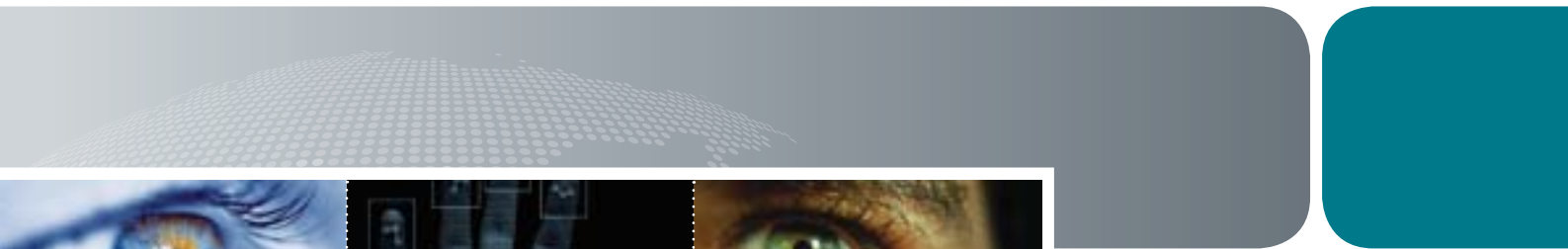




**Australian Government**  
**Department of Immigration  
and Citizenship**

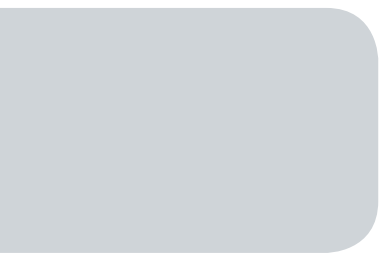
# Identity Business Reference Model (IBRM)

Executive Report



# Contents

Abbreviations . . . . .	3
1 Introduction . . . . .	4
1.1 Purpose of this document . . . . .	4
1.2 Related documents . . . . .	4
1.3 Audience . . . . .	6
1.4 Structure of this document . . . . .	6
2 Goals of the Identity Business Reference Model . . . . .	7
3 Approach for adoption of the Identity Business Reference Model . . . . .	9
4 Overview of the Identity Business Reference Model . . . . .	12
4.1 Business context . . . . .	13
4.2 Business rules . . . . .	14
4.3 Identity events and identity history . . . . .	15
4.4 Identity business intelligence analytic service . . . . .	15
4.5 Identity risk assessments and change management . . . . .	16
5 Identity Business Reference Model . . . . .	19
5.1 Business motivation model . . . . .	20
5.2 Business process model . . . . .	23
5.3 Business events model . . . . .	28
5.4 Location model . . . . .	29
5.5 Organisation and role model . . . . .	31
5.6 Information model . . . . .	32
Appendix A - Related Documents . . . . .	34
Appendix B - Example of a business context for the General Skilled Migration program . . . . .	35
Appendix C - Examples of business events that trigger the receipt stated identity process . . . . .	37
Appendix D - Glossary . . . . .	38



## Abbreviations

CMF	Change Management Framework
DFAT	Department of Foreign Affairs and Trade
DVS	Document Verification Service
ETA	Electronic Travel Authority
HSA	Health Services Australia
IBRM	Identity Business Reference Model
ICSE	Integrated Client Service Environment System
IELTS	International English Language Testing System
IRC	Identity Resolution Centre
IT	Information Technology
NISS	National Identity Security Strategy
NIVA	National Identity Verification and Advice
PAM	Procedure Advice Manual
PID	Person Identification Digit
TRIPS	Travel and Immigration Processing System
4CC	Four Countries Conference

# 1 Introduction

## 1.1 Purpose of this document

This document provides an executive report on the Department of Immigration and Citizenship's (DIAC) Identity Business Reference Model (IBRM), which is a key tool for implementing standardised identity management practices across the department.

Importantly, this document highlights the need for Identity Branch and all other business areas of the department to align their plans for change to business processes and new systems capability to ensure the successful adoption of improved identity management practices.

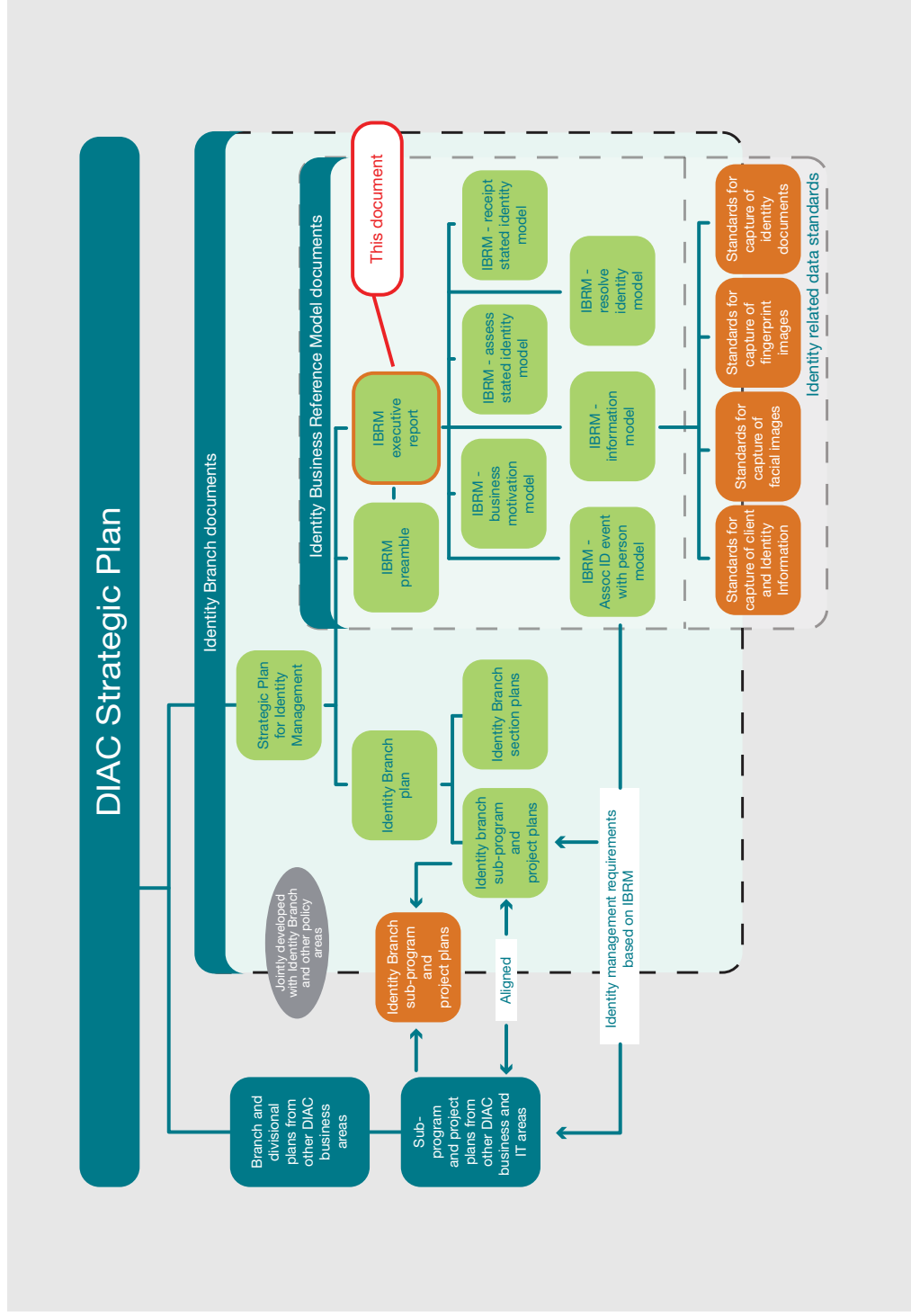
## 1.2 Related documents

The *Strategic Plan for Identity Management in DIAC 2007–2010* is recommended as prerequisite reading.

The full suite of documents that make up the DIAC IBRM are illustrated in Figure 1. The relationship of these documents to Identity Branch planning documents, as well as planning documents across the department, is also illustrated. A description for each of the IBRM documents is provided at Appendix A.

References to individual documents are identified where relevant in the subsequent sections of this document.

Figure 1 - Relationship of IBRM documents to other documents produced by the department



## 1.3 Audience

The primary audience for this document is executive managers, business area managers and IT systems officers in the department. The document will also be accessed by external parties.

The document aims to inform readers about:

- the future state business model for improved identity management practices across the department
- the organisational change required to adopt improved identity management practices
- the need for all business areas to include initiatives and requirements in their branch, section and information technology project plans to ensure the consistent and effective implementation of improved identity management practices in their business areas
- a risk based approach for the progressive implementation of improved identity management practices across the department.

## 1.4 Structure of this document

Section 2 of this document describes the goals of the IBRM, as well as the model's relationship with the *Strategic Plan for Identity Management in DIAC 2007–2010*. Section 3 describes the approach by which business areas can adopt the IBRM. Section 4 provides a brief overview of the model and how it will relate to other business processes across the department. It introduces new concepts and terminology specific to identity management, which will be made clearer in subsequent sections. Section 5 describes the IBRM in more detail and explains the processes, information, events, organisation, roles and geographical locations related to identity management across the department.

## 2 Goals of the Identity Business Reference Model

The IBRM forms the foundation of the business of identity management in the department. The primary goal of the IBRM is to drive the implementation of new and improved identity management practices in the department that will enable the outcomes stated in the *Strategic Plan for Identity Management in DIAC 2007–2010* to be met. These are:

- a greater confidence in the identity of our clients
- improved and consolidated identity information that is readily accessible to decision makers
- an increased capacity to detect fraudulent identities
- strengthened client identity resolution through the implementation of identity resolution services
- an effective legislative framework to facilitate the introduction of improved identity management, supported by biometric technologies.

The IBRM provides a framework to deliver these outcomes by defining a consistent, logical, effective and efficient business model that can be used to:

- link identity management policy, procedures and technological solutions to the vision and goals defined in the Strategic Plan for Identity Management in DIAC 2007–2010
- standardise identity management processes across the department
- standardise the information that is collected and used to assess a client's stated identity at key interactions with the department
- inform the technological future state
- form part of a broader DIAC business architecture.

A variety of new technologies will be required to successfully deliver the IBRM into the department's operational environment. Sophisticated name and data matching tools and the suite of biometric matching tools will need to be integrated with other IT services. A robust, reliable and integrated technology solution will be required to support the improved identity management practices the IBRM aims to deliver.

The outcome for successful implementation of the IBRM across the department will be that all business areas will have a greater degree of confidence in the identity of the clients they are dealing with, particularly where there are repeat encounters with the same client.

In addition, initial investments for standardising and enhancing the way identity information is recorded and assessed during the department's initial dealings with a client, will mean reductions in cost and effort on subsequent interactions. In particular, where a biometric identifier is available to verify a client's identity on subsequent interactions, the need to repeatedly collect the same information can be significantly reduced. This will result in cost savings to the department and will also provide significant benefits to many of our clients who have multiple interactions with the department. Once their identity has been established and anchored by a biometric, they will no longer be required to provide copious amounts of information every time they deal with the department.

It is very important that managers of operational areas and their staff have a clear understanding of the *Strategic Plan for Identity Management in DIAC 2007–2010*, the IBRM and the relationship between these and the work of their areas. In order to achieve the desired outcomes stated in the *Strategic Plan for Identity Management in DIAC 2007–2010*, it is critical that all DIAC business and IT areas work together to:

- plan and prioritise new initiatives and projects
- ensure progressive alignment of identity management processes with the IBRM across all DIAC programs
- ensure that business areas are adequately funded and supported to implement the necessary changes.

The IBRM also provides a mechanism to assist us to identify the gaps between our current identity management capability and the desired future state and thus to determine an approach for transitioning from the current identity management capability to the desired future state.

### 3 Approach for adoption of the Identity Business Reference Model

It would be desirable for the IBRM to be adopted as soon as possible and as broadly as possible. However, legislative, time and resource constraints will restrict how soon and how broadly the IBRM can be adopted. In addition, program targets and potential business impacts on processing times from standardising identity management processes across the department, need to be taken into consideration.

The *Migration Act 1958*, *Australian Citizenship Act 2007*, *Privacy Act 1988*, *Migration Regulations 1994* and associated instructions, define the department's legal mandate. While there are no specific sections/regulations in respect of identity per se for visa processing, our power to make decisions on the basis that we are not satisfied about someone's identity is implicit in the power to grant and refuse visas.

In addition, Identity Branch has developed a set of Procedure Advice Manuals (PAMs) that are consistent with current legislation and which detail the identity management practices suggested in DIAC programs. Similar procedures need to be developed for all departmental programs that deal with clients.

Analysis conducted by Identity Branch has shown that, even within a single visa program, the processes related to assessing a client's stated identity can vary significantly. The IBRM is seeking to formalise and in some cases extend, existing processes used by decision makers to assess identity. Presently, officers in overseas posts, at the border, in the field and in state and territory offices are, to varying degrees, conducting processes similar to those described in the IBRM.

The issues and risks for the department are currently that:

- some processes are not performed in a standardised or consistent manner (meaning that client records might subtly vary and carry the risk of creating more than one record per client, even under the new systems regime)
- the checks performed might vary from officer to officer when dealing with clients
- the rationale for a previous assessment of a client's identity might not be easily understood by officers in subsequent interactions with the same client
- clients are asked repeatedly for the same information in subsequent dealings with the department

- the risk of identity fraud is not addressed in a coherent and transparent manner.

Therefore, significant improvements in the department's ability to correctly identify clients could be expected, even if the IBRM is adopted based on the existing legislation and procedures as described above.

In order to ensure that the business impacts are considered and can be managed, while standardised identity management processes are incrementally introduced across the department, it is proposed that:

- the IBRM be adopted incrementally as an integral component of every IT change project
- initially, the identity information collected and activities for assessing its veracity, be based on existing legislation and procedures relevant to each business area
- in future, changes to what identity information is collected and what assessment activities are undertaken will be based on the outcome of formal risk assessments conducted with individual business areas using the DIAC Risk Management and Change Management Framework as described in section 4.5.

## 4 Overview of the Identity Business Reference Model

The following summary provides an introduction to new terminology and concepts related to the IBRM, which are described in more detail throughout the document.

Figure 2 illustrates the relationship between the future state identity management business process and other departmental business processes. The Identity Business Reference Model (IBRM) is illustrated in the blue box in the middle of the diagram, which shows the steps required to make a decision about a client's identity during key interactions with the department.

The identity management business process is triggered when specific business events occur that have an identity management aspect. The business events can be part of any departmental business process including visa processing, border processing, compliance and detention processing and citizenship and settlement processing.

The key inputs to the identity management business process are the business context within which the business event occurred, the client's stated identity and some additional client information.

The key outputs from the identity management process are the identity history of clients and a decision on whether or not the stated identity is acceptable within the business context that it was provided.

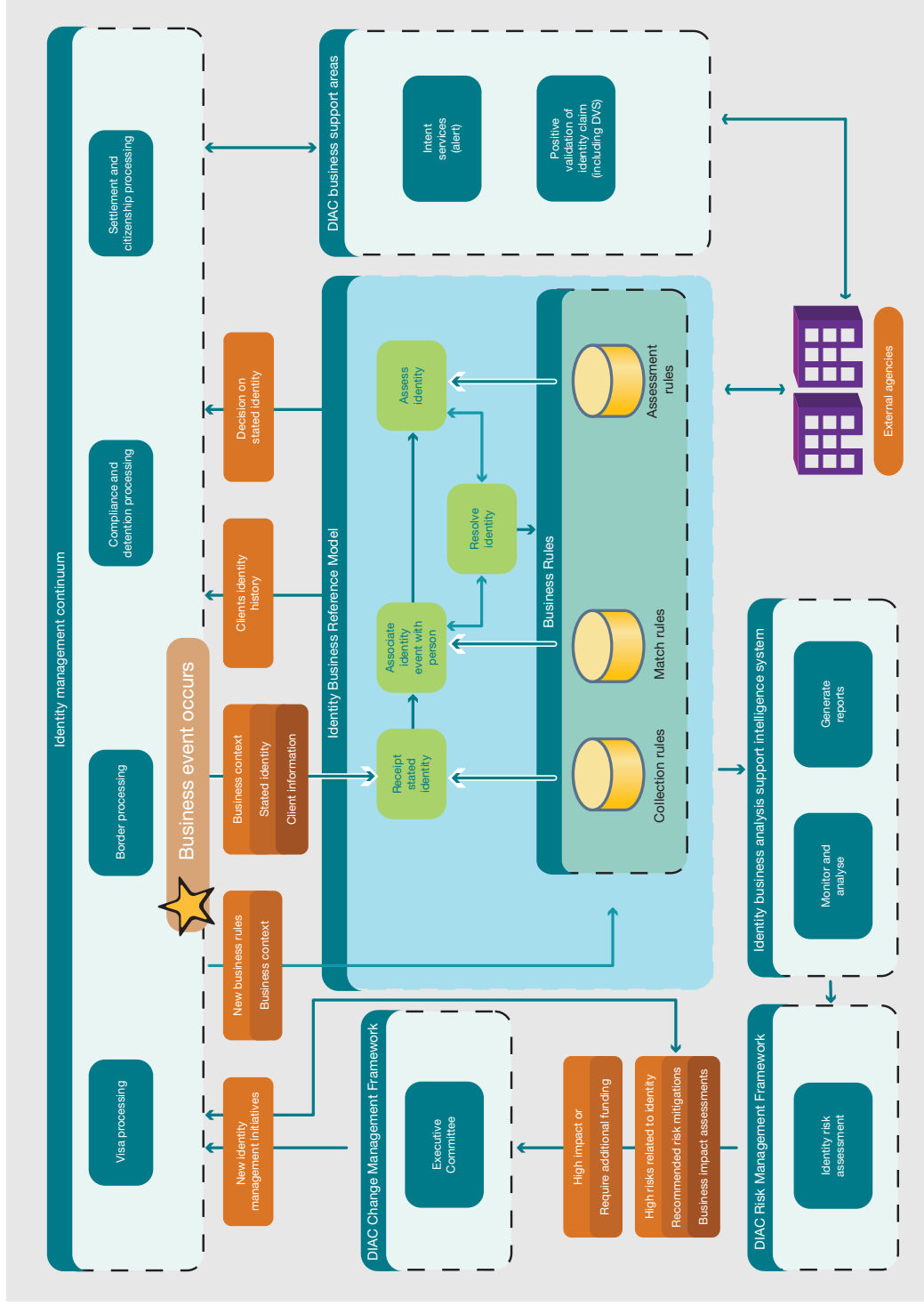
As illustrated in Figure 2, the identity management process is driven by business rules. Business rules provide the flexibility to cater to varying needs for identity management across the department's programs. This is required because the nature of interactions with clients varies significantly across business programs.

Figure 2 also illustrates how other services may be called on to complete the identity management process; for example alert checking, document verification checks and in some cases, services provided by external agencies.

It is envisaged that continuous monitoring of client and identity information, as well as identity related business activity, will enable the department to identify new risks related to our ability to correctly identify a person.

The IBRM allows for a risk based approach for introducing changes in identity management practices across the department. Identity Branch will assist business areas to conduct formal risk assessments according to the DIAC Risk Management Framework. These assessments will allow business areas to identify new treatments to mitigate the highest identity risks. Identity Branch will also provide advice and assistance to business areas to determine the business impact and estimated costs for implementing risk mitigation treatments.

Figure 2 – Future state, identity management in DIAC



For business areas where the introduction of new identity management treatments will have a significant impact on business processes, or where additional funding will be required, business impact statements and recommendations will be formally submitted to the Executive Committee according to the procedures defined in the DIAC Change Management Framework.

The aim of this approach is to ensure well-informed decisions regarding the prioritisation and allocation of funding for initiatives that will reduce the department's risks related to identity fraud or incorrectly identifying a person. This process and approach is discussed in more detail in section 4.5.

The IBRM provides a flexible foundation that can be readily adapted to cater for future changes because it is driven by business rules. Changes to business rules might be required because:

- new identity related risks have been identified
- priorities have changed
- there are changes in government policy.

The flexibility to introduce change is achieved by enabling new business contexts and new identity rules related to specific business contexts to be defined as rules. The fundamental model doesn't change only the rules that drive it within specific business contexts.

The key interactions with the IBRM, illustrated in Figure 2, are described in more detail in the following sub-sections.

## 4.1 Business context

The IBRM is driven by the business context within which interactions with clients take place. The business context is made up of business elements that assist in identifying the level of identity related risk for each business transaction between a client and the department. For example, has the identity information been provided by a trusted third party, or is the visa category one that is known to be vulnerable to identity fraud.

The IBRM allows flexibility in relation to the type of identity information collected and how it is assessed. Variations to the collection and assessment processes will be applied based on the business context and the assessed level of risk of the business transaction. The aim of the model is to ensure that the stated identity is assessed to an appropriate 'level of confidence' applicable to the business context.

For example, if the business context is an Electronic Travel Authority application, the passport details might be the only information receipted as part of a stated identity. The process of checking whether or not the person is already known to the department and assessing the veracity of the travel document and hence the inherent 'claim of identity', might all be automated.

However, if the business context is the reception of a detainee and the detainee is uncooperative, the client's stated identity might initially be regarded as incomplete and unassessed and escalation to the Identity Resolution Centre (IRC) might be required. The IRC could then apply a combination of automated and manual checks before the identity is resolved and a decision is able to be reached on whether or not the stated identity is accepted.

In these two examples, the processes and amount of information recorded about the client's identity are quite different, but both business processes can be aligned with the IBRM by specifying the different business contexts and associated business rules.

The IBRM also makes no assumptions regarding the degree of automation and allows time constraints to be applied via business rules where necessary. Again, these rules are applied based on the business context of the interaction with the client.

The elements that form part of the business context are described, along with an example from the General Skilled Migration program, in Appendix B. As each business area adopts the IBRM, the relevant business context for their area will be identified and documented as shown in the example at Appendix B. Business rules that detail the identity information to be collected for each business context and what activities are required to adequately assess the information will be mapped to each specific business context.

## 4.2 Business rules

The business rules applicable to the business context and, in some cases, certain aspects of the client's stated identity will determine:

- what identity information is collected as part of an identity event
- when an identity event is to be escalated for identity resolution
- what activities are undertaken to assess whether or not the stated identity is acceptable within the business context
- time constraints and other rules relevant to a specific business context, for example, time constraints necessary to meet client service standards.

The use of business rules will provide the flexibility required for identity management across the different business programs of the department. It also allows for rules to change over time as new risks are identified and with the evolution of new technology tools. Furthermore, the use of business rules provides a mechanism for incrementally improving and increasing the identity information collected and the processes for assessing it, as required.

### 4.3 Identity events and identity history

The model predicates that the business context, the stated identity, the identity assessment outcome and other relevant client information will be recorded during specific interactions between a client and the department. All of this information forms part of an **identity event**.

The model also predicates that all identity events related to the same client will be available as part of that client's **identity history**. The cumulative identity events will comprise a client's identity history. A client's identity history must be available to decision makers whenever they are viewing a client's record. This will assist them to determine when a client is already known to the department. It will also help them to assess the stated identity for a new business transaction with an existing client.

The identity history may also be used to determine how much information is collected during subsequent business transactions with the same client. The following scenario is provided as an example.

A client travels regularly to Australia within the business context of an Entertainment visa (visa sub-class 420). The client has recently provided a full set of client and identity information as defined by the business rules applicable to the entertainment visa business context. The information provided has been validated via the comprehensive identity assessment activities that were undertaken the first time the client applied for a sub-class 420 visa, as defined by the business rules. On repeat visits that are within predetermined timeframes, the identity collection rules might indicate that only a facial image and a current passport are required to be receipted and validated. A confirmed match of the new facial image against the facial image captured during the first visit may be sufficient to validate that we are dealing with the same client. Providing the passport proves to be genuine and there are no matches against identity alert checks, no additional identity information may be required.

### 4.4 Identity business intelligence analytic service

The identity business intelligence analytic service will involve continuous monitoring, evaluation and analysis of the following:

- quality and integrity of operational client and identity data
- number and nature of referrals escalated for identity resolution
- reports of suspected and confirmed identity fraud cases
- reports on the nature and relationships of trends related to identity fraud
- metrics (performance measures) captured through the monitoring of identity management business process activity.

Sophisticated data mining, analysis and reporting tools will be used to detect patterns and trends relevant to identity risk and identity fraud.

The output from the identity business intelligence analytic service process will include:

- improved visibility of identity fraud incidents and trends in identity fraud
- identification of new matching rules for more effective comparison of client and identity information
- identification of new identity related risks which will be fed into the identity risk assessments described in section 4.5
- improved understanding of the impact of identity related risks on the department's ability to achieve its corporate goals
- a reduction in the number of duplicate client records across the department's information holdings
- improved quality of client and identity information.

The capability described in this section is not an explicit part of the IBRM, nor has such a capability yet been established in the department. However, the advantages of monitoring and reporting on business activity and information are well known. In addition, it is understood that an initiative is underway to investigate and advise the department on the advantages of the introduction of a broader fraud detection and monitoring capability. Therefore, this section describes how such a capability could be integrated with the new identity management practices to enable the department to continually improve the quality of its fraud information and the operational effectiveness of its detection and mitigation practices.

## 4.5 Identity risk assessments and change management

The DIAC Risk Management Framework provides a methodology, a suite of tools and a governance process for effecting change in the department based on risk. The framework is based on the Australian Standard for Risk Management.

The Risk Management Framework defines risk as:

*“Any event that threatens the achievement of our corporate goals or objectives.”*

In the context of identity management we are concerned with risks that threaten the department's ability to ‘correctly identify a person’, which is directly linked to the Departmental Output 1.3.2:

*“to identify people entering Australia and maintain that foundation identity for use in the Australian community.”*

In accordance with the Risk Management Framework, the risks associated with incorrectly identifying a person within specific business areas will be identified and documented.

These might include risks identified and advised by third parties or the risks identified during the identity business intelligence analytic service process described above.

Identity Branch will liaise with the relevant business areas to determine which risks are of most concern to their area. Individual business areas will undertake the following activities as part of the identity risk assessment, with assistance from Identity Branch as required.

- For each risk identified, the likelihood of the event occurring will be determined, as well as the consequence or impact if it does. These two components will then be used together to assess an overall level of risk.
- During the risk assessment, risk mitigation treatments will be identified for the highest risks. The risk mitigation treatments may involve the collection of more information related to the client's identity and/or additional activities to assess the veracity of the identity information.
- Once the high risks and associated risk mitigations have been determined, Identity Branch will assist business areas to prepare business impact assessments that describe the extent to which the risks will be mitigated. Business benefits that are anticipated through the implementation of the risk mitigation treatments will also be identified. Importantly, the business impact assessment will also balance the identity related benefits against the impacts to other departmental objectives, such as maintaining/ increasing tourism levels, financial incentives for the education sector, processing impacts and the associated costs for adopting the identity risk treatments.
- Where the impact of introducing risk mitigation treatments is low and can be readily funded by the relevant business area, they will be approved through the line area governance process.
- Where the introduction of risk mitigation treatments will be high, or where additional funding will be required, the risk assessment outcome and business impact statements will be submitted to the Executive Committee via the DIAC Change Management Framework. The Executive Committee will decide whether to endorse the risk mitigation treatments or, alternatively, to accept the high risks without implementing the risk treatments.
- Finally, Identity Branch will assist each business area to develop a business transformation plan to manage the implementation of endorsed identity related risk treatments. This will ensure adequate consultation and collaboration between Identity Branch and other programs within the department.

As illustrated in Figure 2, the implementation of new identity management initiatives will involve the definition of new business contexts and related identity business rules.

The nature of risk is dynamic. Unanticipated national and global events, as well as changes in government or government policy, will require changes to the department's approach to identity related risk. In addition, methods and technology tools are continuously evolving and improving in relation to identity management.

While economic downturns or civil disruption in one country may require the department to be more rigorous in assessing the identity of clients from that country, it is also important to note that the opposite may be required. For example, the overall incidence of immigration fraud and identity fraud in particular, tends to diminish in previously high risk countries whose economies have experienced significant growth and development. In such circumstances, as the risks in these caseloads reduce so would our need for extensive identity assessment, leading to a reduction in documentary and processing requirements.

Therefore, it will be important that the department undertakes periodic formal risk assessments to ensure it remains informed of the identity related risks and the most appropriate ways to mitigate them.

The IBRM provides a risk based and business rules based architecture that allows for a flexible and timely approach to external and internal change. The aim of this approach is to ensure executive decision makers are adequately informed:

- when the department is exposed to high risks related to incorrectly identifying a client
- of the cost and impact of implementing appropriate identity risk mitigation strategies
- to enable prioritisation of expenditure so that effort is applied where the department is most at risk
- to identify where additional funding proposals are required in order to implement identity risk mitigation strategies.

## 5 Identity Business Reference Model

The IBRM provides a model for realising improved identity management practices in the department's operational environment. This section describes the following core elements of the IBRM:

- **the business motivation model**, which illustrates how the IBRM will enable the outcomes defined in the strategic plan to be met
- **the business process model**, which identifies and describes the work-flows and processes related to identity management. The following elements of the IBRM are defined in relation to each individual process in the business process model:
  - \* **the business event model** identifies and describes the broader departmental business events that initiate identity management business processes
  - \* **the locations model** outlines the geographical locations where identity management business processes are physically performed
  - \* **the organisation and roles model** identifies and describes the organisational aspects and roles of people involved in identity management in the department.
- **the information model**, which identifies and describes the key information elements required to undertake specific identity management business processes.

These models can be used:

- \* to illustrate how new business processes will improve the effectiveness of identity management
- \* to assess the impact on business processes and the time and skills required in existing business areas for introducing improved identity management practices
- \* to involve and communicate to other business areas where identity management business processes will be invoked
- \* to ensure identity management fits seamlessly and consistently into other departmental business processes
- \* to illustrate how the collection of new identity information will improve the effectiveness of identity management
- \* to determine gaps between information currently collected relating to identity management and what could be required in the future
- \* by Identity Branch and other departmental managers to determine priorities and to assist in planning in relation to structure and staffing when introducing new and improved identity management practices
- \* by legal staff and policy developers to determine where new legislation and policy will be required to support new business processes
- \* by project teams to develop requirements related to identity business processes
- \* by project teams to develop more detailed business processes and business rules associated with identity information.