes iterative, invoking the **receipt stated identity** process again

The activities undertaken to assess the stated identity may be automated or manual. They might also be referred for action by a number of different DIAC officers, or even by third parties. The way a stated identity is assessed might also depend on issues that arise in a specific case, which could require arbitrary assessment activities to be undertaken.

The outcome of the **assess identity** process can be one of two states, that is, the decision-maker is satisfied as to the stated identity or not satisfied.

It is important to note that because a stated identity is assessed as 'satisfied', it does not necessarily mean the department is one hundred per cent certain the client is who they say they are. It means the decision maker has reached a level of confidence acceptable to the business context and risk of the business transaction. Where a biometric identifier has been provided as part of the stated identity, it will also mean that the stated identity is anchored via a biometric, hence making it easier to match with the appropriate client record the next time the client interacts with the department.

The decision on the stated identity is then considered along with all relevant factors applicable to the business context, to make decisions on further processing, such as whether or not to grant a visa or citizenship.

Resolve identity

In most cases, it is expected that DIAC officers will have the tools and skills necessary to 'resolve' a client's identity during the **assess identity** process. However, an escalation path will be available for identity resolution if DIAC officers require expert advice in the field of document examination, fingerprint and facial recognition, or where they are unable to determine whether or not an existing client record is for the person they are dealing with. In these cases, the identity event will be referred to the Identity Resolution Centre (IRC).

The IRC will provide timely, accurate and sustainable (legally and ethically) recommendations to decision-makers. However, the decision-maker will still be responsible for deciding whether they are satisfied about the stated identity given the business transaction between the client and the department.

Where suspected identity fraud is detected during the identity resolution process, it will be recorded against the **identity event** and the associated client record by the DIAC officer who responds to the identity resolution referral.

A suspected fraud case will be referred to the fraud investigations area for appropriate follow-up action where required and all interested parties will be advised. The outcome of the investigation will also be recorded, so that if the suspicion proves to be unfounded, there is no negative inference made regarding the client in the future.

Centralised and consistent identity fraud reporting will contribute to the establishment of a general deterrent to identity fraud through prosecution action and censure.

As part of the identity resolution process, tools will be used to detect and correct where appropriate, poor quality data. Duplicate client records will be detected and resolved using a 'just in time' approach to support operational demand.

Rather than merging records, the identity history of each duplicate record will be linked to form a single, more complete identity history. In the case where an existing client record needs to be split, a new client record will be created and relevant identity events linked to the appropriate client records.

5.3 Business events model

The **business events model** identifies the departmental business events that initiate identity management processes. It defines when identity management takes place within other business processes such as visa application, detention and compliance processing.

Specific business events trigger the identity management processes:

- **receipt stated identity**
- **associate identity event to person**
- **assess identity**
- **resolve identity**

Business events are formally specified in the respective documents that describe each of these processes.

The most significant business events are those that trigger the **receipt stated identity** process, as illustrated by the star in Figure 5. These business events are determined based on the risk to the department of not correctly identifying a person during a specific interaction.

It is important that each business area works with Identity Branch to determine what these events are and to formally define them. The level of granularity of these events and their relevance to identity risks are also very important. An identity event is created each time these business events occur and it is added to a client's identity history. Inappropriate identity events could obscure the important details of a client's identity history, making it difficult for decision makers to determine someone's real identity.

Appendix C provides some examples of business events that trigger the **receipt stated identity** process.

Business events that trigger the other identity management processes 'associate identity event with person', 'assess identity' and 'resolve identity', predominantly result from the completion of a previous identity management process. However, this might not always be the case. For example, the department could receive a request from an external agency to confirm whether a client is who they claim to be. In this situation an external business event could trigger the **assess identity** process directly.

5.4 Location model

The **receipt stated identity** event can occur in any of the locations identified below (as at 1 May 2008):

- Offshore at any of the following locations:
 - * Sixty-nine offshore posts – with one hundred and thirty-seven Australian-based DIAC staff and over nine hundred and fifty locally engaged employees
- Onshore at any of the following locations:
 - * Eleven regional offices (Darwin, Cairns, Brisbane, Gold Coast, Sydney CBD, Parramatta, ACTRO, Melbourne, Dandenong, Adelaide and Perth)
 - * Five processing centres (Sydney, ACT, Hobart, Adelaide and Perth)
 - * Eight Detention and Residential Housing Centres
 - » Maribyrnong Immigration Detention Centre (MIDC) (Melbourne)
 - » Villawood Immigration Detention Centre (VIDC) (Sydney)
 - » Sydney Immigration Residential Housing (SIRH)
 - » Perth Immigration Detention Centre (PIDC)
 - » Perth Immigration Residential Housing (PIRH)
 - » Darwin Immigration Detention Centre (DIDC)
 - » Brisbane Immigration Transit Accommodation (BITA)
 - » Christmas Island Immigration Detention Centre (CIDC)

There are also many geographical locations, both onshore and offshore, where third parties operate on behalf of the department. Geographical locations where identity information is collected are an important aspect of the IBRM because:

- the physical security aspects of each location where identity information is receipted are relevant when determining the identity related risk and consequently, what identity information should be collected and how to assess it.
- the physical infrastructure capacity at each DIAC location needs to be considered as new identity management processes are introduced, with a view to identifying the changes that might be required at each site – eg are the rooms equipped adequately for the collection of biometrics?
- geographical location needs to be considered in combination with the business process model, information model and role model to
 - * assist in planning for staff impact – eg training required at each location
 - * determine the system and network performance and availability requirements at specific locations

Individual business areas should consider locations for which they have responsibility and determine the impact of the adoption of improved identity management practices at each. This activity will be part of the risk assessment and change management activities described in section 4.5.

For example, if fingerprint and facial images are to be captured live with cameras or scanning devices, there will be specific requirements for the physical locations and infrastructure at those locations. These requirements are (or will be) detailed in the following departmental standards:

- *DIAC Standard for Facial Images* is the departmental standard for the processes and data formats for capturing facial images and information relating to the images.
- *DIAC Standard for Fingerprint Images* is the departmental standard for the processes and data formats for capturing fingerprint images.

In addition to the above, the location where the stated identity is receipted will have implications for the identity risk assessment, which might identify additional risk treatments to be applied during the **assess identity** process. The following table is provided to assist in determining identity risks associated with geographical locations.

	In Australia	Offshore
Managed by Australian Government	<ul style="list-style-type: none"> • DIAC state and territory officers in Australia • Australian international airports • Australian seaports 	<ul style="list-style-type: none"> • Offshore posts – Australian High Commissions, Embassies and Consulates-General.
Managed by a trusted third party (subject to Australian physical security standards)	<ul style="list-style-type: none"> • Detention and Residential Housing Centres 	<ul style="list-style-type: none"> • Christmas Island Immigration Detention Centre
Not subject to Australian physical security standards	<ul style="list-style-type: none"> • HSA doctors' practices • In the field anywhere • Migration agents' offices • Any location that has internet connectivity 	<ul style="list-style-type: none"> • International airports • International seaports • IELTS testing centres • Panel doctor practices • Refugee camps • Migration agents' offices • Any location that has internet connectivity

5.5 Organisation and role model

The **organisation model** describes the organisational aspects of the IBRM, identifying where organisational changes are required as the model is adopted.

For example, the **resolve identity** process requires a new organisational unit, the IRC and changes to business processes in existing organisational units, such as National Identity Verification and Advice unit (NIVA) and the Border Operations Centre (BOC), to leverage from the skills that will be available in the IRC.

The identity business intelligence analytics services will also require changes in the roles of existing organisational areas, or perhaps a new organisational unit will need to be established.

The organisation and role model also describe the roles people will fulfil when undertaking identity management processes. They assist in identifying where new skills and training are required. Identity management roles are formally specified in the respective documents that describe each of the identity management business processes.

In particular, improved identity management practices will require some DIAC staff and third parties operating on behalf of the department, to have the skills necessary to capture facial images and fingerprints of the quality required to undertake biometric matching. Identity Branch will develop and deliver the training necessary so that business areas can undertake these activities as required.

As each business area adopts the IBRM, they will need to consider the roles of staff in their business area and which of these roles will take on identity management responsibility and therefore the identity management roles defined for each IBRM process. In some cases, this will not be limited to DIAC staff, but can also include third parties and clients.

The identity management role will need to be aligned or cross-referenced with the DIAC roles being defined by the DIAC Enterprise Architecture team and appropriate access controls to identity management systems functionality put in place.

5.6 Information model

The **information model** describes the information that needs to be available when identity management business processes are being conducted. The model includes the information elements that we wish to store and refer to over time.

The information model is an important component of the IBRM. In particular, it is a key mechanism for achieving the following outcomes of the identity management strategy:

- a greater confidence in the identity of our clients
- improved and consolidated identity information that is readily accessible to decision makers.

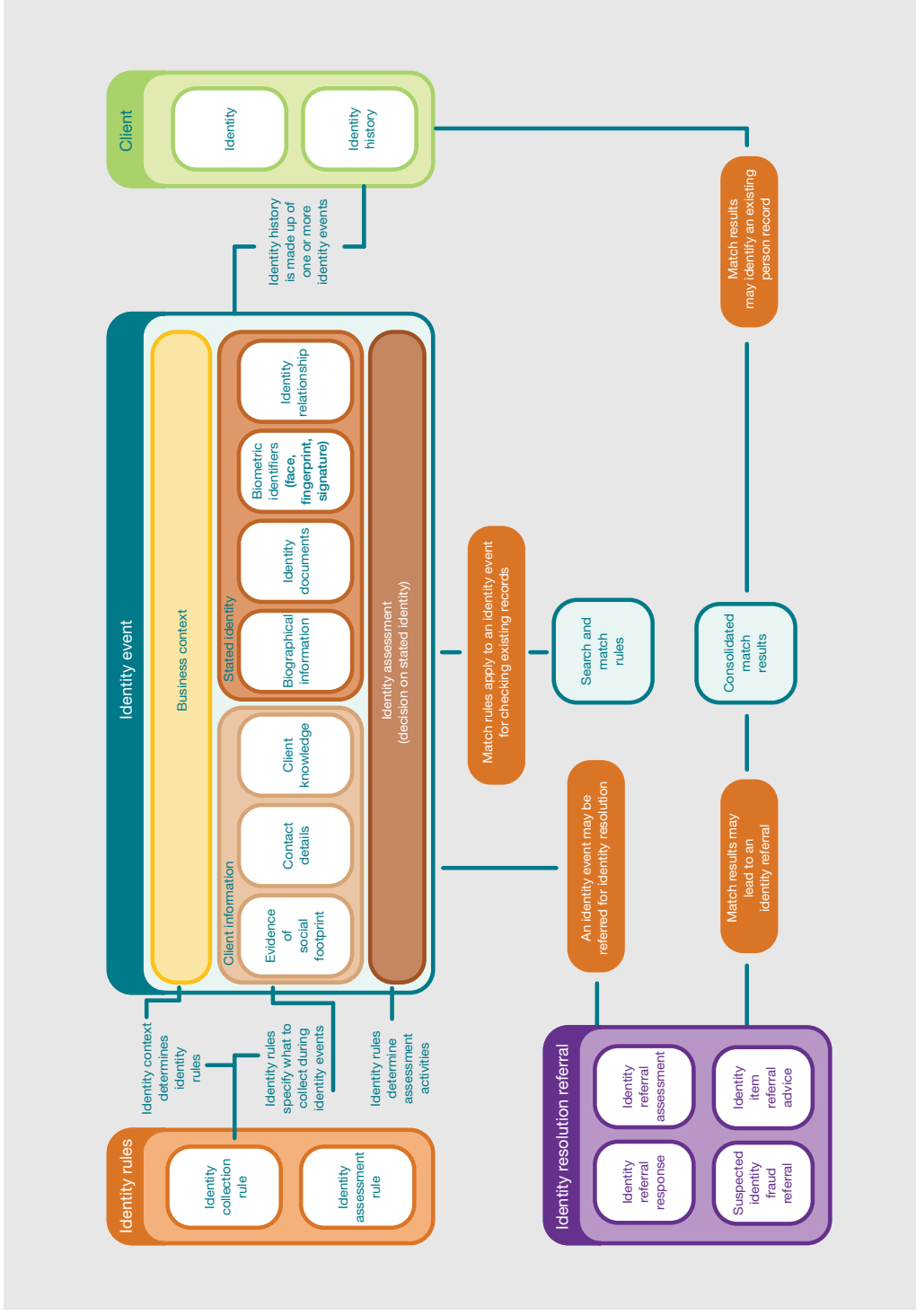
The IBRM does not mandate which information elements are to be collected by different business areas. It does, however, mandate the specific standards (definitions, rules and formats) that must be adhered to when identity information is collected.

Figure 6 illustrates the key information elements that make up the IBRM. As can be seen in the diagram, identity specific rules determine which information elements are collected during an identity event, as well as what identity assessment activities are undertaken. The **identity event** is information rich. It contains all the information required to decide whether or not to be satisfied as to a client's stated identity. A client's **identity history** is also information rich, containing all known identity events for a client.

The Identity Resolution Centre supports the escalation of identity events, particularly cases where multiple duplicate records exist that cannot be resolved during standard operational processing.

More details and the definition for each element, are contained in a separate document, the **IBRM information model**.

Figure 6 - Executive view of the IBRM information model



Appendix A - Related Documents

Title
<p>The IBRM Preamble document describes the approach and methodology being used to develop the Identity Business Reference Model.</p>
<p>The IBRM Business Motivation Model describes the rationale for the design of the model and its various components. It links strategies and goals defined in the <i>Strategic Plan for Identity Management in DIAC 2007–2010</i> with elements of the IBRM, as well as activities, tactics and projects that will be undertaken to deliver the outcomes of the strategic plan.</p>
<p>IBRM – Receipt Stated Identity Model describes the process, information, events, roles, organisational aspects and geographical considerations related to receipting a stated identity.</p>
<p>IBRM – Associate Identity Event with Person Model describes the process, information, events, roles, organisational aspects and geographical considerations related to adding an Identity Event.</p>
<p>IBRM – Assess Identity Model describes the process, information, events, roles, organisational aspects and geographical considerations related to assessing a stated identity.</p>
<p>IBRM – Resolve Identity Model describes the process, information, events, roles, organisational aspects and geographical considerations related to resolving identities.</p>
<p>IBRM – Information Model describes the information elements used or created during identity management processes.</p>
<p>DIAC Standard for Facial Images describes the departmental standard for the processes and data formats for capturing facial images and information relating to the images.</p>
<p>DIAC Standard for Fingerprint Images describes the departmental standard for the processes and data formats for capturing fingerprint images.</p>

Appendix B – Example of a business context for the General Skilled Migration program

Business Context Element	Example	Description
Business Program	General Skilled Migration	The DIAC business program relevant to the business transaction
Primary Business Process	Class BN – Skilled Independent	The primary business process within the DIAC business program
Business Event	Receipt Visa Application	The business event that determines when the ‘receipt stated identity’ process takes place within the context of other business processes such as visa application, detention and compliance processing This triggers the receipt stated identity process
Client Role	Primary Applicant	The role of the person who the stated identity applies to. Other roles could be detainee, passenger or secondary applicant
Process Channel	Electronic – Internet	The mechanism by which the stated identity is provided to the department. Other examples include: manual – over the counter manual – via mail electronic – via phone
External Reference	Visa receipt number: 987654	An external reference that is used to ensure the ‘receipt stated identity’ transaction can be cross-referenced to the broader business process
Source Person ID	Mara 543210	Something that identifies who supplied the stated identity to the department If the identity information is receipted directly by a DIAC officer, this could be the user id of that officer Note: this may not always be applicable or available

Business Context Element	Example	Description
Source Org	ACME Migration Agent Co	If applicable, the name of organisation the source person represents
Source Location	Rajasthan, India	Geographical location where the stated identity was received
Date & Time	16/07/2007: 09:30:00	The date and time the business event occurred. That is the date and time the identity information is received
Person Identifier:	ICSE Id 1234	<p>Where the business process that precedes the receipt stated identity has reason to believe the client is a known client, a unique identifier for that client should also be provided. TRIPS Person Identification number (PID) and ICSE Client Identification number (CID) are examples, however in the future state it will be desirable that there will be one PID consistently used across the department.</p> <p>While the stated identity would not be linked to the known client at this stage, the fact that the person may already be known to the department may change the rules related to the identity collection set. It may also change search rules in the subsequent 'check for existing person' process</p>

Appendix C – Examples of business events that trigger the receipt stated identity process

The following table includes examples of business events that trigger the **receipt stated identity** process. These are by no means exhaustive. The **receipt stated identity** model includes additional events and it is envisaged that the business events will change and mature over time as more business areas adopt the Identity Business Reference Model in their operational processing.

Identity Management Continuum	Event name	Event description
Visa Processing	Receipt of a visa application	The receipt of a visa application is being recorded by the department.
	Receipt of a health assessment outcome	The department receives the outcome of a health assessment for a client
	Receipt of English language test outcome	The department receives the outcome of an English language test for a client
Border Processing	Traveller referred to secondary line on entry to Australia	Potential client of concern referred by Australian Customs Service (ACS) to DIAC officers for verification
Compliance Processing	Receipt of client's identity information by a compliance officer in the field	Compliance officer interviews a suspected unlawful non citizen (UNC) during a field operation and collects identity items to establish identity
	Receipt of detainee's identity information by a GSL officer	DIAC compliance officer presents the unlawful citizen to a GSL officer. GSL officer receipts detainee's identity information
		ACS officer presents the Illegal Foreign Fisher to a GSL officer GSL officer receipts Illegal Foreign Fisher's identity information
Citizenship Processing	Receipt of a citizenship application	The receipt of citizenship application is being recorded by the department
	Receipt of a citizenship test results for a client	The department receives the outcome of an citizenship test for a client

Appendix D – Glossary

Assess Identity	<p>A process model component of the IBRM which determines the identity assessment activities that will apply for a given business transaction. It also includes making a decision as to whether a stated identity actually is who the client claims to be.</p>
Associate Identity Event with Person	<p>A process model component of the IBRM which describes checking existing client records against information provided during the receipting of the identity. It also describes deciding which client records to associate with the identity event or determining whether or not a new client record needs to be created and adding the identity event to a particular client's identity history.</p>
Business Architecture	<p>Describes the future state business model for a business program. Does not focus on technology, but on core business components such as business motivation, business processes, information, locations, roles and business events.</p>
Business Context	<p>The nature of a transaction between a person and the department. It identifies the business interaction in which an identity event takes place and includes the business program.</p>
Business Motivation Model	<p>Validates the vision and goals specified in the Strategic Plan for Identity Management in DIAC 2007–2010.</p>
Business Process Model	<p>Identifies and describes the work-flows and processes related to identity management</p>
Business Rules	<p>The rules on how DIAC will conduct its business.</p>
Client Information	<p>Any additional information provided as evidence to support a stated identity.</p>
Collection Rules	<p>The identity business rules for collection of information forming the stated identity and driven by the business context of the client transaction.</p>

DIAC Change Management Framework (CMF)	<p>A change management framework which ensures that key impacts of changes are considered and documented prior to implementation and that a senior responsible officer must be identified and accountable for the outcomes of every major change.</p> <p>All new initiatives and policy changes must refer to the CMF Guidelines and comply with any mandatory requirements.</p>
DIAC Risk Management Framework	A methodology, suite of tools and a governance process for effecting change in the department based on risk.
DIAC Standard for Facial Images	Describes the departmental standard for the processes and data formats for capturing facial images and information relating to the images.
DIAC Standard for Fingerprint Images	Describes the departmental standard for the processes and data formats for capturing fingerprint images.
Event Model	Identifies and describes the broader departmental business events that initiate identity management processes.
Identity Assessment Rule	A type of identity risk treatment rule that defines an activity performed to assess the validity of a stated identity and the client information. Identity assessment rules apply in a given identity event.
Identity Business Reference Model	The DIAC business model for identity management which transforms current identity management processes to provide capability for standardised identity management practices across DIAC.
Identity Events	Encompasses all aspects of collection and assessment of a stated identity within a particular business context.
Identity History	The complete collection of identity events for a given person. Each identity event includes the business context, stated identities, client information and related assessment outcomes for the event.
Identity Resolution Centre	A capability that will provide timely, accurate and sustainable recommendations to decision makers in regards to identity.

Identity Risk Assessments	An activity undertaken with DIAC business areas to determine the possible identity fraud risks involved in that business context.
Information Model	Identifies and describes the key information elements required to undertake identity management specific business processes.
Locations Model	Outlines the geographic locations where identity management business processes are physically performed.
Match Rules	Define: <ul style="list-style-type: none"> • what constitutes an exact match • what constitutes a possible match • what constitutes no match.
Organisation and Roles Model	Identifies and describes the organisational aspects and roles of people involved in identity management within the department.
Receipt Stated Identity	A process model component of the IBRM which describes recording information and preliminary checks to ensure information is complete, accurate and conforms to the department's identity and information management policies and associated standards.
Resolve Identity	A process model component of the IBRM which describes specialist identity resolution processes such as legal, policy, finger print and facial specialists.
Stated Identity	A claim made by a person that they hold a particular identity.
Strategic Plan for Identity Management in DIAC 2007-2010	Represents a statement of the vision for the management of client identity as an integrated DIAC business function.

