

06: Identity management in DIAC

The vision

57. The vision is expressed in the identity objective which forms Departmental Outcome 1.3.2., which is:

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

58. This relates to Departmental Outcome 1, which is:

'to contribute to Australia's society and its economic advancement through the lawful and orderly entry and stay of people.'

59. Once the foundation identity has been established, it will be consistently matched during subsequent interactions with DIAC and other approved Australian Government agencies as well as key private sector agencies. DIAC clients will benefit because staff will be fully aware of their client history and should be able to address their needs more efficiently. The Australian community will benefit through the improved detection and deterrence of identity fraud, reducing the cost impost as well as enhancing security.

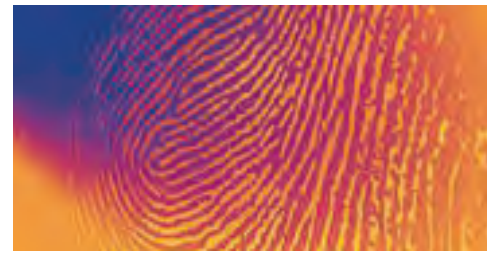
The goals

60. DIAC will achieve this vision through an identity management strategy that will deliver the following outcomes:

- 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
- provide an effective legislative framework to support biometrics and identity management.

Key deliverables

61. The key deliverables to effect the strategy are:
- organisational change via an identity change management strategy
 - an identity services capability
 - an identity resolution capability
 - the Biometrics at the Border capability.



Organisational change

62. The organisational change programme will address the people, process and technology aspects required to support DIAC's identity management vision. The change management strategy will focus on supporting the people component of the change. This will be done by:
- Change management planning – development of the overall portfolio transformation strategy, preparation of the necessary plans, identification of any changes to legislation and regulations, development of new policies and procedures, adoption of appropriate national and international standards, and facilitation and monitoring of the implementation of the strategy.
 - Stakeholder engagement and management – all key business areas will be consulted to communicate the benefits of identity management and engaged to contribute to the implementation of the strategy.
 - Communication – a communication strategy will be developed which details the approach and plan to deliver timely, relevant, and clear information to key stakeholders and managers.
 - Governance – governance for the strategic plan is vested in Border Security Division, which will report through the DIAC governance process. Projects initiated to support this strategy will report through the department's governance committee framework to ensure effective decision making,

management and oversight of the formulation and implementation of the strategy.

- Training – a training plan will be developed and delivered to ensure staff are able to successfully perform their jobs using the enhanced identity policies, procedures, technology and systems. The identity management change programme must ensure that all relevant staff are trained and ready for the new way of doing business.

Identity services capability

63. The purpose of an identity services capability is to manage the complex relationship between personal information, credentials and a biometric (where held) so that staff will be able to see a consolidated, correct and current view of a client's record.
64. DIAC's identity services capability comprises a suite of enabling tools that includes the data repository as well as software and processing engines to manage the biographic data, documentary details, digital facial images and other biometric data relating to the identity of clients. The identity services capability will support the business portals being developed under *Systems for People*. The capability will also manage updated or amended client data.
65. Where a biometric has been captured, this will be used to verify whether differing data refers to the same client.

06: Identity management in DIAC

Identity resolution capability

66. Under *Systems for People*, the department will develop an identity resolution capability to support operational staff by ascertaining a client's identity in complex cases, for example where client records have insufficient information or contain differing identity details.
67. In 2005, DIAC established the National Identity Verification and Advice section (NIVA) to monitor the resolution of cases of unresolved identity in the detention and compliance caseloads through 'information' referrals to NIVA and, when required, to assist line areas in more complex cases through 'action' referrals. NIVA continues to build expertise in the resolution of identity.
68. The identity resolution capability will draw together existing expertise, such as NIVA or identity units in state offices, as well as anticipated departmental resources with expertise in:
 - name searching
 - data matching of biographic and other data related to resolving identity
 - document examination
 - biometric examination (including finger scan and facial biometrics)
 - systematic investigation of identity issues.
69. Under *Systems for People*, the department will develop an identity resolution capability that will:
 - Respond in a timely manner to referrals for identity resolution to support business and operational areas.
 - Provide a holistic approach for identity resolution involving the coherent examination and authentication of biographic data, proof-of-identity documentation and biometrics.
 - Record and notify relevant stakeholders of suspected and confirmed cases of identity fraud.
 - Interact with and support other operational centres such as the Border Operations Centre.
 - Work with external parties (government and international) as required to resolve complex identity cases (through the services of NIVA).
 - Record and provide reports on identity fraud and other matters related to identity as required.

Biometrics at the Border

70. The early resources for identity management came from government approval for the Biometrics at the Border initiative. This initiative remains a core element to the identity management strategy and will be one of the most visible outcomes when it is fully implemented. DIAC is the lead agency in this initiative, which is addressed in more detail in the *Strategic Plan for Biometrics at the Border 2005-2010*.
71. The strategy involves four agencies whose roles are broadly as follows:
- **Customs** – undertakes the primary role for processing border-crossings and is the major user of biometric data at the border. Customs acquires biometric data through SmartGate and uses this data to facilitate border crossing for Australian citizens and selected low risk, high integrity individuals.
 - **DFAT** – provides Australian passports to citizens and acquires biometric and identity data as a part of this enrolment process. The essence of DFAT's contribution to the whole-of-government strategy is the progressive introduction of e-passports which incorporate a biometric chip and utilise facial recognition technology to replace the current passport. Customs then uses this data to facilitate the passage of citizens across the border.
 - **DIAC** – makes first contact with individuals seeking entry, which gives us the broadest capability to acquire biometric identifiers for non-citizens wishing to visit Australia. The identity management strategy facilitates the gradual increased collection of biometric data to support identity management and for matching with Customs and DFAT.
 - **The Office of the Privacy Commissioner** – respect for privacy is a keystone of Australian culture. The role of the OPC is to promote a best practice approach to privacy in the projects undertaken by the border control agencies by providing advice on the application of privacy legislation, assisting agencies undertaking privacy impact assessments and by conducting a schedule of privacy audits.
72. Biometrics at the Border is intended to be fully implemented by June 2009. Much of the work initiated under Biometrics at the Border will underpin the identity services capability and the identity resolution capability.
73. The contribution that the key deliverables make to the identity management strategy is shown in Figure 4.

06: Identity management in DIAC

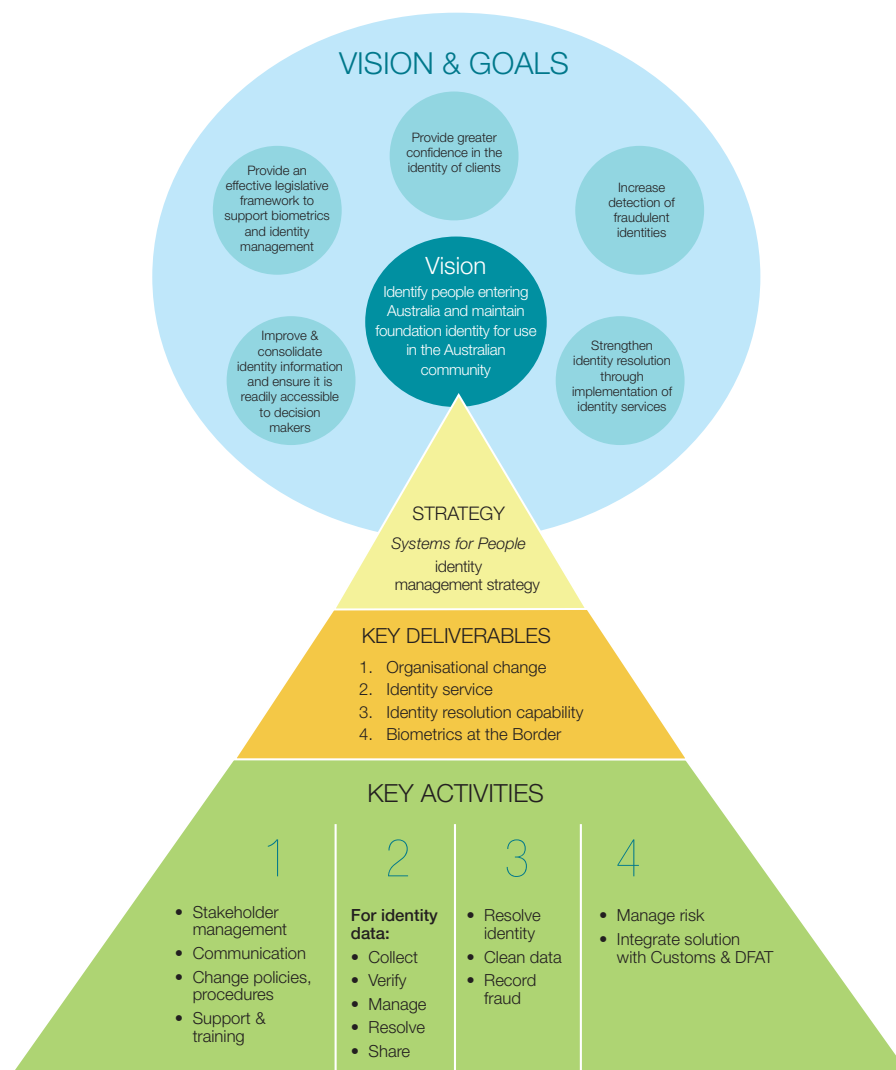


Figure 4 - Identity management strategy

Identity management processes

74. DIAC's identity management strategy will involve:

- **collecting** a richer set of identity attributes from our clients
- **verifying** identity data against existing information held in our own or other agencies' systems
- **managing** identity data in our systems
- **resolving** identity
- **sharing** identity data with other agencies that have a legitimate need to know.

Collecting better identity data from our clients

75. Establishing the identity of a client should be completed as a discrete activity prior to the processing of any request or application. An application should not be processed until the identity of the client is deemed to be adequately ascertained.
76. Client processing staff will use the redesigned business processes to collect a more consistent minimum set of biographic identity data, which will include biographic details such as name, date of birth, aliases and other personal identification information such as current address, current telephone numbers, national identity card information and other proof-of-identity credentials.
77. For selected business processes, staff will collect a richer set of identity data. This could include scanning the credentials or proof-of-identity documents provided with an application as well as biometric information – particularly facial images and finger scans. The combination of identity information staff collect will vary depending on the business process or service the client is seeking and the assessed risk.
78. The aim is to ensure consistent and standardised client identity enrolment across the department's programmes.

Verifying identity data against existing information held in DIAC's or other agencies' systems

79. The next step is that staff will verify the evidence of identity documents rather than accepting them at face value – an unverified identity is a 'claimed' identity. The preferred way to verify identity is to check the document details against the issuing authority databases. Staff will be able to use appropriate online authentication processes, which are being developed to support increasing electronic lodgment and management of many types of applications.
80. The document verification service is a whole-of-government approach being developed to allow other government agencies to perform online checks of DIAC-issued documents against DIAC databases. Conversely, it will enable DIAC staff to check proof-of-identity documents issued by other agencies – online and in real time. This includes documents such as drivers' licenses, birth certificates and Australian passports.
81. If an online capability does not exist, staff can perform checks using existing identity document verification systems like Edison, DIAC databases or commercially available data holdings. Staff can also check identity information via interviews with the client, employers, other government agencies (especially law enforcement) and appropriate third parties.

06: Identity management in DIAC

82. Once a base set of identity data has been collected on a client, staff should refer or check back to this original data set in all future interactions. This approach will ensure we verify that the client continues to present as the same identity each time we deal with them while, at the same time, building up our identity information base. Staff will record all changes of identity details so that we develop a full client identity history.

Managing identity data

83. DIAC has an obligation to administer the identity data held in its systems in accordance with the *Migration Act 1958* and the *Privacy Act 1988*. The *Migration Act 1958* has been amended to provide a comprehensive regime for the collection, storage, use and sharing of biometric and personal identifiers.
84. Staff will use the identity services capability to manage client identity data. As part of the capability appropriate tools will also be developed to assist staff in assessing and treating identity related risk – including the capacity for matching to selected watch and alert lists and compiling identity confidence levels.
85. The management of consolidated identity data in an identity service capability, using appropriate verification of proof-of-identity information and the use of risk assessment tools will enable DIAC staff to derive a confidence level in the identity information held on a client.
- Staff can use this confidence level when deciding how the application will be processed. They will also be able to ascertain what identity information has been collected and whether it has already been verified.

Resolving identity

86. DIAC staff have an obligation to record client data accurately and to pursue any anomalies. Where staff have difficulty resolving a client identity due to duplicate or mismatching data or inadequate proof-of-identity credentials they can seek advice from, or refer the case to, NIVA. NIVA has developed a forensic identity investigation service and is developing expertise and networks important for seeking matches for a client whose identity is difficult to verify.
87. The NIVA functions will be expanded as part of the identity resolution capability being developed. It is anticipated that the capability will be the recipient of referrals from processing areas, the Border Operations Centre or state identity verification teams. The staff initiating the referral will be advised of the outcome of the identity resolution and the status of the identity will be updated in the identity service capability.

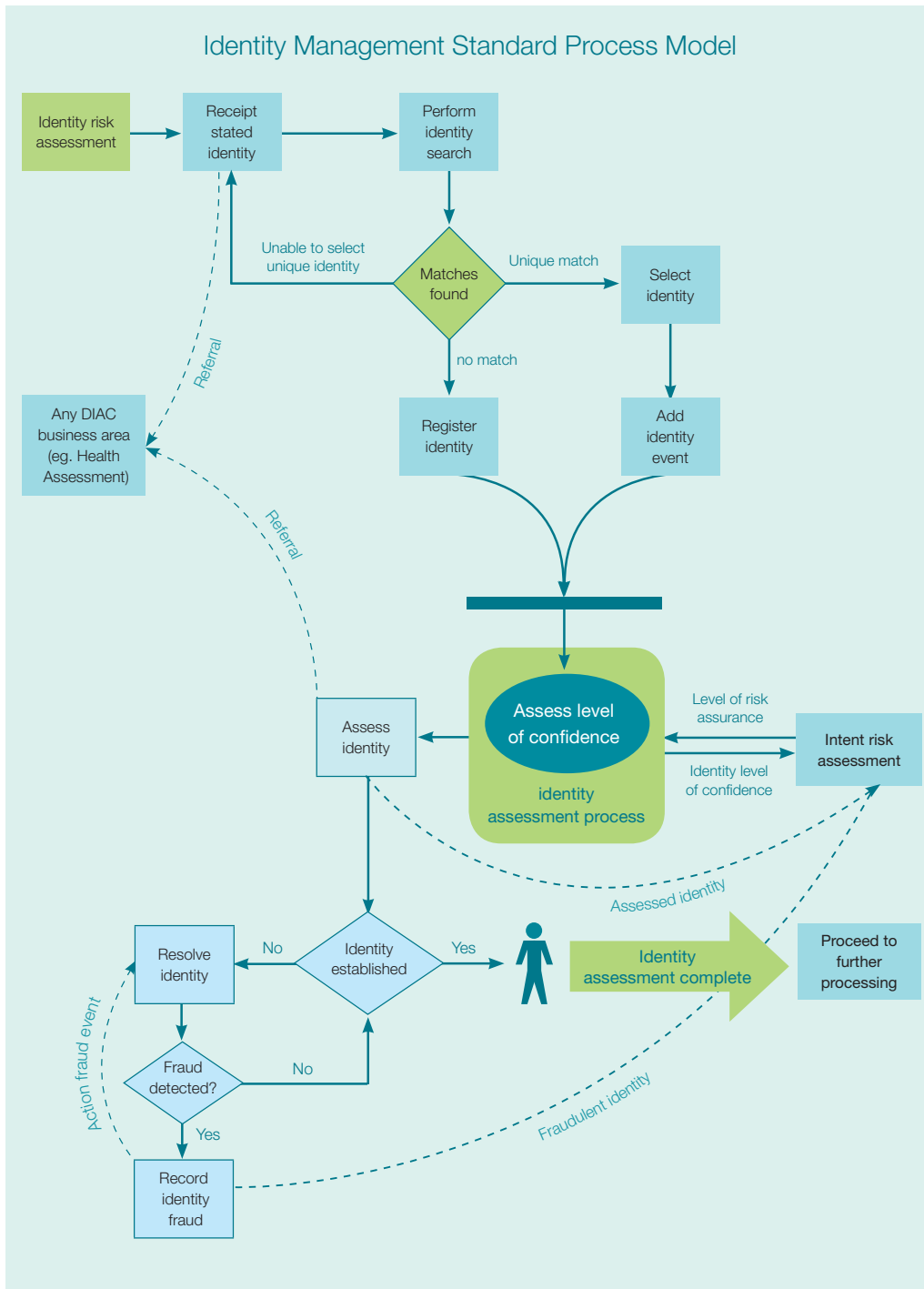


Figure 5: Identity Management Standard Process Model

06: Identity management in DIAC

88. At the strategic level, the department has a responsibility to improve the accuracy of personal identity information held in its databases, including the 'cleansing' of existing records where appropriate. This is consistent with one of the key elements of the National Identity Security Strategy, which relies on agencies improving the integrity of their identity data holdings.
89. Data integrity is particularly necessary for the effective operation of the national Document Verification Service. The existence of multiple, incorrect or fraudulent registration in key agency data holdings would compromise the efficient working of the Document Verification Service and could lead to a compounding of fraudulent identity information.
90. The way in which a client's identity will be managed using these new tools and services is represented in Figure 5.

Sharing identity data with other agencies that have a legitimate need to know

91. It is important that the DIAC identity management strategy takes into consideration the initiatives being developed and implemented by other agencies to ensure that appropriate data is able to be shared when there is a clear business need and appropriate safeguards are in place.
92. In the performance of their duties, DIAC staff may need to access biographic and/or biometric data collected by other Australian Government or state and territory agencies. The matching of identity data might be used to detect and combat identity fraud and identity theft. All data matching and the collection of biometrics are subject to privacy and other legislative provisions. Some of the potential uses include intelligence analysis, the verification of eligibility for benefits and services, law enforcement and counter terrorism.
93. Significant identity data sharing opportunities exist in relation to the National Identity Security Strategy, the Biometrics at the Border initiative, a number of international biometric initiatives and the Australian national law enforcement databases administered by CrimTrac.

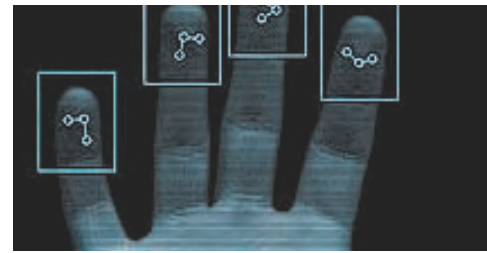


07: National Identity Security Strategy

94. The preservation and protection of a person's identity is a key concern and right of all Australians. In recognition of this, on 14 April 2005, the Australian Government announced the National Identity Security Strategy (NISS) to combat the misuse of stolen or assumed identities in the provision of governmental services. The NISS is coordinated by the Attorney-General's Department.
95. Key components of the NISS include:
- the development and implementation of a national Document Verification Service to combat the misuse of false and stolen identities
 - investigation of the means by which reliable, consistent and nationally interoperable biometric security measures could be adopted by all jurisdictions
 - a process to ensure identity data integrity
 - a gold standard client enrolment process
 - new document security standards.
- ### DIAC's role in the NISS
96. As the first Australian Government agency to encounter non-citizens, DIAC has a responsibility to determine and record a non-citizen's identity as accurately as possible so that it can be relied on by other Australian agencies in their subsequent dealings with these clients.
97. The DIAC identity management strategy contributes to the whole-of-government NISS in a number of ways:
- wherever possible, DIAC will adopt the gold standard client enrolment process for all high-value transactions conducted by the department
 - DIAC issued documents that are used as proof of identity will adhere to security standards adopted as part of the NISS
 - DIAC will be a major participant in the development of the Document Verification Service
 - DIAC will continue to improve the integrity and quality of its identity data through the client data cleanse project.
98. The department is represented on all five working groups that report to the Commonwealth Reference Group on Identity Security, as depicted in Figure 6 on page 29.

08: International identity strategies

99. There are a range of international fora that work on biometric and other identity issues of which DIAC is a member. Some of the key groups for DIAC are:
- The **Four Countries Conference Biometrics and Technology Sub-Group** – was created in February 2006 and comprises Australia, Canada, the UK and USA. Australia (DIAC) is the inaugural chair and secretariat, (positions are to be rotated among the members). The objective of this sub-group is to identify and pursue options for improved collaboration and interoperability between the four countries on biometrics and identity issues.
 - The **IGC Technology Working Group** – is an informal, non-decision making forum for information exchange on policy and practical issues relevant to technology (including biometrics). Government officials attend from Western European and North American countries, as well as Australia, New Zealand, the European Commission, UNHCR and IOM. This Working Group is chaired by Australia (DIAC) for the time being.
 - The **APEC Business Mobility Group** – develops strategies and initiatives to streamline the mobility of business people to facilitate trade and investment in the APEC region.
- Australia (DIAC) also chairs this group and provides its secretariat function. A number of identity-related projects are sanctioned by the group.
- Other international technical and standardisation groups – responsible for developing specifications for travel documents, such as the **ICAO Technical Advisory Group on Machine Readable Travel Documents** and the **ICAO New Technologies Working Group**.
100. Identity Branch maintains a research function that monitors national and international biometric and other identity-related developments. A bulletin encapsulating the research outputs is distributed within DIAC, to other Australian Government agencies and internationally to inform identity and biometric policy development.



Global Document Examination Network

101. The Global Document Examination Network is responsible for supporting the integrity of Australia’s borders and our visa and citizenship programmes by providing a forensic document examination service, establishing national standards and procedures, offering technical training opportunities for document examiners and providing document examination training for departmental staff whose work involves reliance upon documents.

102. The department has also developed desktop accessible systems to assist departmental staff to recognise counterfeit or fraudulently altered documents. The Global Document Examination Network also supports the department’s endorsed international engagement agenda by undertaking international capacity building activities at home and abroad. This support includes providing document examination training and establishing document examination laboratories for countries in the Asia-Pacific region.

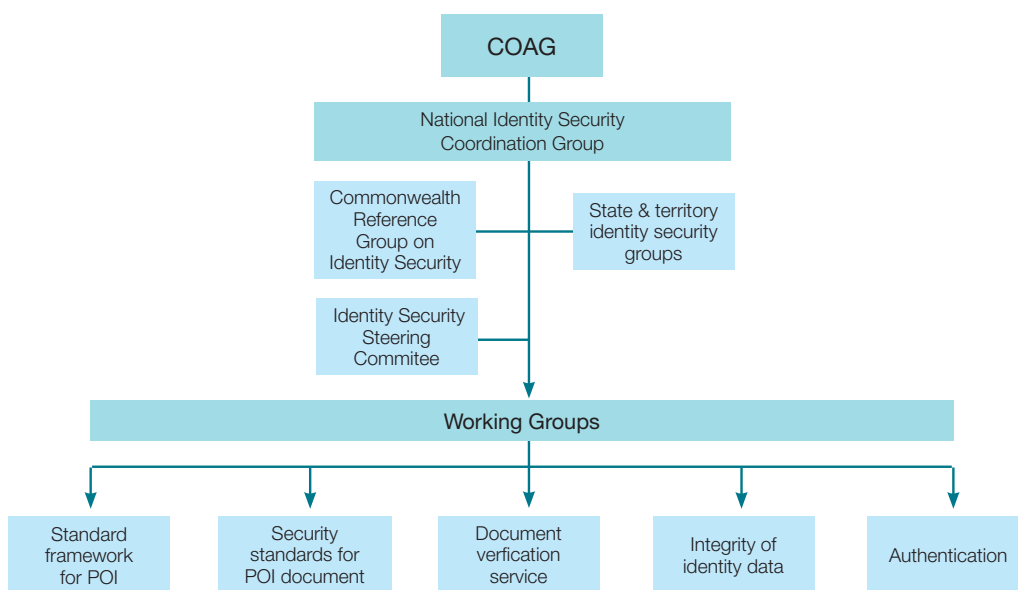


Figure 6: Commonwealth Reference Group on Identity Security

09: Governance and reporting

103. The DIAC identity management strategy must be consistent with, and contribute to, the National Identity Security Strategy as well as international standards and developments in our major international partners.
104. The projects established to implement this strategy will report through the department's governance committee framework via the following committees:
- Border Security Governance Committee quarterly in relation to the performance of the branch
 - Systems Committee via the Border Systems Committee on matters of IT and technology and integration with *Systems for People*
 - Executive Management Committee via the above-mentioned committees
 - Fraud, Integrity and Security Committee (bi-monthly) via the Compliance Framework Branch
 - Strategic Policy and Steering Committees as required.
105. DIAC is represented on, and reports to a variety of national and international working groups related to identity management, and these are addressed separately under those sections in this plan.
106. The department's implementation of its identity management strategy and the deployment of biometric tools is subject to internal audits as well as regular audits from the OPC as part of the Cabinet implementation plan for Biometrics at the Border. The department's planning for identity management and the introduction of biometrics will also be the subject of a performance audit by the Australian National Audit Office (ANAO).

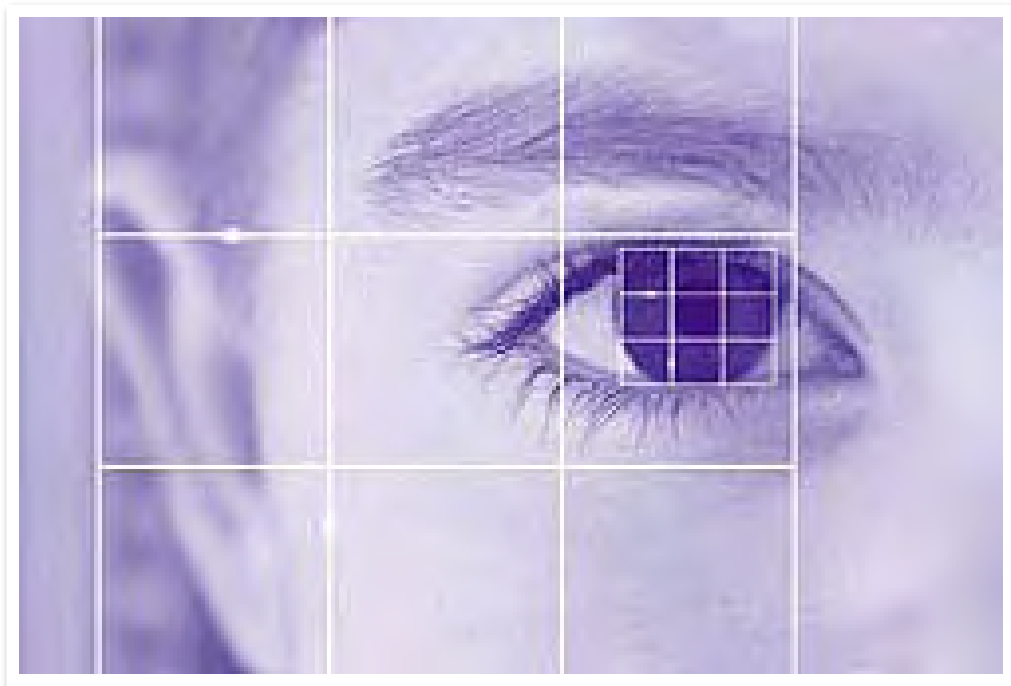
10: Key benefits of DIAC's identity management strategy

107. The key benefits to the Australian Government and society derived from an increased focus on the verification of identity and the employment of biometric tools are:

ESTABLISH IDENTITY	Establish foundation identity of applicants	Initial verification of identity and detection of false or assumed identities. Ensure visas granted only to people approved for travel and that previously rejected applicants are deterred.
	Enhance national security – Detect and refer persons of concern	More effective identity screening mechanisms offshore due to biometric alert list matching that will identify persons of concern before travel to Australia allowing the risk to be managed offshore. For Australian citizens this includes a highly secure Australian passport. Enhanced ability to detect document fraud.
CONSOLIDATE IDENTITY	Consolidate client view	Consolidation of client interactions using biometric tools to 'anchor' identity, that provides DIAC with a single client view. Reduction in the inadvertent generation of multiple identities as well as greater detection of clients using name variations as alternative identities.
VERIFY IDENTITY	Facilitate and secure border movement	Legitimate travellers to Australia should have their movement across Australian borders facilitated efficiently due to the implementation of biometric technology at the border. Increased detection of identity fraud and any substitution at the border.
MAINTAIN IDENTITY	Identify visa breaches	Non-citizens who breach their visa conditions should be readily identified through biometric technology and dealt with by the Australian Government in a consistent manner within the terms and conditions of their visa. It will also assist in the removal of unsuccessful asylum seekers in detention.
	Protection from personal identity theft	Australian residents should have greater protection from having their identities stolen due to the implementation of a consistent identity management strategy and the deployment of biometric technology.
	Protection from identity fraud	Australian industry and government should have greater protection from fraud caused by false or multiple identities due to the improved identity management of non-citizens in Australia. It will also reduce the capacity for the use of fraudulent identities by protection visa applicants and reduce the costs to the legal system of contesting actions mounted by this litigious group.
	Know who our future citizens are	Australia will have greater confidence in the identity of the non-citizens who are our future Australian citizens.

1.1: Major milestones during 2007-2010

108. The identity management strategy will be delivered in increments of identity management capability that is progressively rolled out across DIAC functions. The table at Attachment A provides details on the progressive delivery of the strategy on a financial year quarterly basis.





12: Description of the vision at 2010

109. DIAC anticipates that the key deliverables will be progressed to the extent outlined below.

Organisational change

110. By 2010 there will have been a significant change to DIAC's core business processes. New and enhanced identity management practices, including the use of biometrics where relevant, will be incorporated into all interactions with DIAC's clients. This business and organisational change will be managed as follows:

- The Migration Act 1958 and associated regulations will allow for the collection, use and sharing of biometric information during application processing, at the border, post arrival and during citizenship application processing.
- New and enhanced identity management business processes will be operational in support of:
 - detention reception processing
 - compliance activities
 - application processing of the refugee and humanitarian and onshore protection caseloads
 - settlement processing
 - secondary line processing at air and seaports
 - citizenship application processing
 - interactions with approved external Australian and international agencies
 - other business processes according to risk.
- All stakeholders will be aware of DIAC's strengthened identity management capability including:
 - the general public
 - DIAC stakeholders across all business streams
 - other government departments
 - international agencies.
- New and improved identity management business processes will include:
 - collection of an extended range and improved quality of identity information
 - enhanced searching techniques, including the use of biometric matching
 - enhanced alert capability involving the use of biometric watch lists
 - enhanced and extended document examination techniques
 - new processes to cater for the detection and recording of identity fraud.
- Policies and associated procedure advice manuals will be available to support the above business processes.

12: Description of the vision at 2010

- DIAC staff and partners who interact with DIAC clients will have the necessary knowledge and skills required to support the new and enhanced identity management processes.
- DIAC standards will exist that are aligned with the appropriate international standards and the NISS gold standard client enrolment process. They will be adopted as part of the identity management business processes.

Identity services capability

111. By 2010, the DIAC identity services capability will be fully operational as follows:

- The capability will be the interface to the DIAC system of record for all identity information. It will:
 - support the capture, storage and retrieval of identity information of DIAC clients including:
 - biographic information
 - proof-of-identity document images and associated information
 - facial images of biometric quality and associated information
 - finger scan images of biometric quality and associated information
 - provide a single identity for DIAC clients regardless of which business processing system is being used: application, border, compliance, detention, settlement or citizenship
 - interface with DIAC alert systems, including the biometric alert system,

to enhance the detection and prevention of identity fraud and to support the identity risk profiling capability

- support searching for and identifying DIAC clients using any or all of the following techniques:
 - name searching
 - simple field data matching
 - automated facial recognition
 - automated finger scan recognition
- interface with Australian Government, international and commercial systems supporting the sharing and validation of identity information on DIAC clients
- segment identity information and include relevant access and security controls to protect the privacy of DIAC clients
- support the recording, monitoring and reporting on known and suspected attempts at identity fraud
- support a risk profiling capability to assist in identifying clients suspected of committing, or being likely to commit, identity fraud.

Identity resolution capability

112. By 2010, an identity resolution capability will be fully operational and support the following:

- New and enhanced business processes will be operational supporting the escalation and resolution of complex identity related issues.

- Operational capabilities, such as system help desks and NIVA, will be consolidated or integrated, providing extended and improved identity resolution services.
- Identity resolution processes will be fully integrated with other DIAC business processes, including visa processing, border processing, detention and compliance activities.
- Staff responsible for resolving complex identity cases will have the necessary knowledge and skills required, including the ability to:
 - compare facial images using automated and manual methods
 - compare finger scan images using automated and manual methods
 - undertake advanced document examination techniques
 - use enhanced name searching and data matching tools
 - detect, monitor and report on identity fraud
 - undertake identity risk profiling.
- The identity resolution capability will be supported by the centralised identity service, which will interface with other DIAC systems as required.
- Policies and associated procedure advice manuals will be available to support identity resolution.
- The capability will contribute to improving the quality and integrity of identity and client records.

Biometrics at the Border

113. The Biometrics at the Border initiative had already delivered significant capability by 2007. The following milestones are specific Biometrics at the Border initiatives and remain an integral part of this strategy:
- An integrated border solution will have been determined that makes effective use of the DIAC and Customs border systems and DFAT's passport database.
 - Mobile and fixed biometric equipment will be operational and used to collect biometrics (facial images and finger scans):
 - at all DIAC detention facilities
 - by compliance officers
 - at selected offshore posts processing refugee and humanitarian applicants
 - at DIAC state and territory offices where onshore protection visas are processed
 - at secondary lines at air and seaports.
 - A biometric watch list capability will be fully operational and effectively integrated with the centralised identity service.
 - A biometric facial image and finger scan search and matching capability will be fully operational and integrated with the centralised identity service.

13: Critical success factors

114. The key critical success factor for implementing this strategy is the availability of *Systems for People* technical resources to support identity management projects. In addition, the following are also critical factors for the successful implementation of identity management into DIAC:

Organisational change

- Full integration with *Systems for People* business transformation.
- Robust, integrated and comprehensive planning that clearly communicates the vision, the key benefits and what is required.
- A corporate approach and support for the business transformation required and the adoption of identity management in all relevant business processes.
- Alignment of key managers and stakeholders around the programme and future state.
- Alignment with organisational priorities, including the imperative for efficient processing of applications and movements of people.
- Clearly defined business policies and procedures, underpinned by sound enabling legislation.

- Timely guidance and training for DIAC staff required to identify clients in all relevant business processes.

Identity services capability

- Best use of, and effective integration of, the tools provided by DIAC's strategic partners IBM and Unisys.
- DIAC's strategic partners understand DIAC business and provide credible and user-friendly solutions that are also agile and scalable to ensure DIAC is positioned to continue to make best use of technology.
- Delivery of a fully centralised identity services capability that works with all *Systems for People* portals and effectively manages client identity data to support DIAC decision makers.
- Delivery of a centralised identity management capability that enables DIAC to detect identity fraud and mitigate the risks associated with identity crime.
- DIAC client data meets national client data enrolment and integrity requirements and is able to be effectively shared with other authorised agencies.



Identity resolution capability

- Availability of an accessible, comprehensive and effective identity resolution capability to support DIAC decision makers and mitigate the risks associated with unresolved identity.
- Effective capitalisation of DIAC's existing expertise to provide a best practice identity resolution capability which meets national and international standards, including document examination techniques.

Biometrics at the Border

- Timely contribution by DIAC to the Biometrics at the Border programme with initiatives that are well-integrated with the work of DFAT and Customs and also accord with best practice privacy legislation and principles as determined by the OPC.
- The ability to efficiently and effectively match biometrics captured as part of Biometrics at the Border against specified DIAC, national and international watch lists.

115. In summary, the DIAC identity management strategy is a comprehensive strategy designed for implementation across the department's processes, aligned and in conjunction with the whole-of-government approach to managing identity, and in a manner that is compatible with international developments and requirements.