Tasmanian Government
Identity and Access Management Toolkit

Part 1
Assessing Identity Risk Guidelines
Contents

Assessing identity risk .............................................................................................................. 5

Step 1– Determine business requirements ............................................................................. 7

Step 2 – Determine Access Assurance Level ......................................................................... 11

Step 3 – Determine Identity Registration Assurance Level .............................................. 23

Step 4 – Determine Credential Assurance Level ................................................................. 33

Step 5 – Perform Cost Benefit Analysis .............................................................................. 39

Step 6 – Implement Business Processes ............................................................................... 47

Step 7 – Review ...................................................................................................................... 47
Assessing identity risk

Different types of government services face different levels of risk. For example, services involving sensitive information or financial transactions face the risk of more severe consequences if the information is misused than other less sensitive services.

The higher the risk a service faces, the more assured the service owner needs to be that only authorised people are accessing the service delivery information. This concept is expressed in the Identity and Access Management Toolkit as the Access Assurance Level, which must be commensurate with the level of risk identified for the particular service.

It is important for Government agencies to provide a level of access assurance that is appropriate for the service involved. This is necessary for the proper functioning of the service, as well as for preventing improper use and fraud. It is also necessary to ensure that agency risks are managed and clients are protected.


In most cases, agencies will undertake two processes to ensure an applicant meets the required level of assurance to utilise their service: initial registration and subsequent verification. In assessing these aspects, an agency must ensure that the level of registration assurance and the level of verification assurance are equal to or higher that the required level of access assurance.

On this basis, the Toolkit involves establishing the level of risk for a service and translating this level across three areas:

1. Access assurance
2. Identity registration assurance
3. Credential assurance (ie subsequent verification)

Part 1 of the Toolkit is intended to be applied by an agency business unit in assessing the business processes to be applied for a particular service. It takes a seven step process to determine relevant assurance levels for a service, as illustrated in the diagram overleaf.
Guidelines for completing each individual step are detailed in the following pages.
Step 1
Determine Business Requirements

At the completion of Step 1, you will have:

- Reviewed the business requirements associated with the service you are assessing
- Considered the intended service delivery channel and how this will impact on your business requirements
- Considered Personal Information Protection legislation and its impact on your service delivery
- Considered whether there is a need to share information with other agencies or bodies
- Considered any other legislation that may impact on your service delivery

The Worksheet at the end of this Toolkit will assist you to complete these steps.

The first step in understanding access assurance is to ensure that the business requirements for that service are accurately identified. All future steps in the Identity and Access Management Toolkit are reliant upon these business requirements, so it is important that they are accurate and complete. Failure to correctly identify the business requirements can result in a higher or lower level of assurance being implemented than is necessary. This could result in an unwarranted increase in implementation and maintenance costs, or an increase in the identity risk associated with a service.

Service delivery channels

A service delivery channel is the way in which services are provided or transactions are conducted. There are many different types of channels, which can be grouped into three main types.
Physical Delivery Channels

Physical delivery channels are those that involve non-electronic channels. These include face-to-face interactions between the client and the agency, or the movement of physical documents through the post. These channels usually involve paper-based forms as a means of verification, which incorporate a signature, or they may require a visual or knowledge-based credential verification. The primary physical delivery channels are via mail or through a service counter.

Voice Delivery Channels

These are telephone-based service delivery channels, which can use operators, or be automated through voice recognition and response systems, or through the use of interactive menus.

Data Delivery Channels

Data-based delivery channels are those that are delivered electronically and generally do not require any human interaction on behalf of the agency. Common channels include the Internet, private networks, public kiosks or mobile links. These channels require the user to have a credential (eg a password or PIN) that can be remotely verified, typically using the data channel. It is vitally important to consider the security of the information being delivered through these channels, as the threats to electronic data delivery channels can be significant.

Multi Channel

A multi-channel environment is one where a single business service is made available through several different channels. For many reasons, it is important that government clients have a choice of the service delivery channel. Consequently, many government services are made available through multiple channels (service counter, call centre and web is a common combination). The identification of the service delivery channel composition is important in determining appropriate credential and verification process.

Different channels will require different methods to verify returning clients. For example, a different verification procedure may be used to verify a client using a web channel (eg user-ID and password) from that used for over-the-counter services (eg presentation of a photo identification card and check of a signature).

The different ways of verifying credentials may provide different levels of assurance. What is important is that the different processes used in various forms and channels meet the minimum access assurance level required. For example, the access assurance gained from showing a photo identification document (such as a driver's licence) in person may be higher than actually needed for the service, but this does not mean that other channels have to meet this higher standard.

Determining a Credential Assurance Level is dealt with in more detail in Step 4.
Public preferences for service channels

The report *Australians’ Use of and Satisfaction with E-Government Services (2007)*, commissioned by the Australian Government Information Management Office, may be useful when considering the design and delivery of a service and the selection of appropriate service delivery channels. The survey provides detailed information on household computer and Internet access and usage. The 2007 survey included questions regarding people’s preferences for accessing Government information and services. The full survey report may be accessed online via the Australian Government Information Management Office website at www.finance.gov.au/publications/interacting-with-government/index.html

Personal Information Protection (PIP) legislation

An individual’s privacy is an important consideration when establishing a service. *The Personal Information Protection Act 2004* regulates the collection, maintenance, use and disclosure of personal information by personal information custodians (ie the Tasmanian public sector, local government authorities and the University of Tasmania). The Act requires agencies to follow the Personal Information Protection Principles (PIP Principles) about how individuals’ personal information is collected, stored, used and disclosed.


The PIP Principles require agencies to be discriminating and purposeful in collecting personal information about individuals.

The PIP Principles provide an important perspective for the implementation of sound identity and access management processes. Using appropriate processes for a given type of transaction helps the agency fulfil these Principles. By reaching the required level of access assurance concerning the validity of a claimed identity, an agency can be sure that a proposed disclosure of personal information will be made for its intended purpose and not inadvertently for another purpose, or to a third party-impostor or a third party.

The PIP Principles also present challenges for identity and access management processes. When determining an appropriate identity registration assurance level under the Identity Enrolment Guidelines (Part 2), agencies must consider whether collection of real-world identifiers (such as an individual’s real name, residential address, date of birth, etc, for linkage with an assigned unique identifier) accords with PIP Principle 1, which specifies that personal information may only be collected where it is necessary for one or more of its functions or activities.

Before determining the identity and access management requirements for a service or entitlement, agencies should undertake an assessment of the potential impact of the provisions of the Personal Information Protection Act.

Opt in / opt out and information accessibility

Generally speaking, it is the client’s choice as to which service delivery channel they use. As electronic service delivery becomes more widespread, agencies must ensure that clients choosing not to use such channels (due to lack of infrastructure or concerns regarding privacy) are not disadvantaged.
When a client chooses to opt out or not opt in to a service delivery channel, the same level of access to information must apply regardless of which alternative service channel they choose.

It should be noted that the choice of service delivery channel might raise privacy issues for clients. Some people may feel that registering for electronic service delivery could invade their privacy (e.g., because an email address is required to receive information), particularly if the same service delivered over a counter does not require them to leave an email or contact address.

**Information sharing**

Agencies must, when registering users (involving collecting personal identification and contact information) follow the PIP Principles. In line with these Principles, information gathered during the registration process must not be shared with other agencies or business partners unless the client’s permission to do so has been obtained.

Likewise, when recording transaction details in relation to services provided, agencies must protect this data and not make it available to other agencies or commercial entities in a way that a client's transaction profile could be constructed. Any data that might be shared with another agency must be depersonalised or aggregated so that an individual's identity is not discernable where their consent has not been obtained.

Additionally, where multiple agencies are using the one identity and access management infrastructure, each agency must only access the identity information they have collected. The ability to access other client information that was not collected by the agency is prohibited unless the client's consent to do so has been obtained.

**Legislation**

Agencies should understand the relevant legislative constraints relating to the delivery of a specific service. For example, is there a requirement under legislation to:

- Ensure anonymity?
- Provide access to a particular transaction or a piece of information?
- Provide an official receipt?
- Store and retrieve a history of dealings with a specific client?
- Make a transaction legally binding?

These questions are important for determining the Access Assurance Level (see Step 2).
Step 2
Determine Access Assurance Level

At the completion of Step 2, you will have:

- Considered the Information Security Classification Level (ISCL) of the service you are evaluating (if applicable) and determined the associated Access Assurance Level (AAL)
- Undertaken a risk assessment to determine the AAL by:
  - Considering possible threats to the service you are evaluating
  - Identifying potential impacts that could result from an identity and access management failure and assessing the Impact Severity for each
  - Assessing the likelihood of harm for each consequence
  - Calculating the identity risk using the matrix at Table 5 for each impact and establishing an overall risk for the service based on the highest risk indicated
  - Determining the AAL using the matrix at Table 6
- Compared the AAL based on the ISCL (if applicable) and the AAL based on the risk assessment and chosen the highest as the AAL to be used throughout the rest of the Toolkit

The Worksheet at the end of this Toolkit will assist you to complete these steps.

Access assurance indicates the level of confidence the agency has, based on the premise that the client using a service is in fact the client registered to access that service. In addition, the higher the level of assurance, the greater the level of confidence can be held that the real world identity of the client is known.

The Toolkit proposes five Access Assurance Levels (AAL), as described in Table 1.
Table 1: Access assurance levels

<table>
<thead>
<tr>
<th>Access Assurance Level (AAL)</th>
<th>AAL-0</th>
<th>AAL-1</th>
<th>AAL-2</th>
<th>AAL-3</th>
<th>AAL-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Assurance</td>
<td>No assurance</td>
<td>Minimal Assurance</td>
<td>Low Assurance</td>
<td>Moderate Assurance</td>
<td>High Assurance</td>
</tr>
<tr>
<td>Low confidence is required in the client’s identity</td>
<td>Minimal confidence is required in the client’s identity</td>
<td>Low confidence is required in the client’s identity</td>
<td>Moderate confidence is required in the client’s identity</td>
<td>High confidence is required in the client’s identity</td>
<td></td>
</tr>
</tbody>
</table>

Access assurance levels are a composite of many factors. The Toolkit provides a methodology for setting the appropriate levels based on:

- The Information Security Classification Level, if applicable; and
- An assessment of the risk associated with access management failure;
- Performing a final cost benefit analysis step to ensure business needs are being appropriately met.

**Information Security Classification Level**

Many services provide information to clients, or the ability to change information recorded in systems. The information involved in these services should have been assessed for an Information Security Classification Level, which can be used to guide the Access Assurance Level (see the *Tasmanian Government Information Security Framework, Section 3 – Record Security Guidelines* available at [www.egovernment.tas.gov.au](http://www.egovernment.tas.gov.au) for further information; more detailed classification guidelines are currently under development by the Department of Premier and Cabinet).

Information security classifications and access assurance levels will generally align – that is, the higher the information security classification, the greater the level of access assurance required.

Table 2 shows the determination of the Access Assurance Level based on the information security classification assessment. Note that this assessment is to be performed based on the most highly classified information accessed by the service.

Table 2: Determination of Access assurance level based on Information Security Classification Level

<table>
<thead>
<tr>
<th>Information Security Classification Level</th>
<th>Public</th>
<th>Unclassified</th>
<th>In Confidence</th>
<th>Protected</th>
<th>Highly Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AAL-0</td>
<td>AAL-1</td>
<td>AAL-2</td>
<td>AAL-3</td>
<td>AAL-4</td>
</tr>
</tbody>
</table>

Access Assurance Level (AAL)
Access management failure risk assessment

The level of access assurance required by a service is influenced by the impacts that may arise as a result of an access failure. The greater the level and probability of an impact occurring and the greater that impact is likely to have, the higher the level of access assurance will be.

The level of access assurance provides guidance on appropriate measures to reduce the risks and impacts that may be caused by a failure in access management. It is important to ensure that the level of assurance is appropriate to the business service, as increased levels of assurance are likely to increase the cost of the access management solution.

The risk assessment process outlined below will help ensure the correct access assurance levels can be determined and help to balance the cost of implementation against the benefit gained.

Risk is determined by considering two dimensions: the impact of a particular threat and the likelihood of that threat occurring.

A total security risk assessment of a service or system carried out by risk practitioners is concerned with assessing the likelihood of harm arising from a threat. They consider many more aspects than just an identity risk assessment.

It is paramount that the following identity and access management risk assessment is not used to replace a comprehensive security risk assessment of services and that the difference between these two risk assessments is understood. For more information on a complete information security risk assessment see the Tasmanian Government Information Security Framework, Section 8 – Risk Management Guidelines (available at www.egovernment.tas.gov.au).

The identity risk assessment described in the Toolkit is based on the ordinal risk model outlined by AS/NZS 4360:2004, Risk Management (available at www.standards.com.au). This risk assessment should be incorporated into an agency’s overall risk management process and is only part of a whole-of-service risk assessment.

A risk assessment estimates the ‘impact severity’ that may result from an access management failure and the probability of there being an occurrence of harm as a result of that failure. The combination of impact severity and the corresponding probability determines the level of access assurance required.

A risk assessment attempts to identify any event or circumstance that has the potential to cause harm (ie a consequence or impact) that may arise due to an access management failure. The severity of the potential harm is estimated using the Impact Assessment Matrix (Table 3). For each circumstance, the probability of its occurrence is estimated using the consequence – probability rating matrix. These two values (the impact severity rating and its probability rating) are combined to obtain the overall risk level associated with access management failure on the service being evaluated.
Agency risk programs

An identity risk assessment should be included in any current agency risk program and practices. If an agency wishes to use its current risk program and practices for assessing identity risk, it is important to ensure that the assessment used can be mapped to the identity risk process. This will ensure that the access assurance levels determined are equivalent to levels determined in other agencies, thus allowing for easier interoperability.

Threats

Included below is a discussion of the possible identity and access related threats involved in service delivery. This should help inform an agency’s assessment of impacts and the probability of those impacts occurring.

There are a number of threats to information stored by agencies. When assessing the identity and access related risk of a service, it is important to consider the boundaries of the agency’s identity and access management processes. The identity and access management processes of a system or business process are only responsible for ensuring the successful registration, identification and verification of a client to access a service.

There are two main categories to consider when assessing the level of threat to information in the event that an agency’s identity and access management processes fail: intentional and non-intentional.

*Intentional threats*

Intentional threats can include fraudulent activities that are intentionally attempting to gain unauthorised access to information in order to conduct a range of illegal activities. Fraudulent activities may be for personal financial gain; to discredit the reputation of a third party; to cause distress, embarrassment and inconvenience to others; to commit violent acts; or to illegally establish an identity to conduct criminal activities.

It is important to note that an agency may be the key target of fraudulent activity, or could be subjected to attacks and information gathering in order to conduct a fraudulent activity against a client.

*Non-intentional threats*

Generally, within the context of identity and access management, non-intentional threats relate to an authorised client who is registered, identified and verified to transact with an agency. Information may be received that is not related to their transaction as a result of an accidental disclosure due to mistaken identity. An example could be where a staff member of the agency unintentionally provides information to a client who has similar attributes to another.

The main difference to intentional threats is that the entity that receives the unauthorised information in this non-intentional manner may or may not use that information for a purpose other than it was initially collected. This may depend on who received the information, the level of sensitivity surrounding the information and the probability for personal gain as a result of receiving the information.
Impact assessment

Within the context of the Toolkit, when determining risk, the approach to assessing impact severity is to assume that there are no access controls currently protecting the service and to evaluate the risk that this 'open door' would pose. This is very important, since if suitable verification is factored in and operating correctly, there should always be 'negligible risk' from the verification-related aspects of a service and such a result would be meaningless for determining the correct Access Assurance Level.

The question to be evaluated is: 'if access to this service / transaction was to be given to a person who should not have that access, what impact could result?' The likelihood of the impact occurring is not taken into account when determining impact severity.

It is important to ensure that agencies assess the impact of the release of information as well as the impact of allowing an unauthorised person to modify or change information stored in systems. The assessment of risk can also make use of existing information, statistics or trends from pertinent information, which may be available from an agency's own data or another source known to the agency. Regardless of the availability of qualitative information, it will never be possible to provide a completely qualitative assessment of all impact types and in particular impacts such as public order or government policy.

The Impact Assessment Matrix at Table 3 is to be used when assessing the severity of impacts that may arise for a service as a result of an access management failure. The matrix outlines possible considerations agencies may make when assessing each impact type. Agencies may have other considerations when assessing those impacts. It might be useful for agencies to develop their own guidelines on the considerations that may apply to each impact type.

The following are important notes about the Matrix:

- The impact severity ratings used here are based on similar information contained in the Australian Government Authentication Framework (AGAF 2005). The main difference is that this table adds a 'no impact' level, so that the Toolkit can address services that do not require any form of verification.
- The risk levels and descriptors (eg minimal, minor etc) used in the matrix and throughout the Toolkit are those used in the AGAF and may vary from those used in other risk assessments within Tasmanian Government agencies. The use of the AGAF levels is deliberate to ensure alignment between AGAF and the Toolkit.
- The Impact Assessment Matrix is based on the AGAF table 'Criteria for determining risk assurance levels' and is provided as a guideline only. For example, it is not possible to provide clear definitions applicable in all circumstances of assessments such as 'short term distress' or 'limited long term distress'. These descriptions are provided to assist agencies in their consideration of severity, but cannot be prescriptive.
- The impacts identified are generic in nature to enable the broadest possible application. Agencies may find that some impact types are not relevant to their particular business and that other impact types that are relevant are not included within the table. Agencies are encouraged to adapt the table to suit agency business and risk management requirements, while being mindful of the need to preserve the original intent of the impact assessments.
The determination of risk is not merely a mechanical computation. Stakeholders need to apply their judgement based on the unique factors associated with the agency’s business, the nature of the user base, the overall environment and the transaction aspects (This paragraph is substantially reproduced from the AGAF ‘Implementation Guide for Government’).
## Table 3: Impact Assessment Matrix

<table>
<thead>
<tr>
<th>Impact</th>
<th>Possible Considerations</th>
<th>Impact Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Lowest: None, Minimal, Minor, Moderate, Substantial</td>
</tr>
<tr>
<td>Risk to any party’s safety</td>
<td>Consider any risk of any injury or impact on safety, as well as the possibility of loss of life. An example might be someone being registered for a job that they should not have been because they were not appropriately qualified (e.g., unqualified truck driver who causes an accident which injures or kills someone), or are prevented by previous criminal history. Other examples might include release of names or locations of undercover officers, people under protection orders, etc.</td>
<td>None, Minimal, Minor, Moderate, Substantial</td>
</tr>
<tr>
<td>Distress caused to any party</td>
<td>From the client’s or the public’s point of view, many things, including denial of expected services, could cause distress. From an agency’s point of view, potential impacts might be minor or major rework or reprocessing of the transaction, through to stress impacts on employees and possible loss of jobs or major reorganisation forced by the inappropriate access.</td>
<td>None, Minimal - Short term distress, Limited long term distress, Substantial long term distress</td>
</tr>
<tr>
<td>Damage to any party’s standing or reputation</td>
<td>Issues to consider include potential for adverse publicity, either locally or more widely and the potential for damage to either the agency’s or the client’s ongoing reputation. If an incorrect decision was made or inappropriate access to information was granted etc, would it be of interest to the media?</td>
<td>None, Minimal - Short term damage, Limited long term damage, Substantial long term damage</td>
</tr>
<tr>
<td>Inconvenience to any party</td>
<td>From a client’s point of view, consider factors such as causing the client to reapply for a service or entitlement, denial of service provision, delays in service provision. From an agency’s point of view, consider factors such as job stress caused by the failure, loss of jobs, re-work or reprocessing. For example, the need to recall and reissue licences / tickets or registrations.</td>
<td>None, Minimal inconvenience, Minor inconvenience, Significant inconvenience, Substantial inconvenience</td>
</tr>
</tbody>
</table>
**Part 1 – Assessing Identity Risk Guidelines**

<table>
<thead>
<tr>
<th>Impact on public order</th>
<th>Need to consider whether disclosure of information could pose a threat to community relations and public order. This might occur when information is released that can cause alarm in a way that then results in damage to public order. For example, disclosure of an offender’s identity or whereabouts where the community could then react and disturb public order.</th>
<th>No Impact</th>
<th>Impact</th>
<th>Prejudice</th>
<th>Seriously prejudice</th>
</tr>
</thead>
</table>

| Release of personally or commercially sensitive data to third parties without consent | Could information that should not be made public be released? For example, medical records, commercially sensitive information that could impact on current or future business, personal information that should be protected from release. | No impact | Would have no significant impact | Measurable impact, breach of regulations or commitment to confidentiality | Release of information would have a significant impact | Would have major consequences to a person, agency or business |
| Impact on government finances or economic and commercial interests | Would disclosure of information result in financial or economic consequences to government? Release of information may result in financial gain or loss. For example, disclosure of planning decisions which could result in changing valuations. | No Impact | Cause financial loss or loss of earning potential | Work significantly against | Substantial Damage |

| Financial loss to any client of the agency or other third party | Consider this from the client's perspective - what losses could they incur? Consider the possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by changing ownership details), payments being made to the wrong party (eg a grant or benefit), etc.. The amounts to be considered are suggested as: Minimal <$50, Minor $50-$200, Significant $200-$2,000 and Substantial ≥ $2,000, but these figures here guidelines only based on impact on an ‘average’ individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted to something more akin to the figures used for financial loss to the agency. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients. | None | Minimal | Minor | Significant | Substantial |

| Financial loss to agency | Consider this from the agency’s perspective - what losses could they incur? Considerations include possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by changing ownership details), payments being made to the wrong party (eg a grant or benefit) etc | None | Minimal < 2% of monthly agency budget | Minor 2% – < 5% of monthly agency budget | Significant 5% – < 10% of monthly agency budget | Substantial ≥ 10% of monthly agency budget |
### Part 1 – Assessing Identity Risk Guidelines

<table>
<thead>
<tr>
<th>Threat to government agency’s systems or capacity to conduct their business</th>
<th>Would an access management failure of this transaction have the potential to reduce or prevent an agency or external party conducting their business? For how long would this reduction / prevention last? Could data be inappropriately damaged? How extensively? Could systems be made inoperable? The period here may vary from agency to agency – some agencies may be able to endure a halt in business for a number of days without serious impact on the government or society. Others more directly involved in public safety and similar services would be less tolerant of outages.</th>
<th>No threat</th>
<th>Agency business or service delivery impaired in any way</th>
<th>Agency business halted or significantly impaired for a sustained period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistance to serious crime or hindrance of its detection</td>
<td>Would an access management failure of this transaction have the potential to assist in the conduct of a crime? This might include release of information enabling the planning of a crime, the creation of a false identity, or change to information that may help prevent the detection of a crime.</td>
<td>Would not assist in, or hinder detection of unlawful activity</td>
<td>Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts</td>
<td>Impede investigation or facilitate commission of serious crime</td>
</tr>
<tr>
<td>Impact on development or operation of major government policy</td>
<td>Would disclosure cause embarrassment to Government in the stages where policy is being formulated? The impact may be that a major policy initiative will not proceed.</td>
<td>No impact</td>
<td>Impede effective development or operation</td>
<td>Seriously Impede</td>
</tr>
</tbody>
</table>
Likelihood of harm

Whether an individual or group receives unauthorised information through intentional or non-intentional means, harm may or may not result, depending on the nature of the information released and the intent and actions of the recipient of this information. Thus, when assessing the level of risk from a threat, it is necessary to assess the probability of there being any harm from each impact as a result of the access controls failing. In other words, how probable (or likely) is it that the possible impact identified will actually occur?

The probability rating shown in Table 4 should be used in this assessment. Each probability rating has been given a guideline percentage to assist in its application. This is a rating of the probability that someone (client, agency, member of the public or other organisation) will suffer harm as a consequence of a failure in access management. So, the question is: Given an instance of access management processes failing, how probable (or likely) is it that the impact identified will actually be incurred? This is a different style of probability assessment than that commonly used in an information security context.

In making an assessment, it should be noted that the probability of an impact occurring might be linked to a person’s motivation. In other words, where there is a potential for financial gain, the probability of that impact occurring is likely to be high.

Table 4: Consequence Probability Rating

<table>
<thead>
<tr>
<th>Probability Rating</th>
<th>Definition</th>
<th>Guideline Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>It is almost certain that an impact will occur from a failure in access management processes</td>
<td>95-100%</td>
</tr>
<tr>
<td>Likely</td>
<td>It is likely that an impact will occur from a failure in access management processes</td>
<td>50-95%</td>
</tr>
<tr>
<td>Possible</td>
<td>It is possible that an impact will occur from a failure in access management processes</td>
<td>10-49%</td>
</tr>
<tr>
<td>Unlikely</td>
<td>It is unlikely that an impact will occur from a failure in access management processes</td>
<td>1-9%</td>
</tr>
<tr>
<td>Rare</td>
<td>It would be rare that an impact will occur from a failure in access management processes</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

Identity risk

Table 5 outlines a matrix that can be applied to determine identity risk. For each consequence or impact, the identity risk can be graded by locating the intersecting ranking of Impact Severity and Probability.
Table 5: Determining identity risk

<table>
<thead>
<tr>
<th>Probability</th>
<th>Impact Severity</th>
<th>Probability rating</th>
<th>Identity Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Minimal</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Almost Certain</td>
<td>Negligible</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td>Likely</td>
<td>Negligible</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td>Possible</td>
<td>Negligible</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Negligible</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td>Rare</td>
<td>Negligible</td>
<td>Minimal</td>
<td>Low</td>
</tr>
</tbody>
</table>

When determining the overall identity risk, each individual impact must be subjected to the risk assessment process. It is possible for lower impacts to be a higher risk due to a higher probability. The final identity risk to be used in subsequent steps in these Guidelines is the highest risk grading indicated by any of the impacts. The Worksheet at the end of the Toolkit can be used for this.

**Worked example**

In the following example, one impact has been rated as high risk. Therefore, the risk level which needs to be managed, and therefore should be used in the rest of the Guidelines, is ‘High’.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Impact Severity</th>
<th>Probability rating</th>
<th>Identity Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk to any party’s safety</td>
<td>None</td>
<td>Rare</td>
<td>Negligible</td>
</tr>
<tr>
<td>Distress caused to any party</td>
<td>Moderate</td>
<td>Almost Certain</td>
<td>Moderate</td>
</tr>
<tr>
<td>Damage to any party’s standing or reputation</td>
<td>Moderate</td>
<td>Likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>Inconvenience to any party</td>
<td>Substantial</td>
<td>Possible</td>
<td><strong>High</strong></td>
</tr>
<tr>
<td>Impact on public order</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>Release of personally or commercially sensitive data to third parties without consent</td>
<td>None</td>
<td>Rare</td>
<td>Negligible</td>
</tr>
<tr>
<td>Impact on government finances or economic and commercial interests</td>
<td>Minimal</td>
<td>Unlikely</td>
<td>Minimal</td>
</tr>
<tr>
<td>Financial loss to any client of the agency or third party</td>
<td>None</td>
<td>Rare</td>
<td>Negligible</td>
</tr>
<tr>
<td>Financial loss to agency</td>
<td>Minimal</td>
<td>Possible</td>
<td>Minimal</td>
</tr>
<tr>
<td>Threat to government agency’s systems or capacity to conduct their business</td>
<td>None</td>
<td>Rare</td>
<td>Negligible</td>
</tr>
<tr>
<td>Assistance to serious crime or hindrance of its detection</td>
<td>None</td>
<td>Rare</td>
<td>Negligible</td>
</tr>
<tr>
<td>Impact on development of operation of government policy</td>
<td>Minimal</td>
<td>Possible</td>
<td>Minimal</td>
</tr>
</tbody>
</table>
Final Access Assurance Level

The final Access Assurance Level to be used in the remainder of the Toolkit process is determined by comparing the Access Assurance Level from the risk assessment with that from the information security classification assessment and selecting the highest Access Assurance Level determined by these two processes. Table 6 shows the determination of the Access Assurance Level based on the risk assessment.

<table>
<thead>
<tr>
<th>Identity risk level</th>
<th>Access assurance level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>AAL-0</td>
</tr>
<tr>
<td>Minimal</td>
<td>AAL-1</td>
</tr>
<tr>
<td>Low</td>
<td>AAL-2</td>
</tr>
<tr>
<td>Moderate</td>
<td>AAL-3</td>
</tr>
<tr>
<td>High</td>
<td>AAL-4</td>
</tr>
</tbody>
</table>

The following examples may help to explain why both measures (risk and information security classification level) are used:

- A service that licences someone to operate heavy equipment may only contain information of an in-confidence classification (some personal details, perhaps, but nothing which needs a protected level of security classification), which would lead to an Access Assurance Level-2 rating using the information security classification assessment. However, due to the potential for harm which may occur if a person were incorrectly licensed to operate this equipment, the risk assessment may indicate moderate risk (due to the potential of someone being incorrectly granted and using a licence), which would thus in turn indicate an Access Assurance Level-3 rating was required.

- Likewise, it is also possible that a service may be evaluated with a low risk assessment, but in fact it provides information classified as highly protected. In theory, this would be unlikely to occur often, as the classification of information is based itself on a similar risk assessment process.
Step 3
Determine Identity Registration Assurance Level

At the completion of Step 3, you will have:

- Analysed your business requirements and determined which identity registration level (IRAL) should be applied to the service
- Referred to Table 7 to ensure the determined IRAL reflects your business needs
- Considered the proof of identity (POI) documents required to support your nominated IRAL
- Finalised the IRAL and drafted the business requirements

The Worksheet at the end of this Toolkit will assist you to complete these steps.

The overall Access Assurance Level (AAL) for a given service would be a combination of the assurance provided by the registration process and that provided by the credential verification process that occurs with each service delivery.

The Identity Registration Assurance Level (IRAL) indicates the level of confidence an agency requires in the registration of a client. The higher the level of confidence required, the greater the evidence of the client’s identity the agency needs during the registration process. This allows the agency to be confident that the identity being registered is in fact a real world entity.

Depending on the level of access assurance required, the registration process needs to defend itself against an applicant impersonating an identity and possibly against repudiation of the registration process.

The IRAL will generally be at the same level as the Access Assurance Level, which was determined in Step 2. However, the level of identity registration assurance indicated by the Access Assurance Level may not be feasible for an agency in terms of cost or complexity of delivery. This may indicate that the Access Assurance Level should be reassessed.
It is important to note that if the risk assessment suggests an AAL-4, the identity registration processes cannot be at a lower level. If this situation arises, Step 2 should be undertaken again to determine whether the AAL has been correctly assessed.

Table 7 indicates the Identity Registration Assurance Levels that are used in the Toolkit.

### Table 7: Identity Registration Assurance Levels

<table>
<thead>
<tr>
<th>Identity Registration Assurance Level (IRAL)</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| IRAL-4 High Risk                           | High level verified identity  
Substantial evidence of the real-world identity is required and verified. External checks must be performed on the evidence of identity and the person is required to be physically present at the registration authority during registration.  
Requires the taking of a biometric (such as a photograph) during registration to ensure non-repudiation of the registration process. | Used when a high level of confidence is required in the registration process, the identity needs to be linked to a real-world client and non-repudiation of the registration process is required.  
Does not support remote registration (ie registration conducted electronically or over the phone) due to the need for the client to be physically present at the registration authority. |
| IRAL-3 Moderate Risk                       | Moderate level verified identity  
Moderate evidence of the real-world identity is required and verified. External checks should be performed on the evidence of identity. | Used when the identity needs to be directly linked to a real world client and the transaction indicates it is legally binding (ie service delivery non-repudiation is supported at a moderate level). |
| IRAL-2 Low Risk                            | Low level or basic identity  
Some minimal evidence of real-world identity is provided during the registration process. The registration authority knows the client's real-world identity and hence transactions can be verified against a real world identity if required. | Used when the service requires the client to be specifically identified during the conduct of transactions or the registration process and only low levels of access assurance are required.  
Used, for example, when registering for a low risk service that requires eligibility criteria to be met (eg age, qualifications, etc). |
| IRAL-1 Minimal Risk                        | Pseudonymous or Self-Registered identity  
Registration is performed but no proofing is carried out on the data. The registration would usually be performed by the client (ie self-registration), but may be performed by the agency or third party registration authority.  
Does not require real-world identity registration data. The client could identify using any name or data they wished and thus create a pseudonym. | Useful for recognising return visits to the service, even though the individual entity remains unknown (eg where a client’s return visits automatically load personal preferences linked to a pseudonym).  
This level also supports a form of further contact so the client can be further contacted if required, but there is no support for non-repudiation or for knowledge of the real-world identity of the client.  
An example would be where a client has registered an email address that cannot be converted to a real-world identity, but is sufficient to allow information to be sent or continue further interaction. |
| IRAL-0 No Risk                             | Not Identified – anonymous  
No registration and hence no identification is performed. | Supports requests for information that is freely available, such as access to online information about government programs or services.  
Generally, public information that is freely available. |
Business requirements analysis

There are specific business requirements that need to be established before an agency can fully establish the required Identity Registration Assurance Level for a service as the business requirements will guide the appropriate choice of registration level. Information gathered in Step 1 will assist in informing this step.

Higher Identity Registration Assurance Levels generally imply more invasive registration processes, which may hinder the take-up of a service by clients and may limit the choice of service delivery channels. For example, in the case of the provision of information on a website, clients are generally happy to download information where it is available without any registration. Many clients would be happy to provide a simple email address before downloading the requested information, although some would not be. However, a significant number may not be willing to provide information such as home phone number, name, or street address before gaining access to the information.

When deciding on what type of identity registration is required for a service, the following questions should be taken into consideration. The information on the following pages will help you determine your responses to these questions. You can record your responses in the Worksheet at the end of this Toolkit.

- Is there a legislative or policy need to ensure anonymity?
- Is it important that the agency is unable to identify the real-world identity of the client?
- Does the agency need to make future contact with the client?
- Is the information being provided restricted in anyway?
- Are there privacy considerations?
- Is it acceptable if the information is provided to anyone / everyone?
- Is there a need for payment?
- Does the payment need an official receipt?
- Does the receipt require identifying data?
- Does the agency need to keep a record of payments made by a client?
- Do payments and receipting require knowledge of the real-world identity of the client?
- Is there a need to store and retrieve a history of dealings with a specific client?
- Is the transaction legally binding?
- Is non-repudiation of the registration process and service delivery required?
- Does the client require access to a particular transaction or a piece of information?
- Does the client need to have particular attributes (eg be of a certain age or have certain qualifications)?

Table 8 shows how the different Identity Registration Assurance Levels support different business requirements. This table can be used as a basis for the selection of the correct Identity Registration Assurance Level based on the gathered business requirements and the previous assessment of Access Assurance Level.
Part 1 – Assessing Identity Risk Guidelines

There can be more than one suitable Identity Registration Assurance Level for a given set of business requirements, particularly where the business requirements are not particularly demanding. On these occasions, an informed choice can be made.

Table 8: Identity Registration Assurance Levels Business Capabilities

<table>
<thead>
<tr>
<th>Identity Registration Assurance Level (IRAL)</th>
<th>Client Anonymity Maintained</th>
<th>Allows Contactability and Service History and Personalisation</th>
<th>Real World Identity link, service delivery non-repudiation</th>
<th>Supports overall Access Assurance Level &gt; 2</th>
<th>Supports Non-repudiation of registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRAL-4 High</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IRAL-3 Moderate</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IRAL-2 Low / Basic</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IRAL-1 Pseudonymous or Self Registered</td>
<td>Yes by Pseudonym</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IRAL-0 No registration</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Terms used in the table above are expanded and explained in the following sub-sections.

Third party registration authorities

An agency is not constrained to registering clients themselves and may use a third party to perform the registration process. The third party registration authority will receive all evidence of identity on behalf of the client and verify their authenticity against the requirements of the agency. The agency is provided with an identity that has been fully verified by the third party, allowing the agency to trust the identity without having to perform the identity registration phase themselves.

It should be noted that third party registration is allowable at all Identity Registration Assurance Levels, although appropriate trust must be established between the third party registration authority and the agency, particularly at the higher levels of registration.

It is also important to note that a Tasmanian Government Agency may also be a third party providing the registration processes for other agencies or external organisations. This trust relationship needs to be understood as part of the requirement for establishing the Identity Registration Assurance Level.

Anonymity

When providing a service, it must be clearly defined whether the transaction requires a real-world identity to be known or not known to the agency. Where a real-world identity is not required (eg an IRAL-0 rating, which involves no registration and hence no verification), the transaction is simple and cheap to implement. Anonymous services can also assist in attracting public participation in a service that may have a social stigma attached, hindering utilisation.
Part 1 – Assessing Identity Risk Guidelines

Note that absolute anonymity can be supported by IRAL-0 (no registration required) and IRAL-1 (pseudonymous registration), but not by IRALs- 2, 3 or 4, which all require the real world identity to be known by the registration authority (see Alias or identity escrow). If IRAL-0 is the identified registration assurance level required, the following checklist should be reviewed to ensure that the selection is correct.

- Confirm that the information provided by the transaction may be viewable to anyone (ie is it public domain?)
- Confirm that there is no need to know who the client using the service is, because there is no need for client follow up, no relation to other transactions, no history of transactions required, or there is no harm in communicating with an unknown client
- Confirm there is no need for the client to have a particular attribute to complete the transaction (eg does the client need to be of a certain age, or have certain licences or qualifications?)

It is also important to note that the use of shared logins or other credentials means that the identity of the person undertaking the transaction cannot be established and therefore considered IRAL-0.

**Pseudonym**

A pseudonym is an identity where only the entity that generated the pseudonym knows the real-world identity. As the real-world identity of the client using a pseudonym is not known to the agency, it may be used in some systems for privacy reasons as it provides an effective form of anonymity.

Some transactions can be completed successfully through the use of a pseudonym. Pseudonyms are used for transactions that require the agency to be able to remain in contact with the client without needing to know the details of the real-world entity (see Contactability). A typical example is a transaction that may involve registering to receive newsletters or information. In this situation, the client may create their own user-ID and password. This allows them to return and modify their preferences or remove themselves from the service, but there is no need for the agency to know the real name of the recipient of the information. The created user-ID forms a pseudonymous identity, which maintains client anonymity as the identity does not provide any link to a real-world identity.

**Alias or identity escrow**

An alias is an identity where the registration authority that generated the alias knows the real world identity of the entity, but provides the client with a different identity (termed here as an alias, but is in fact a form of pseudonym) that hides their real-world identity. An alias may be used in some systems for privacy reasons, or where the sharing of information is occurring with parties or organisations that are separate from the agency.

It is possible for an alias to be used at IRAL-2, 3 and 4, although this would be at the discretion of the agency and confirmed by an agreement between the third party registration authority and the agency.
It is important to note that the agency may only know the client by their alias. However, if required, the process may include a mechanism for gaining access to the real-world identity of the client through the third party.

The main difference between an alias and a pseudonym is that an alias is able to be traced back to a real world identity, so anonymity is not absolute and the agency can safely assume that the client identity has been verified by the registration authority.

Identity escrow occurs when a client uses a third party registration authority to establish and register their identity and the third party passes on an alias for the client (ie they keep the client's real-world identity hidden from the agency and provide some other identifier such as a client ID number) to the agency. Identity escrow may be used for various reasons, including the preservation of client anonymity while allowing the agency to know that a real-world entity does actually exist, even if the agency does not know that identity.

**Contactability**

Contactability is where the agency requires a mechanism to be in place to enable further correspondence with the client. For example, does the agency need to provide the client with further related material and/or regular updates or news?

This may be achieved simply by storing and using an email address or a postal address and may not require the client to use their real-world identity. Although, some process to capture the contact information is required.

Technically, a registration process involving the creation of a unique client identifier (eg user-ID) may not be required. The data collected may not necessarily need to be retained. For example, if a website is used to request that information be sent to a postal address, the address provided could be deleted once the information was sent. In a case like this, no registration or client identifier needs to be applied. Although, not doing so would prevent service history and personalisation functionality, as described below.

It is important to know if the transaction being analysed requires a contact capability. A requirement for being contactable necessitates some identity registration and verification to occur. The transaction will not be completely anonymous if there is a need for further contact, as the agency must know who it is interacting with. If there is no need for further contact, there may be no need for clients to identify themselves at all, which leads to the possibility of an anonymous identity category.

**Service history**

Similar in many ways to contactability is the requirement to maintain a service history. That is, does either the agency or the client need to trace repeat uses of the service so that a history of all services provided is retained? If so, the service cannot be completely anonymous and some level of registration, allocation of a unique client identifier and subsequent verification is required. In essence, by providing a unique client identifier, a method of associating multiple interactions is enabled.
Personalisation

The requirement to offer service personalisation is also similar to service history. This allows for a client’s preferences to be automatically loaded on repeat visits, or allows the agency to customise future interactions with the client to their specific needs or interests. In each case, a minimal level of registration requiring identification of the client is implied. A common example of a basic level of personalisation is used by many pizza delivery businesses, where the client provides a telephone number. This is stored in the agency’s database to provide information on the client’s name, address and even personal preferences for future visits by that client.

Real-world identity

Many transactions will require the agency to know the real-world identity of the client. This might be because there is a need to provide an official receipt for payment that identifies the client, or a need to know something about the client (such as their age) in order for them to qualify for the service, or for other legal reasons. If a real-world identity link is required, registration at a minimum IRAL-2 must be completed by the agency or by a trusted third party registration authority to prevent fraud or misrepresentation. Self-registration cannot be used.

Non-repudiation of registration

Some transactions may require undeniable proof that the transaction has occurred involving a specific client. Non-repudiation controls are controls that are designed to prevent a client, as well as the agency, from being able to subsequently deny receipt or transmission of information or participation in a transaction.

The aspect of interest with non-repudiation here is the non-repudiation of the registration process itself. What is required is sufficient evidence to prevent either party from repudiating the registration.

A person may claim that they were not the person who was registered by the registration authority. This may occur when a dispute arises about inappropriate activity using a credential provided to a client. To prevent this situation arising, a biometric of some sort could be taken during registration, such as a photograph. If a dispute arises, the biometric can be checked against the client to determine if that person is in fact the same person who was registered by the registration authority.

Such levels of protection would not be required in all circumstances and hence the taking of a biometric during registration would be necessary for IRAL-4 and IRAL-3 registrations.

Service delivery non-repudiation

Service delivery non-repudiation is classed as non-repudiation that validates that the originator of the service sent a transaction, the transaction was not interrupted or corrupted in transit and the recipient received the transaction with full integrity. This does not necessarily imply that the transaction was conducted electronically. Service delivery non-repudiation can be achieved by the physical delivery of documents that have been signed by either party.

A high-level registration process, combined with a high level Credential Assurance Level (see Step 4) will provide a high level of service-delivery non-repudiation. In other words, this feature would make it difficult for a client or agency to deny involvement in a particular service transaction.
Non-repudiation of service delivery does not apply to IRAL-0 and IRAL-1 as there is no knowledge of who the client is. However, IRAL-2, 3 and 4 provide increasingly higher levels of confidence in the identity of the client who conducted a transaction.

**Proof of identity document requirements**

In registering clients, the agency or registration authority is required to assess that the proof of identity (POI) provided by the client meets the Identity Registration Assurance Level required. Issues that should be considered when choosing to use such evidence are dealt with more fully in **Part 2 – Identity Registration Guidelines and Standards**.

For individuals, biometric data can also be collected during the registration process and used later as evidence of who was registered and received the credential (eg as mentioned earlier, this could possibly support non-repudiation of registration).

To achieve the identity registration assurance levels, minimum POI requirements will be applied to the initial process of establishing the identity of the client, as indicated by Table 9. The suggested documentary requirements are provided in **Part 2 – Identity Registration Guidelines and Standards**.

**Table 9: Identity Registration Assurance Levels**

- **Negligible Risk**: Anonymous transaction that does not require the person to be identified
  - **IRAL – 0** (Nil points)
  - POI Assessment not required
  - Example: Cash transaction for a product, such as a map

- **Minimal Risk**: Pseudonymous transaction that does not require the person to be specifically identified, but does need contact details
  - **IRAL – 1** (Nil points)
  - POI Assessment not required
  - Example: Enrolment for a community information service

- **Low Risk**: Transaction that requires the person to be specifically identified with a medium level of assurance
  - **IRAL – 2** (50 points)
  - Some POI Objectives to be satisfied
  - Example: Enrolment and fee collection for a renewable service or permit

- **Moderate Risk**: Transaction that requires the person to be specifically identified with the highest level of assurance
  - **IRAL – 3** (100 points)
  - All POI Objectives to be satisfied
  - Example: Issuing a licence or permit that may be used as a commonly accepted identity document

- **High Risk**: Transaction that requires the highest level of assurance
  - **IRAL – 4** (150 points)
  - Gold Standard Enrolment process
  - Example: Issuing of very identity document, such as a Passport or a Visa
Verification

In some instances, particularly where a high level of assurance in an identity is required, verification of a credential that is submitted to support a claimed identity is appropriate. State government areas currently participate in national facilities that enable limited credential verification (e.g., the Certificate Validation Service for all births, deaths and marriage certificates, and the National Exchange of Vehicle Driver Information System for driver licence data), for which fees may apply. Details of these services are available from the relevant Tasmanian Government agencies, such as the Registry of Births, Deaths and Marriages, Department of Justice (www.justice.tas.gov.au/bdm) and Transport Tasmania, Department of Infrastructure, Energy & Resources (www.transport.tas.gov.au/home).

In other instances, credential issuing agencies may provide verification advice on request, generally for a fee or other consideration.

As part of the National Identity Security Strategy, the national Document Verification Service (DVS) will be established to enable State and Commonwealth Government agencies to verify key identity credentials including Australian passports, citizenship certificates, entry visas, Births, Deaths and Marriages Registry data, and driver licence data.

Further details on the DVS will be incorporated in Part 2 of the Toolkit when the service becomes operational.

**Document business requirements**

To complete this step and to draft the business requirements and processes for identity registration and ongoing management of this, refer to the section of Part 2 – Identity Registration Assurance Guidelines and Standards that is relevant to the IRAL you have identified.
As described in the Introduction to the Toolkit, the overall Access Assurance Level is achieved for a given service is a combination of the assurance provided by the registration process and that provided by the identity verification process, which is measured by the Credential Assurance Level (CAL).

The CAL determines the level of confidence an agency requires in the verification of a returning client. That is, the level of assurance or confidence the agency has that, when a client returns to the service, they are in fact the same entity that registered for the service.

The CAL will generally be at the same level as the Access Assurance Level, which was determined in Step 2. However, the level of credential assurance indicated by the Access Assurance Level may not be feasible for an agency in terms of cost or complexity of delivery. This may indicate that the Access Assurance Level should be reassessed.
It is important to note that if the risk assessment suggests an AAL-4, the identity registration and verification processes cannot be at a lower level. If this situation arises, Step 2 should be undertaken again to determine whether the AAL has been correctly assessed.

Table 10 details the Credential Assurance Levels and the level of confidence achieved through each level. The table also provides guidance on the capabilities of related credentials to ensure that the level of confidence is met.

**Table 10: Credential Assurance Levels**

<table>
<thead>
<tr>
<th>Credential Assurance Level</th>
<th>Confidence Provided</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAL-4</td>
<td>High Risk</td>
<td>The highest practical access assurance is required. Strong cryptographic authentication mechanisms must be used and authentication will require at least two factors.</td>
<td>A passport or visa</td>
</tr>
<tr>
<td>CAL-3</td>
<td>Moderate Risk</td>
<td>A moderate level of confidence in the authentication mechanism is required. Strong cryptographic authentication mechanisms must be used. Generally speaking, this level of authentication will require two factors.</td>
<td>A driver's licence or firearms licence</td>
</tr>
<tr>
<td>CAL-2</td>
<td>Low Risk</td>
<td>A low level of confidence in the authentication mechanism is required. The mechanism needs to prevent common forms of attack, such as: eavesdropper, replay and online guessing attacks. For example, a password over an encrypted link. However, strong cryptographic authentication is not mandatory.</td>
<td>A senior’s card</td>
</tr>
<tr>
<td>CAL-1</td>
<td>Minimal Risk</td>
<td>Authentication is performed, but there is little assurance placed upon it. For example, a challenge-response password mechanism.</td>
<td>Subscription to an information service</td>
</tr>
<tr>
<td>CAL-0</td>
<td>Negligible Risk</td>
<td>No authentication is performed. Included for completeness only, but does not represent any authentication process.</td>
<td>Cash transaction for a product, such as a map</td>
</tr>
</tbody>
</table>

The determination of the likely Credential Assurance Level is achieved by applying the matrix detailed at Table 11. This table identifies the minimum Credential Assurance Levels required for a particular service or transaction. Higher-level Credential Assurance Levels may be used provided the client has been given sufficient authentication credentials in the registration process.

Any unnecessary increase in the Credential Assurance Level will increase the costs of implementation without offering any significant benefit. The decision to increase the Credential Assurance Level should be carefully considered by the agency. During the cost-benefit phase (Step 5), the agency can assess if a higher level of Credential Assurance Level is desired or warranted.
Table 11: Minimum credential assurance level matrix

<table>
<thead>
<tr>
<th>IRAL</th>
<th>IRAL-0 (None)</th>
<th>IRAL-1 (Minimal)</th>
<th>IRAL-2 (Low)</th>
<th>IRAL-3 (Moderate)</th>
<th>IRAL-4 (High)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL-0</td>
<td>CAL-0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>AAL-1</td>
<td>CAL-0</td>
<td>CAL-1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>AAL-2</td>
<td>CAL-0 (1)</td>
<td>CAL-1</td>
<td>CAL-2</td>
<td>CAL-3</td>
<td>N/A</td>
</tr>
<tr>
<td>AAL-3</td>
<td>CAL-0 (1)</td>
<td>CAL-1</td>
<td>CAL-2</td>
<td>CAL-3</td>
<td>N/A</td>
</tr>
<tr>
<td>AAL-4</td>
<td>CAL-0 (1)</td>
<td>CAL-1</td>
<td>CAL-2</td>
<td>CAL-3</td>
<td>CAL-4</td>
</tr>
</tbody>
</table>

There may be occasions where the business requirements simply do not match. For example, a proposed service is designed and intended for self-registration (IRAL-1), but the information to be shared is classified as ‘in-confidence’ (AAL-2). Self-registration means that the client can use any name or identifier they like (eg Joe Bloggs) and be essentially anonymous. There is no circumstance where ‘in-confidence’ information can be shared with an anonymous client.

In these instances, the business requirements may need to change, or the classification of the information may be incorrect. In either instance, further discussion needs to occur with the business unit and information stakeholders to resolve the situation.

An alternative may be to redesign the service, perhaps removing potentially harmful information that may not be required by all clients and allowing anonymous access to the information. A second transaction could be created for clients who do need to access the ‘in-confidence’ information and implemented using an appropriate registration process. These clients are unlikely to have issue with the application of a more onerous registration process, given the information to which they are being granted access.

**Credential selection**

Potentially, several different types of credentials could be used for each Credential Assurance Level. The difficulty in choosing an appropriate credential is significant, given the array of options available and the number of variables which enter into the decision making process. This decision needs to balance the three elements of security, cost and convenience.

When selecting a credential, an agency should consider the following:

- Ease of use and registration for users
- Ease of implementation by an agency, including consideration of credentials that are already supported by an agency
- Credentials that are commonly used in the client community
- The likelihood that clients will be able to use the credential with other agencies
- Cost per client (to both the agency and the client)
Part 1 – Assessing Identity Risk Guidelines

- Setup costs for verification systems for this type of credential
- Ongoing costs for verification systems for this type of credential, including software licences, administration etc

Determining which credential to select

An issuing agency may decide to issue a credential or other form of identification document to clients – a credential may be a physical thing or it may be electronically based. There are many different forms of credential that may be issued and each has its own benefits and suitability for its task, such as:

- Plastic / polymer card
- Paper or cardboard card
- Paper certificate
- Username and password

An agency should choose the form of credential that best matches the assessed risk for the particular service and is fit for its intended use.

For example, if a credential needs to be kept by a client for an extended period of time, such as 2-5 years, and is to be used to access the service on multiple occasions, a durable plastic / polymer card may be suitable. However a paper document may be more suitable if the credential only needed to be displayed or produced on request as evidence of an entitlement.

The steps to be followed in determining which credential best suits the service being provided include the following:

- Assess the risk associated with the transaction – see Steps 1 to 5 above
- Determine the type of credential that best matches its intended purpose (ie which service delivery channel: phone, online, or in person)
- Determine the type of credential that matches the Identity Registration Assurance Level (as per Step 4)
- Determine the required security features for the credential
- Determine the required design and style for the printing of information on the credential (eg Tasmanian Government logo, Agency details, font size requirements etc)
- Determine the relevant information to be displayed on the credential (eg name of the cardholder, date of issue, date of expiry)
- Determine if a unique identifier will be incorporated in the credential and if so, its form (eg card, service or client number) – as an additional security measure, more than one unique identifier could be included to allow for verification purposes
- Determine the period of currency for the credential (see ‘Expiration of identities and authentication credentials’ in Step 6)
- Determine business rules for the renewal, cancellation and replacement of the credential
- Determine business rules for the recording of credential issuing, activation, cancellation, replacement and renewal processes in the agency common directory
Part 1 – Assessing Identity Risk Guidelines

- Determine the required authentication factors for the credential
- Determine the manufacturing process for the credential (if none already in place, may need to undertake a procurement process – see Treasury for details, www.treasury.tas.gov.au)
- Determine the quality assurance procedures to be applied to the production of the credential
- Determine the method for delivering the credential to the client
- Determine ongoing access management processes for the credential (see Part 4 – Access Management Guidelines)
- In determining the requirements for the credential, a comparison between the required Identity Registration Assurance Level and the preferred security features to be incorporated in the credential (as detailed in the Standards in Part 2 should be made to select the appropriate Credential Assurance Level
- Finalise and document the business rules for the issuing and managing of the credential, including appropriate verification requirements
- Update the client information store (if one exists) to document the process
- Determine the means by which a client’s application (an issuing order) will notify the appropriate staff member within the issuing agency that an issuing order has been submitted for appropriate action (ie creating the identity in the agency’s data store)

Document business processes

To complete this Step and to draft the business requirements and processes for the credential and its management, refer to Part 3 – Credential Management Guidelines and Standards.
Step 5
Perform Cost Benefit Analysis

At the completion of Step 5, you will have:

- Assessed the key cost considerations and any other cost factors relevant to your agency
- Considered your business processes and other relevant documentation to assess the cost of implementing the indicative assurance levels and recorded what documents informed this step
- Confirmed or revised your assurance levels based on the outcome of the Cost Benefit Analysis and amended the business requirements you developed in steps 3 and 4

The Worksheet at the end of this Toolkit will assist you to complete these steps.

The three assurance levels determined in the previous steps are the Access Assurance Level, Identity Registration Assurance Level and the Credential Assurance Level. It is important when implementing the Toolkit that agencies have some flexibility in applying these levels.

It is also important to note that the initial Access Assurance Level should, in virtually all circumstances, never be reduced to a lower level of assurance, as doing so will significantly increase the risk of harm arising from the service.

However, an agency should have the ability to accept and manage residual risks that accrue solely to it. So, if the risk assessment of a service indicates that the highest level risks identified affect the service-providing agency only and not its clients, the agency could choose to accept that risk and adopt a lower Access Assurance Level for the service. However, an agency should not reduce the Access Assurance Level when the harm identified would accrue to other parties. Any decisions to lower overall Access Assurance Levels must be taken with extreme care.
Cost / Benefit

A main consideration when implementing the Toolkit is to consider the costs of implementation against the benefit gained. As a general guideline, the cost and inconvenience related to a particular access control solution increases as the Access Assurance Level increases. This is reflected in the increased costs of collection and proofing of data during registration (and re-registration) and also in the increased implementation and/or operating costs of issuing credentials and the associated technology.

The key cost considerations are:

- The number of potential and likely clients
- The cost of the registration process (self-registering versus registering in person)
- The cost and lifespan of any credentials issued (certain credentials may only last a couple of days, such as one-time passwords)
- The cost of credential management (requirement for manual versus automatic management such as password resets)
- Any existing technology infrastructure that can be leveraged
- The expected life of the service (short lifespan with costly authentication management may not be feasible)

Analysis

The following example may help explain the analysis process.

During the evaluation of a service, an agency identifies a need for an overall AAL-3 and an IRAL-3. This would indicate a required CAL-3, which would generally involve a two-factor verification process. However, the nature of the service is such that this level of verification is likely to be costly.

To decrease the Access Assurance Level, an agency would need to change the service delivery proposal, considering aspects such as reducing the amount of sensitive information being provided in relation to the transaction, which may in turn reduce the access management failure risk level and hence may reduce the Access Assurance Level.

It is also possible for an agency to increase the Access Assurance Level directly, although this would significantly increase the implementation costs without any real additional benefit to the service. An agency may wish to increase the Access Assurance level if it was expecting to change the service in the future in a way that may require a higher level of Access Assurance, or to take advantage of existing processes or issued credentials already operating at a higher level. It may be feasible and more cost effective to implement the final solution in the first instance. Consequently, an assessment of future services at this point may be useful.
Other considerations may come into play during cost benefit analysis. The Credential Assurance Level matrix detailed in Table 11 in the previous section indicates the minimum Credential Assurance Level required. There are cases where the business requirements may drive the need to implement high Credential Assurance Levels. This can occur where a client wishes to use a service anonymously, such as for receiving personal test results for a pathology, or an aptitude test; or for making human resource enquiries or complaints; or any other business scenarios. In these situations, it may not be important that the client provide a real-world identity. However, the agency needs to be certain that the client who made the initial inquiry or request is the same individual who receives the results or response.
Step 6
Implement Business Processes

At the completion of Step 6, you will have:

- Recorded your assurance levels in your agency’s information asset register
- Confirmed and implemented the identity registration processes for the service
- Confirmed the type of credential to be used for the service
- Confirmed and implemented the business requirements for managing the credential, including verification and processes for the expiry of identities and credentials
- Confirmed and implemented ongoing access management processes for the service.

The Worksheet at the end of this Toolkit will assist you to complete these steps.

After completing Steps 1 to 5 above and establishing the required assurance levels, the next step is to confirm, document and implement the relevant business processes that support the identified assurance levels.

The guidelines and standards contained in Parts 2, 3 and 4 of the Toolkit will assist in this step.

**Information asset register**

Under the *Tasmanian Government Information Security Charter*, agencies are required to maintain an information asset register. This is the most appropriate place to record the assurance level for the information asset derived through this process. This evaluation information will allow for future reviews of assurance levels to be conducted quickly and easily.
Identity registration procedures

Under Step 3, the business requirements for client identity registration (in terms of the Identity Registration Assurance Level) will have been determined and documented. Following the cost benefit analysis under Step 5 above, any changes to these processes should be made and the confirmed processes documented.

A plan for implementing may be appropriate, particularly if there is a need to inform clients of the process, or to train staff in applying the identity and access management procedures, or there is a lead in time for the production of a credential.

Credential management procedures

The type of credential or verification process to be applied to the service will have been determined under Step 4 above. This includes documenting the confirmed procedures, following the completion of the cost benefit analysis under Step 5 above.

Planning for the implementation of the credential needs to be consistent with the implementation of the client registration and ongoing management procedures.

Ongoing access management procedures

Before implementing the identity registration and credential management processes for the delivery of a particular service, the ongoing access management process for these processes must be determined and documented.

Part 4 – Access Management Guidelines is laid out in the same manner as Part 2 – Identity Registration Assurance Guidelines and Part 3 – Identity Credential Management Guidelines. That is, specific guidelines are provided for each Access Assurance Level (ie levels 0 to 4).

If the Access Assurance Level has been assessed as Level 3 (see Step 2), the guidelines for Access Assurance Level 3 detailed in Part 4 would be consulted to determine the ongoing access management procedures for the service. As noted earlier, in most cases, the assessed Identity Registration Assurance Level and Credential Assurance Level would be consistent with the Access Assurance Level (ie both Level 3).

From the Access Management Guidelines in Part 4, the appropriate ongoing access management business procedures would be confirmed and documented.

Some planning for the implementation of these requirements would be appropriate, particularly to ensure that all relevant staff are aware of, and apply the relevant business procedures.

A critical issue in the ongoing access management process is dealing with managing changes to the identity data. This is particularly important when managing the access rights of an enrolled identity when they are no longer entitled to have access.
Part 1 – Assessing Identity Risk Guidelines

Expiry of enrolled identities and credentials

The expiry of an enrolled identity needs careful consideration at this stage and should be managed through appropriate business processes.

The length of time that an enrolled identity should remain valid depends on a range of business requirements. The following should be considered:

- An enrolled identity expiry policy should cover both the expiry of the enrolled identity and the associated credential
- Expiration of an enrolled identity should result in a de-activation of the identity
- Enrolled identities that have expired will need to undergo a reactivation process if they are to be restored and credentials that have expired will need to be reissued
- In some instances, an enrolled identity never expires, only the associated credential does (e.g. passwords)
- An agency may require that passwords be reset regularly (e.g. every 60 days)
- Expiry of an enrolled identity will prevent the use of a linked credential – this may be the most practical approach when a credential in use does not have an easy means of expiry (e.g. a photograph)
- To give an enrolled identity a finite active life, either of the following processes would be applied:
  - The enrolled identity is given a set life (e.g. 12 months) commencing on the day of registration
  - The enrolled identity is kept active by use of the credential, but it will expire after a specified period of non-use
  [In which case, the period of currency for the enrolled identity would be shorter, and be set in terms of days or weeks – e.g. if a client has not ‘logged-in’ to a service for twelve weeks, the enrolled identity would be deactivated and the client required to re-register or re-enrol]

Similar approaches would be applicable in relation to the expiry of credentials.
Step 7  
Review

At the completion of Step 7, you will have:

- Scheduled a regular review of the identity and access management requirements of the service
- Ensured that your business systems require a review of assurance levels when additional transactions are made to a system

To maintain the integrity of the identity and access management process, regular reviews of the business requirements for the service should be conducted.

Such a review would be conducted, either:

- After a predetermined period, to ensure that the assurance requirements have not altered from the original scope. This review will identify any changes in information sensitivities and highlight if any changes are to be made to the various identity and access management processes discussed in this document and their subsequent implementation.
- When additional transactions are added to the same system. The purpose of this review is to ensure that there are no other flow-on transactions resulting from a service implementation. It is possible that one service may result in further transactions that are of a different nature. These additional transactions are to be independently reviewed to determine their access assurance levels. The implementation of a set of related levels will often mean the highest level of assurance required is implemented for all services / transactions.