Australian Government

Digital Transformation Office

Third Party Identity Services Assurance Framework

Accreditation Framework

Version 2.0 December 2015

Digital Transformation Office

Licence

Use of the Coat of Arms

Contact us

Enquiries or comments regarding this document are welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Executive summary

There is an emerging commercial provider market for a range of on-line identity related services such as personal data vaults, digital mailboxes, verification and authentication services. These services have been developed and marketed in what amounts to a caveat emptor (buyer beware) market.

In response, this Third Party Identity Services Assurance Framework (Assurance Framework) sets out the compliance criteria and accreditation requirements for Third Party providers of broadly defined "identity services".

The underlying premise of the Framework is that, based on an understanding of agency requirements, individuals will be able to choose to use the services offered by Accredited Service Providers in order to access online government services. Equally, a key premise is that individuals should not be forced to hold multiple credentials to access the range government services they require.

The Assurance Framework is underpinned by existing Australian Government security frameworks and informed by existing identity management policy frameworks and standards. The value of an individual's personal information must be recognised by Providers and reflected in the development of privacy and risk based security controls that meet agency requirements.

Consistent with international standards and Australian and international government policies, the Framework establishes four Levels of Assurance (LoAs) for the provision of broadly defined "identity services". For each LoA the Framework specifies performance outcomes and standards to be achieved by Providers and particular conformity assessment requirements (including commercial security standards such as the Payment Card Industry Data Security Standard (PCI-DSS)) that must be satisfied.

Section 3.4 sets out the roles and responsibilities of participants under the Assurance Framework, in particular the responsibility of the Assurance Framework Competent Authority (Competent Authority). Sections 3.5 – 3.7 outline the accreditation process for Providers.

The Competent Authority is responsible for ensuring that the Accreditation Process is conducted with due care and in a timely manner but is not liable for any errors and/or omissions in the final Documents (see Disclaimer at Section 3.8).

Section 4 details the specific compliance criteria and accreditation requirements for each category of Service Provider – data vault/mailbox, verification and authentication services.

Section 6 contains guidance for agencies in relation to ICT Procurement and Attachment 1 contains further guidance material for Service Providers.

Contents

1. Introduction

Australia has no nationally recognised framework for managing or coordinating digital identity services. While Government has traditionally played (and will continue to play) a central role in terms of providing identity documents there is evidence that the market has matured to the point where Service Providers are offering a variety of identity related solutions, for example:

- digital mailbox providers (such as Australia Post and Fuji Xerox) which enable people to receive correspondence from participating organisations in a single in-box;
- personal identity management (or authentication) providers who provide people with credentials (e.g. a user name and password, digital certificates etc) to enable access to a variety of services;
- online verification services which enable people to have claims regarding their identity or other attributes verified online; and
- personal data management or data vault services, which enable people to store and retrieve their personal data electronically, including storage of electronic copies of personal records such as birth certificates.

The Assurance Framework is:

- underpinned by existing Australian Government security frameworks – the Protective Security Policy Framework[1] (PSPF) and the Australian Government Information Security Manual[2] (ISM) as well as current and new privacy legislation ; and
- informed by existing policy frameworks such as the National e-Authentication Framework (NeAF), the Gatekeeper Public Key Infrastructure (PKI) Framework, the National Identity Security Strategy (NISS) and activities currently underway in relation to matters such as off-shoring, cloud computing and Data-Centres-as-a-Service (DCaaS).

The Framework and its accreditation processes have been endorsed on a whole of government basis by the Secretaries' ICT Governance Board (SIGB). Therefore agencies intending to utilise services of the type encompassed by the Framework should use Providers accredited at the appropriate Level of Assurance. From a Provider perspective, the Framework is voluntary in that there is no obligation (except as may be required by a particular agency for delivery of particular services) to independently seek accreditation.

The Digital Transformation Office (DTO) is also leading work to investigate the scope for agencies to:

- leverage the use of higher assurance digital credentials issued by Providers such as financial institutions, and
- utilise, on a risk-basis, existing digital credentials, including third party credentials.

These initiatives will be accompanied by the development of appropriate trust arrangements that meet the needs of all parties including individuals, businesses and government agencies.

The investigation will build on discussions in relation to the national Trusted Digital Identity Framework currently being developed by the DTO.

Investigation into the use of third party credentials will draw significantly on work being done through groups such as the Open Identity Exchange (OIX), IDCommons and its Internet identity Workshops, the Kantara Initiative, and the Personal Data Ecosystem Consortium.

---

[1] Australian Government PSPF: https://www.protectivesecurity.gov.au/Pages/default.aspx

[2] Australian Government ISM: http://www.asd.gov.au/infosec/ism/index.htm

A key piece of work will be the socialisation of this Framework – both nationally and internationally – and feedback will inform the additional work required to achieve the necessary cross recognition between different national trust frameworks.

1.1 Terms and Definitions

The terms and definitions used in this document are defined in the *Identity and Access Management Glossary*.

1.2 Purpose and Principles

The purpose of the Assurance Framework is to guide Providers and Agencies on the policies and standards that apply, within a risk management context, to the provision of digital mailbox, data management and authentication services to Government.

The Framework establishes the following core principles:

- Agencies will specify the Level of Assurance required for a particular service or services;
- Providers will adopt robust risk management approaches to deliver the levels of privacy and security required by agencies in relation to people's personal data; and
- People will eventually be able to choose from a range of Providers in order to access the range of Government services they require.

In addition:

- Agencies may additionally choose to specify particular requirements in relation to matters such as data integrity, security and identity assurance levels;
- Agencies will engage directly with Providers for the delivery of specific services; and
- In accordance with the PSPF, accountability for the performance of the service or function and responsibility for outcomes remains with the Contracting Agency.

Providers must satisfy all the requirements for accreditation at a specific Level of Assurance (LoA) in order to be granted accreditation and subsequently listed on the DTO website. Agencies may choose (at their own risk) to utilise services from Providers that are "in the process" of completing the accreditation process.

In some circumstances Providers may hold accreditations at different Levels of Assurance for the same type of service; for example a Provider may be accredited to provide authentication services at both LoA 1 and 3.

In relation to data vault / mailbox services a Provider holding accreditation at LoA 3 would be able to offer such services at lower assurance levels without the requirement to be accredited at those levels.

Verification Services apply only at LoA 3.

1.3 Review Date

This document will be reviewed regularly and updated in line with changes to the relevant government protective security policies, manuals and frameworks.

1.4 Advice on the Framework

Advice on the Assurance Framework or suggestions for amendment is welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

2. Assurance Framework Accreditation Process

2.1 Overview

The accreditation process set out in this Framework produces a whole of government outcome. That is, Providers do not need to undergo the accreditation process for each separate agency that engages their services, except in circumstances where the agency requires a higher level of assurance than the Provider has obtained through its accreditation. In such circumstances the accreditation process will only involve the additional requirements associated with the higher LoA.

The accreditation process involves a combination of self-assessments, third party evaluation processes and documentation requirements. These are regarded as being no more than Providers would prepare to demonstrate the security and integrity of their operations to clients.

The costs of all third party assessments are to be met by the Provider.

For LoA 1 and 2 the accreditation process is effectively based on a self-certification process (with the exception of the requirement for an independent Privacy Impact Assessment (PIA)) although Providers will still be required to enter into a Memorandum of Agreement (MOA) with the Commonwealth.

Third party conformity assessment is a common feature of other international trust framework arrangements.

Under the UK Government's ID Assurance program:

- The UK Cabinet Office has joined a standards certification organisation (*tScheme*[3]), to provide the necessary independent assessment of the framework suppliers for compliance with the standards (defined and published by the Cabinet Office and the National Technical Authority (CESG)) for providing a trusted, reliable and secure service.

In the US:

- The Federal Government has established Trust Framework Solutions to leverage industry-based credentials that citizens already have for other purposes. The Trust Framework Provider Adoption Process (TFPAP) is used to assess existing, industry-based Trust Frameworks and approve them as Trust Framework Providers (TFPs). TFPs in turn define the processes for assessing Identity Provider credentialing processes against federal requirements for issuance, privacy, and auditing as codified by the US Government.

2.2 Conformity Assessment

Conformity assessment is the 'demonstration that specific requirements relating to a product, process, system, person or body are fulfilled. Conformity assessment procedures, such as testing, inspection and certification, offer assurance that products fulfil the requirements specified in regulations and standards' (Source: ISO/IEC 17000 *Conformity Assessment – Vocabulary and General Principles*).

[3] *tScheme* is an independent, industry-led, self-regulatory scheme similar to the US Kantara Initiative. It was set up to create strict assessment criteria, based on industry best practice, for Trust Services (professional assurance and advisory services that address the risks and opportunities of digital technology) such as Identity Assurance.

In circumstances where Providers offer broadly defined “identity services” that purport to be adequate for reliance by government agencies delivering services and benefits to individuals, it is expected that such services will meet, at a minimum, baseline ICT security management standards.

From an information assurance perspective the nature of the conformity assessment process is directly proportional to the level of assurance offered/required for such services[4].

ISO/IEC 27001:2005 – Information technology -- Security techniques -- Information security management systems – Requirements requires that management:

- systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

2.3 General Requirements

Privacy

The *Privacy Act 1988* (Cth) (Privacy Act) applies to government and private sector entities that handle personal information.

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Reform Act) passed through the Australian Parliament on 29 November 2012 and received royal assent on 12 December 2012. The new legislation came into effect on 12 March 2014.

When entering a Commonwealth contract, section 95B of the *Privacy Act* requires an agency to take contractual measures to ensure that a ‘contracted service provider’ (CSP) for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle (IPP) if done by the agency. This requirement remains unchanged as a result of the Reform Act.

All Providers **MUST** demonstrate compliance with all National Privacy Principles (NPPs), the Information Privacy Principles (IPPs) as applicable and, from 12 March 2014, all Australian Privacy Principles (APPs).

Security

The provisions of the Australian Government PSPF and ISM establish the over-arching requirements to be satisfied by Providers under this Framework.

Security is a combination of physical, logical (ICT) and personnel security. These measures are designed and implemented to provide “defence in depth” appropriate to the perceived threats/risks to the assets being secured.

[4] This is the approach adopted in the US for the National Strategy for Trusted Identities in Cyberspace (NSTIC).

All Service Providers **MUST** have a documented Security Risk Management Plan (SRMP) including as appropriate implementation of ASD Mitigation Strategies

Further information on security, privacy, liability and incident management considerations is at Attachment 1.

2.4 Accreditation Process – Roles and Responsibilities

The Service Provider is responsible for:

- Preparing all the required documentation necessary for the required LoA for submission to the DTO;
- Obtaining all the required 3rd party assessment reports and certifications; and
- Ensuring that, where the Service Provider utilises secure data storage services from a 3rd party (e.g. a Cloud Service Provider) the 3rd party's privacy and security policies and practices[5] are duly incorporated into its own security and privacy documentation.

The Contracting Agency[6] is responsible for:

- Working with the Service Provider and the DTO to agree milestones and deliverables;
- Working with the Service Provider to ensure that milestones and deliverables are achieved;
- Where the Service Provider supports storage of digital copies of government issued documents and credentials, liaising with relevant issuing agencies to ensure that the Provider's privacy and security arrangements meet the requirements of the issuing agency; and
- Providing oversight support to the DTO in the management of the accreditation process.

The DTO, as the Accreditation Authority, is responsible for:

- Reviewing, within agreed timeframes, all documentation to ensure compliance with the standards and policies set out in the Assurance Framework; and
- Preparing a recommendation to the Assurance Framework Competent Authority (Competent Authority).

The role of Competent Authority will rest with the Gatekeeper Competent Authority on the basis that, through its administration of the Gatekeeper accreditation program, the DTO[7] has the skills and experience required to manage the accreditation of Service Providers.

The accreditation process is driven by two underpinning requirements:

- The PIA and
- The Security Risk Assessment and resultant Security Risk Management Plan.

The Contracting Agency's IT Security team will be involved in ensuring that the Service Provider's security policies and practices are consistent with the agency's requirements at the specified LoA.

---

5 Including where appropriate any industry certifications

6 Only in circumstances where the Provider has negotiated a service agreement with an Agency. Where no such agreement is in place it will be the Provider's responsibility to work with the DTO and relevant document issuers.

7 Supported by the Australian Signals Directorate as required in relation to ISM compliance and cryptographic issues

2.5 Authorised Assessors

- Organisation Services – Qualified accountant who is a member of a professional accounting body.
- Privacy Impact Assessors. See http://www.privacy.gov.au/aboutprivacy/helpme/psp for a list of potential privacy Service Providers (NOTE: these providers are NOT endorsed by the Office of the Australian Information Commissioner).
- I-RAP assessor (see http://www.asd.gov.au/infosec/irap.htm).
- PCI-DSS Qualified Security Assessor (QSA). See https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php for a list approved QSAs.
- JAS-ANZ accredited ISO/IEC 270001 Certification body (see http://www.jas-anz.com.au/).

2.6 Decision Making Processes and Authorities

- Service Provider applies to the DTO for accreditation for a particular service at a particular LoA(s).
- Service Provider presents documentation to the DTO for review.
- Service provider presents required certificates of compliance to the DTO.
- The DTO and Contracting Agency work through the accreditation process with the Service Provider.
- The DTO prepares Briefing to Assurance Framework Competent Authority.
- Assurance Framework Competent Authority grants accreditation at appropriate LoA.
- Service Provider details are published on the DTO website and advice provided to agencies through GovCIO.

2.7 Management of Accredited Service Providers

At the completion of the accreditation process the Service Provider and the DTO will sign a Memorandum of Agreement (MoA). This MoA will set out the respective rights and obligations of the Commonwealth and the Service Provider for the provision of services to agencies, including the obligations on the Provider to provide its services in accordance with the documentation that underpins their accreditation.

It will not address commercial matters that are more appropriately the subject of a commercial Service Level Agreement between the Service Provider and the Contracting Agency.

The MoA will also specify arrangements in relation to:

- Maintenance of accreditation – what actions providers MUST take in order to maintain accreditation from year to year;
- Dispute settlement, including appeal mechanisms; and
- Management of security and privacy breaches.

Maintenance of Accreditation

In general terms accreditation will continue from year to year, subject to a satisfactory compliance audit (i.e. the Provider is able to demonstrate through the annual audit process that it continues to offer services in a manner consistent with the documents that formed the basis for their accreditation).

Maintenance of accreditation will be dependent on the Provider:

a. continuing to comply with the Assurance Framework;

b. providing services from within Australia and in accordance with its Approved Documents; and

c. complying with reasonable directions from the Competent Authority relating to the Assurance Framework.

Dispute Settlement

While there are well-established dispute resolution mechanisms available (e.g. the Australian Commercial Disputes Centre (ACDC)) the MOA will highlight that the parties will undertake their obligations and exercise their rights in good faith and in a spirit of cooperation.

Breach Management

It is expected that Service Level Agreements (SLA's) between the Provider and Agencies will contain explicit mechanisms for dealing with breaches of security. Section 95B of the *Privacy Act* requires such agreements to contain clauses obliging Providers to not breach the Information Privacy Principles or IPPs (or APPs from 12 March 2014). Containment of privacy breaches is a requirement of existing IPP 4, which will continue under APP 11. Those principles require adequate security measures to be implemented to protect personal information from unauthorised access, disclosure, misuse or modification.

In all such instances the Provider **MUST** also notify the Competent Authority. The Competent Authority will then work with the Provider to determine the consequences of the breach for the Provider's accreditation.

Under proposed mandatory data breach notification legislation Providers may be required to notify the Office of the Australian information Commissioner and affected individuals about data breaches that give rise to a real risk of serious harm to those affected individuals.

Providers are also encouraged to use the ASD Cyber Security Incident Reporting (CSIR) scheme (see http://www.dsd.gov.au/infosec/reportincident.htm) to report security breaches.

2.8 Disclaimer

The Assurance Framework Competent Authority is responsible for ensuring that the Accreditation Process is conducted with due care and in a timely manner.

The Assurance Framework Competent Authority is not liable for any errors and/or omissions in the final documents, which remain the responsibility of the Service Provider.

By granting accreditation to a Service Provider, the DTO

makes no representation and gives no warranty as to the:

- accuracy of any statements or representations made in, or suitability of, the documents of the Accredited Service Provider; or
- the standard or suitability of any services thereby provided for any Agency.

3. Accreditation Requirements

3.1 Data Vault or Mailbox Service

LoA – Data Management Services (data vaults, mailboxes etc)

Minimal assurance	Low assurance	Moderate assurance	High assurance
Level 1	**Level 2**	**Level 3**	**Level 4**
Minimal confidence in the services offered	Low confidence in the services provided	Moderate confidence in the services provided	High confidence in the services provided.

Important Note
Achieving LoA 4 Assurance requires completion of the requirements for LOA1 – LoA 3.

IMPORTANT NOTES

- Where the Provider supports storage of digital copies of government issued credentials (e.g. passports or motor vehicle licences) these credentials remain the property of the issuing agency.
  - The Contracting Agency is responsible for liaising with relevant issuing agencies to ensure that the Provider's privacy and security arrangements meet the requirements of the issuing agency.
  - Where the Provider supports storage of financial data such as credit card details, demonstrated compliance with the Payment Card Industry Data Security Standard (PCI-DSS) will apply (see https://www.pcisecuritystandards.org)[8].
- Where a Provider utilises secure data storage services from a 3rd party (e.g. a Cloud Provider) the security and privacy controls **MUST** clearly identify the respective roles and responsibilities of both the Provider and 3rd party.
  - In this regard recognition would be given to accreditations/certifications issued under other overseas national programs insofar as they are applicable to the Provider or 3rd party's operations under the Assurance Framework.
  - Consideration should also be given by the Provider (and Contracting Agency) to ASD's guidance on cloud security[9] particularly with respect to the storage of personal information.
- Providers **MUST** specify the physical location of data centres used to store personal information. Where a Provider utilises services outside Australia to store, backup, process, transmit, manage or otherwise support its Australian operations these **MUST** be clearly identified and included in the Provider's security and privacy documentation[10].

[8] It is understood that a Service Provider has limited control over what types of information/documents that an individual chooses to store in their personal data vault. Service Providers may choose to specify (for example in the mailbox/vault terms and conditions) the types of documentation/information for which their services are considered "fit-for-purpose" (i.e. the Service Provider has implemented security and access controls that are appropriate for the types of documentation/information specified in the terms and conditions).

[9] ASD's guidance on Cloud Security: see: www.dsd.gov.au/infosec/cloudsecurity.htm

[10] For further information see the *Australian Government Policy and risk management guidelines for the processing and storage of Australian Government information in outsourced or offshore ICT arrangements* at www.protectivesecurity.gov.au/Pages/default.aspx.

- Consistent with the requirements of the PSPF agencies will apply a risk assessment process in making decisions to rely on data or credentials known to be stored by an individual outside Australia.
- Providers may choose to require users of their data vault / mailbox services to undergo an identity proofing process as a pre-requisite to signing-up for services.
  - Where Providers adopt this approach the authentication LoA **MUST** be equivalent to that of the data vault / mailbox services. That is, if the Provider is offering mailbox services at LoA 3 then the evidence of identity processes **MUST** also be at LoA 3.

Compliance Criteria

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Organisation Services	• Fully operational legal entity compliant with all relevant legal requirements including agency specific legislation and policies (self assessed).	• Published Liability Policy Financial situation sufficient for liability exposure (self assessed).	• Financial situation sufficient for liability exposure (independent assessment by a qualified accountant who is a member of a professional accounting body).	
Privacy	• Independent Privacy Impact Assessment (PIA) – see http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html for further information. • Demonstrated compliance with all National Privacy Principles (NPPs), the Information Privacy Principles (IPP's) as applicable and from 12 March 2014 all Australian Privacy Principles (APP's). • Destroy an individual's stored data within a reasonable time of the person terminating their relationship with the Provider. • Provide a means for subscribers to securely amend their stored information.			

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Information Security Management System **Requires specification of relevant technical and security standards and controls.**	• Documented Security Risk Management Plan (SRMP including ASD Mitigation Strategies (see http://www.asd.gov.au/infosec/mitigationstrategies.htm). • Appropriate operator access controls and data protection mechanisms (at rest and in motion) are implemented.	• Defined managerial responsibility for all security policies. • ISMS complies with ISO/IEC 27001 (self assessment) • Documented incident management plan addressing in particular security and privacy breach management. • Effective personnel security controls are in place • Adequate Physical Security controls are in place to protect premises and information resources. • 2 yearly security audits by an IRAP assessor to ensure documented security controls are being effectively implemented and remain adequate for the services provided. • A secure log of all relevant security events is maintained. • Shared secrets appropriately secured (physical and logical).	• An independent Protective Security Risk Review (PSRR) is performed at least annually by an IRAP assessor.	• DR plan tested and reviewed annually. • ISMS has been certified by JAS-ANZ accredited certification body to ISO/IEC 27001 and is subject to annual audit – see http://www.jas-anz.com.au/ for further information.

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Storage and electronic transmission of personal information	• Use an encryption product that implements a AACA as per ISM requirements. • Where practical, cryptographic products MUST provide a means of data recovery. • Use an encryption product that implements an AACP to communicate sensitive information over public network infrastructure – see http://www.asd.gov.au/infosec/ism/index.htm for further information.[11]		• Use an Evaluation Assurance Level (EAL) 2 encryption product from ASD's Evaluated Products List (EPL) that has completed a DCE – see http://www.asd.gov.au/infosec/ism/index.htm for further information. • Data centres used to store personal information MUST be located in Australia and listed on ASD's Certified Cloud Services List – see http://www.asd.gov.au/infosec/irap/certified_clouds.htm for further information	
Physical security	• Demonstrate an appropriate physical security environment for the protection of business assets and processes. • Documented Physical Security Policy as part of overall SRMP.		• Compliance with the PSPF Physical Security Protocol at http://www.protectivesecurity.gov.au/physicalsecurity/Pages/Protocol.aspx .	

[11] Providers should note that the use of encryption may introduce challenges to meeting data availability requirements

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Personnel Security	• Compliance with PERSEC 1 in the PSPF (self assessment).	•	• Documented Personnel Security Management Plan including: verification of qualifications, police records check, referee checks, identity verification.	• Vetting of personnel and contractors in Positions of Trust in accordance with AS4811-2006: *Employment Screening* including appropriate personnel security aftercare arrangements.
PCI-DSS requirements for storage of payment card data	• Not allowed.	• Not allowed.	• Completion of the Attestation of Compliance with the Payment Card Industry Data Security Standard (PCI DSS) by a Qualified Security Assessor (QSA).	•

Accreditation Documentation

Level of Assurance	Accreditation Requirement
LoA 1	• PIA and published Privacy Policy. • Documented SRMP including application of ASD Mitigation Strategies as appropriate and incorporating a Disaster Recovery and Business Continuity Plan. • Documented Physical Security Policy as part of overall SRMP.
LoA 2	• Published Liability Policy. • Documented Incident Management Plan addressing in particular security and privacy breach management. • A secure log of all relevant security events including a mature log audit process.
LoA 3	• Documented Personnel Security Management Plan.
LoA 4	• No additional documentation.

Accreditation Requirements

Level of Assurance	Component	Accreditation requirement
LoA 1	Organisation Services – financial, service management	• **Self** assessment and Declaration by the CEO that the organisation's financial situation is sufficient for liability exposure.
	Privacy	• **Independent** PIA that demonstrates the Provider's compliance with IPPs/NPPs and from 12 March 2014 the APPs.
	Security	• **Self** assessment and Declaration by the CEO that appropriate Physical, Logical and Personnel security policies, plans and practices have been implemented.
LOA2	Organisation Services – financial, service management	• **No** additional requirements.
	Privacy	• No additional requirements.
	Security	• 2 **yearly** security audit by an independent IRAP Assessor to ensure documented security controls are being effectively implemented and remain adequate for the services provided.
LoA 3	Organisation Services – financial, service management **See** NOTE 1 below	• The Provider **MUST** have its f**inancial** situation independently assessed by a qualified accountant who is a member of a professional accounting body as being sufficient for liability exposure.
	Privacy	• **No** additional requirements
	Security	• **An** independent Protective Security Risk Review (PSRR) is performed at least annually by an IRAP assessor. • Compliance with the PSPF Physical Security Protocol (see http://www.protectivesecurity.gov.au/physicalsecurity/Documents/Australian-Government-physical-security-management-protocol.pdf)). • **If** Appropriate – Completion of the Attestation of Compliance with the Payment Card Industry Data Security Standard (PCI DSS) by a Qualified Security Assessor (QSA).

Level of Assurance	Component	Accreditation requirement
LoA 4	Organisation Services – financial, service management	• No additional requirements.
	Privacy	• No additional requirements.
	Security	• **Disaster Recovery and Business Continuity Plan** tested and reviewed annually. • Information Security Management System (ISMS) has been certified by JAS-ANZ accredited certification body to ISO/IEC 27001: *Technology – Security techniques – Information security management systems – Requirements* (most recent version) and is subject to annual audit. • Documented evidence that personnel / contractors in Positions of Trust have been vetted in accordance with AS 4811-2006: *Employment Screening* including appropriate personnel security aftercare arrangements.

NOTE 1

Providers and Contracting Agencies **MUST** ensure that the following elements of *ASAE 3402*: *Assurance Reports on Controls at a Service Organisation* are incorporated in the SLA and that metrics are agreed to enable an adequate review of both Provider and Contracting Agency performance:

- Non-financial performance or conditions (for example, performance of an entity) for which the subject matter information may be key indicators of efficiency and effectiveness.
- Physical characteristics (for example, capacity of a facility) for which the subject matter information may be a specifications document.
- Systems and processes (for example, an entity's internal control or IT system) for which the subject matter information may be an assertion about effectiveness.
- Behaviour (for example, corporate governance, compliance with regulation, human resource practices) for which the subject matter information may be a statement of compliance or a statement of effectiveness.

3.2 Verification Service

In the context of this Assurance Framework the ability to verify the authenticity of documentation or personal information submitted by an individual assists in providing increased assurance that “the individual is who they say they are”.

Important note

Providers of Verification Services operate **ONLY** at LOA3 and above.

In the context of this Framework the term Verification Services is a reference to a Provider with the capacity to verify with an authoritative source that information (e.g. name, date of birth, address etc) submitted (for example to an Identity Provider) by an individual is true and correct.

The Assurance Framework requires Providers, in addition to the requirements specified below, to also satisfy the data-vault/mailbox security requirements at **LoA 3**.

Where a Verification Service Provider utilises third party services (e.g. a Cloud Service Provider) for storage of its personal information holdings then the same requirements will apply as for Data-Vault/Mailbox Providers.

Compliance Criteria

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Verification services (these services apply only at authentication assurance LOA3 and above)			• Independent PIA completed. • Published Privacy Policy. • Demonstrated compliance with all National • Privacy Principles (NPPs), the Information Privacy Principles (IPP's) as applicable and from 12 March 2014 all Australian Privacy Principles (APP's). • Appropriate contractual arrangements established with issuing authorities. • If personal information is retained satisfy the requirements for mailbox/data vault providers at LOA3.	

Accreditation Documentation

Level of Assurance	Component	Accreditation requirement
LoA 3	Privacy	PIA and published Privacy Policy.

Assessment Process

Level of Assurance	Component	Accreditation requirement
LoA 3	Privacy	Independent PIA that asserts Provider's compliance with IPPs/NPPs and (future) APPs.

Verification Service Providers **MUST** establish and provide evidence that appropriate contractual arrangements have been established with issuing authorities.

The term “issuing authorities” includes for example:

- government agencies that issue credentials or documents that also serve as evidence of identity credentials (e.g. DFAT for passports); and
- government agencies and or commercial bodies that may be regarded as authoritative sources of “truth” regarding particular items of personal information (e.g. an electricity utility for an individual’s home address).

The following principles apply in relation to any contract between the Verification Service Provider and the relevant “issuing authority”:

Liability

The Verification Service Provider **MUST** not seek to avoid or exclude liability for any breaches of its core obligations to ensure the security and privacy of its data holdings, including

- the prevention of unauthorised access to the information / data that it holds; and
- the privacy of any personal information that may be collected, used or disclosed by it as a result of its service offering.

Data Breach

Verification Service Providers should comply with the OAIC Data Breach Notification Guide, which may, in the event of a data breach that occurs in the context of a Verification check or from the Provider’s data holdings, include advising affected individuals and the OAIC where a real risk of serious harm to those individuals might arise. As noted above, proposed Commonwealth legislation, if enacted, would introduce a mandatory data breach notification scheme.

Operations

Verification checks are undertaken with the full knowledge and cooperation of the issuing authority.

Verification checks should not impede the normal operational performance of the issuing authority’s ICT systems.

Consent

Verification checks are undertaken with the full and informed consent of the individual whose personal information is being verified.

From an operational perspective, Verification Service Providers **MUST** demonstrate that requests to verify a document or personal information are encrypted and sent via a secure communications pathway to the issuing authority and that no personal data is transferred from the issuing authority.

In this regard Providers are directed to controls specified in the ISM in relation to securing data at rest and in transit:

> *Use an encryption product that implements an AACP to communicate sensitive information over public network infrastructure – see http://www.asd.gov.au/infosec/ism/index.htm for further information*[12]

[12] Providers should note that the use of encryption may introduce challenges to meet data availability requirements

These requirements also apply to Data Vault/Mailbox Providers.

The nature of the response to a Verification check **MUST** take the form of a Boolean response (i.e. Yes/No). This requires the Provider to ensure that it's checking process only allows for the provision of such responses.

Document Verification Service (DVS)

The national DVS is part of the Australian Government's commitment to protecting the identity of Australians. The DVS is a tool to verify the accuracy and validity of data on key Australian identity credentials provided at enrolment. It is a secure, on-line system used to check, in real time, whether the information on a credential (such as document number, name and date of birth) 'matches' information held by the issuing agency. The DVS does not store any personal information. Requests to verify a document are encrypted and sent via a secure communications pathway to the document issuing agency. No personal data is transferred from the document-issuing agency.

Currently, the DVS is only available to government agencies. However, the Government is working with the States and Territories to extend access to the DVS to private sector organisations. The initial focus is on organisations with client identification obligations under Commonwealth legislation. Some of these organisations may choose to access the DVS via a third party identity service provider. Over time, DVS access could be further extended to some private sector identity service providers in their own right, subject to privacy and other requirements being met.

3.3 Authentication Service

Important Note

Achieving LoA 4 Assurance requires completion of the requirements for LoA 1 – LoA 3.

National e-Authentication Framework (NeAF) Levels of Assurance – Identity/Attributes

Minimal assurance	Low assurance	Moderate assurance	High assurance
Level 1	Level 2	Level 3	Level 4
Minimal confidence in the identity assertion / credential.	Low confidence in the identity assertion / credential.	Moderate confidence in the identity assertion / credential.	High confidence in the identity assertion / credential.

In the context of this Framework, an Authentication Service is principally a reference to Identity Providers:

> Entities that "create, maintain, and manage identity information for principals and provides principal authentication to other service providers within a federation".

Identity providers may utilise the services of independent Verification Service Providers to enhance the assurance associated with authentication credentials or attribute assertions that may be supported through their services. Alternatively a Provider may seek accreditation as both an Authentication Service Provider and Verification Service Provider in order to provide clients with a higher assurance authentication solution.

Note also that the term identity is not a fixed concept – it comprises a number of different, often context based attributes. Further, not all attributes may relate to an individual's identity yet may still be

necessary for the delivery of government services (e.g. a physical address). Identity Providers may offer authentication services that address a variety of identity / non-identity attributes.

Note

Given the sensitivity of the personal information collected and stored, Providers of authentication services at LoA 2 and above **MUST** satisfy the security and privacy requirements for mailbox/data vault Providers to a minimum of LoA 3. An important consideration in relation to the operation of authentication services relates to the security and privacy of personal information held by the Service Provider. Because of the potential "attractiveness" of this information the Providers of these services **MUST** also satisfy the data-vault/mailbox security requirements at Level of Assurance 3.

Compliance Criteria

REQUIREMENT	LoA 1	LoA 2	LoA 3	LoA 4
Identity Proofing (Providers to demonstrate completion of NeAF assessment **[reflected in Identity and Credential Policies] and implementation of provisions of ISO/IEC 29115)**	• Ensure that each applicant's identity record is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity. • Accept a self-assertion of identity • Accept self-attestation of evidence. • Accept pseudonyms – self asserted, socially validated.	• Perform all identity proofing strictly in accordance with its published Identity Proofing Policy • Applicant provides name, DOB, address, email/phone (to be verified as appropriate) • Maintain appropriate Identity and Verification Records in accordance with the Archives Act. • Optional ID proofing: • AS4860—2007. *Knowledge-based identity authentication—Recognizing Known. Customers*). • 3rd party verification (authorised referee[13] where possible).	• Electronic verification where possible (DVS or other authorised data verification service provider – see below) of presented documents with the specified issuing authority to corroborate date of birth, current address of record[14], and other personal information. • The primary document MUST be a Government issued credential with a biometric. • GSEF processes may be considered on a risk basis. • Optional ID Proofing: • Known Customer.	• Only face-to-face identity proofing is acceptable. • Gold Standard Enrolment Framework (GSEF) processes apply (see (www.ag.gov.au/identitysecurity): Applicant presents: • Secondary Government Picture ID (not the same as the primary document) or credential issued by a regulated financial institution. OR • two items confirming name, and address or email address, such as: utility bill, professional license or membership, or other evidence of equivalent standing (see Gatekeeper EOI Policy). • All presented credentials and information are where possible electronically verified with relevant issuing authority.

[13] An authorised referee is a person or organisation that holds a position of trust in the community and is known and listed by the enrolling agency to perform the function of a referee.

[14] Note that the DVS does not verify address records.

REQUIREMENT	LOA 1	LOA 2	LOA 3	LOA 4
Credentials	Account for the following system threats and apply appropriate controls: • the introduction of malicious code; • compromised authentication arising from insider action; • out-of-band attacks by other users and system operators (e.g., the ubiquitous shoulder-surfing); • spoofing of system elements/applications • malfeasance on the part of subscribers and subjects. • Single factor authentication solutions acceptable.	• Published Credential Policy and Practices Statement approved by internal Policy Management Authority. • Strong passwords as per ISM • Non-PKI multi-factor authentication protocols required.	• Cryptographic technology deployed through a Public Key Infrastructure – "soft" certificates.	• Cryptographic technology deployed through a Public Key Infrastructure deployed on hardware tokens protected by password or biometric controls.
Privacy	• Demonstrated compliance with all National Privacy Principles (NPPs), the Information Privacy Principles (IPP's) as applicable and from 12 March 2014 all Australian Privacy Principles (APP's).	• Amendment of subscriber personal information requires either: i. re-proving their identity, as in the initial registration process, or ii. by using their credentials to authenticate their revision.	• Successful amendment of personal information should result in re-issuance of the credential.	

REQUIREMENT	LOA 1	LOA 2	LOA 3	LOA 4
Key Management		• Documented Key Management Plan (KMP) assessed by commercial IRAP assessor (see Gatekeeper PKI Framework for details of KMP requirements).	• Full Gatekeeper accreditation.	• Gatekeeper High Assurance accreditation. • Specifications for hardware tokens from EPL.

Accreditation Documentation

Level of Assurance	Accreditation requirement
LoA 1	• Published Privacy Policy.
LoA 2	• Published Identity Proofing Policy • Published Credential Management Policy and Practices Statement – Consistent with Privacy Policy and SRMP. • Documented Key Management Plan (KMP).
LoA 3	• Gatekeeper Accreditation – Certificate Policy. – Certification Practices Statement. – Security Profile (including SRMP and KMP). – Operations Manual. – Disaster recovery & Business Continuity Plan.

Level of Assurance	Accreditation requirement
LoA 4	• Gatekeeper High Assurance Accreditation – Certificate Policy. – Certification Practices Statement. – Security Profile (including SRMP and KMP). – Operations Manual. – Disaster recovery & Business Continuity Plan. • Specifications for hardware tokens from ASD Evaluated Products List (EPL).

Assessment Process

Demonstrated compliance with all the National privacy principles (NPPs), the Information Privacy Principles (IPPs) as applicable, and from 12 March 2014, all Australian Privacy Principles (APPs).

Providers to demonstrate completion of a NeAF risk assessment (reflected in the Identity Proofing Policy and Credential Management Policy and Practices Statement) and implementation of the appropriate provisions of ISO/IEC 29115 – Entity Authentication Assurance.

Details of the assessment processes required for Gatekeeper accreditation can be found at https://www.dto.gov.au/.

4. Assurance Framework for Government Agencies

Risk Management

Agencies **MUST** undertake a protective security risk assessment to determine the required LoA that Providers **MUST** demonstrate in order for the agency to rely on the services offered.

The PSPF states:

> *"Agencies **MUST** adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standard for Risk Management AS/NZS ISO 31000:2009 and the Australian Standards HB 167:2006 Security risk management."* (see http://www.protectivesecurity.gov.au/pspf/Documents/Protective%20Security%20Policy%20Framework.pdf)

Implementation of this Assurance Framework will require:

- Agencies intending to rely on services provided by third party Providers to undertake a thorough risk assessment (as per the PSPF) to determine the LoA required to be demonstrated by Providers. The outcome of the risk assessment, including all protective security measures and resultant residual risks, **MUST** be signed-off by the agency head.

Note that some services, such as the ability of individuals to store personal information and copies of documents may not be directly applicable to an agency's engagement with a Provider.

> For example, an individual may choose to store a digital copy of their Passport in their mailbox. The fact that the individual has a copy of their Passport stored in the mailbox may have no bearing on their interaction with a given agency. However, the fact that the Passport remains the property of the issuing agency will have implications for the security controls implemented by the Provider.

The nature and extent of data storage supported by the Provider will provide a necessary input into an agency's risk assessment. This is because the quantity and sensitivity of stored information will increase the attractiveness of the service as a target for cyber-criminals, and therefore the potential for compromise to agency operations.

The risk assessment should focus on the possible threats to the agency arising from reliance on the services to be offered by the Provider on which the agency intends to rely.

It should consider:

Mailbox/vault Services

The potential type and quantity of information that an individual may choose to store in their vault (e.g. electronic copies of personal documents, digital credentials, answers to shared secrets etc) as well as the aggregate volume of such data holdings.

Authentication Services

The type and volume of personal information/documentation that is collected and stored in order to issue an authentication credential (individual and aggregate), whether such data is verified and if so whether the verification outcomes are also stored.

Verification Services

The type and volume of personal information/documentation that may be collected and stored.

The risk assessment should include:

i. a protective security risk review.

ii. a National e-Authentication Framework (NeAF) assessment[15] as appropriate.

iii. an outsourcing or offshoring risk assessment as appropriate.

The *Australian Government Business Impact Levels (BILs)*[16] form a part of the PSPF. They provide agencies with common set of rules that leads to a consistent approach to assessing business impact from an Australian Government perspective. BILs will vary greatly between agencies, based on their functions and size. BILs in themselves do not measure the size of the risk associated with the information.

[15] The NeAF provides agencies with a methodology to undertake identity-risk assessments and thereby determine the level of authentication assurance required for a particular online transaction (or set of similar transactions). See http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html.

[16] http://www.ag.gov.au/Documents/Australian%20Government%20protective%20security%20governance%20management%20guidelines%20-%20Australian%20Government%20Business%20impact%20levels.pdf. See Annex 6 (Background Material) for details.

5. ICT Procurement

The Commonwealth Procurement Rules (CPRs) represent the Government Policy Framework under which agencies govern and undertake their own procurement and combine both Australia's international obligations and good practice. Together, these enable agencies to design processes that are robust, transparent and instil confidence in the Australian Government's procurement.

Further detail is available at http://www.finance.gov.au/procurement/procurement-policy-and-guidance/commonwealth-procurement-rules/index.html.

Limiting Supplier Liability in ICT Contracts with Australian Government Agencies

The Australian Government's ICT liability policy recognises that requiring unlimited liability and inappropriately high levels of insurance can be a significant impediment to companies wishing to bid for Australian Government contracts. This is particularly the case for small and medium sized ICT firms.

A Guide to Limiting Supplier Liability in Information and Communications Technology (ICT) Contracts with Australian Government Agencies, was issued in May 2010 (second Edition) by the Department of Industry, Innovation, Science, Research and Tertiary Education. This policy relates to Government agencies subject to the Financial Management and Accountability Act 1997 (the FMA Act) and requires that the liability of ICT suppliers contracting with agencies, in most cases, be capped or limited at appropriate levels based on the outcomes of a risk assessment. http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/Documents/LimitingLiabilityReport.pdf.

The ICT liability policy is stated in Finance Circular 2006/03 *Limited Liability in Information and Communications Technology Contracts*. Procurement related Finance Circulars are located at http://www.finance.gov.au/publications/finance-circulars/procurement.html and 2003/02 – Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort.

Additional Resources

Finance Circulars link is http://www.finance.gov.au/publications/finance-circulars/index.html.

6. Attachment 1: Supporting Information

Security Risk Management Plan

Given that one of the principal products 'sold' by a data-vault / digital mailbox Service Provider is 'trust', they **MUST** be able to demonstrate a thorough understanding of the security threats facing them, their clients and contracting agencies.

The Service Provider **MUST** document in their SRMP:

- a rigorous identification of possible threats and risks to its operations in accordance with the Australian Standard for Risk Management AS/NZS ISO 31000:2009 and the Australian Standards HB 327:2010, *Communicating and consulting about risk* and HB 167:2006 *Security Risk Management*; and
- effective threat mitigation plans that reduce the residual risk to a level acceptable to the Provider and Contracting Agency (and where necessary any document issuing agencies or authorities) respectively.

Protection of mission-critical assets involves the identification and classification of threats and risks to the Provider's facilities, IT systems, staff and other people; and development and implementation of appropriate risk management strategies including:

- physical security such as building construction, locks on doors and windows, alarm systems etc;
- personnel security such as employee screening and authentication;
- administrative or operational security, such as investigation of security breaches; and
- information/data security such as controlling access to and reproduction of sensitive material (e.g. personal information).

The key components in a Provider's SRMP should include at a minimum:

- system description
- data description / flows
- security policy objectives
- system users
- system mode
- physical security
- logical access control
- personnel security
- networking
- emergency destruction
- firewall management
- communications security and backup procedures
- disaster recovery / business continuity
- control of removable media
- inventory control

- data transfer procedures
- system maintenance
- audit
- security administration
- vulnerability awareness (including 3rd party assessments and penetration tests)
- configuration management
- system integrity and quality assurance
- security incident monitoring and management
- education and training

Personnel Security Management Plan

The use of appropriate personnel security measures can prevent or deter a wide variety of insider attacks against a provider's ICT systems and personal or sensitive information held by the Provider.

Decisions regarding personnel security **MUST** be made in the context of the Provider's Security Risk Management Plan.

All personnel and contractors **MUST** acknowledge the terms and conditions derived from the Personnel Security Management Plan as a condition of employment.

Where a Provider utilises secure data storage services from a third party (e.g. a cloud provider) that third party **MUST** have equivalent personnel security management plans in place.

The Personnel Security Management Plan **MUST** be audited at least annually to ensure the ongoing effectiveness of mitigation controls and a report prepared for the Contracting Agency.

For further information see:
http://www.protectivesecurity.gov.au/personnelsecurity/Documents/Agency%20personnel%20security%20guidelines.pdf

Incident Management Plan

IT Infrastructure Library (ITIL) terminology defines an incident as:

> *Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to or a reduction in, the quality of that service. The stated ITIL objective is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.*

The Incident Management Plan will address in particular security and privacy incident management.

The Incident Management Plan should be integrated within the Provider's Security Risk Management Plan.

The types of security incidents that Providers should address in their Plan include (but are not limited to):

- suspicious or seemingly targeted emails with attachments or links
- any compromise or corruption of information
- unauthorised access or intrusion into an ICT system

- data spills
- theft or loss of electronic devices that have processed or stored Australian government information
- theft or loss of electronic devices that have processed or stored personal or sensitive information
- intentional or accidental introduction of malware to a network
- denial of service attacks
- suspicious or unauthorised network activity

Personal information security breaches are not limited to malicious actions, such as theft or "hacking", but may arise from internal errors and failures to follow information handling policies, causing accidental loss or disclosure. If there is a real risk of serious harm as a result of a personal information security breach, the affected individuals **MUST** be notified.

Privacy

Privacy and Security are inherently linked insofar as good security practices will contribute to the protection of an individual's personal and sensitive information. Similarly an analysis of data flows will identify potential privacy issues that will require mitigation as part of the Provider's overall security risk management practices.

A Service Provider **MUST**:

- conduct a PIA that addresses measures to protect the privacy of an individual's communications with other organisations.
- publish their Privacy Policy that incorporates the outcomes of the PIA.
- require customers to acknowledge that they have read their Privacy Policy prior to registering for a mailbox/data-vault.

The *Privacy Act* does not refer to PIAs nor does it require agencies to undertake a PIA. However, the success of a Service Provider's offering will depend in part on it complying with legislative privacy requirements but more importantly how well it meets broader community expectations about privacy.

PIA's are usually undertaken as part of a sound risk management strategy, to assess whether it is safe to proceed to the implementation phase of the project. Further information on the conduct of PIA's can be found at http://www.privacy.gov.au/materials/types/guidelines/view/6590.

By feeding PIA information into their risk management processes, Service Providers will be in a better position to assess the level of risk which privacy impacts represent to their service offering, and decide on the most appropriate avoidance, mitigation or management strategies.

It is important to note however that, whilst information privacy is the regulatory focus of the Office of the Australian Information Commissioner, it is only one aspect of privacy more broadly. For example, there are other types of privacy (such as bodily privacy; territorial privacy; communications privacy).

A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws at Federal or State level and a breach of Australia's international human rights obligations. It may also result in prohibitive costs in retro-fitting a system to ensure legal compliance or address community concerns about privacy.

Providers are encouraged to read the Consultation Paper on "Reasonable steps to protect personal information" available at http://www.oaic.gov.au/publications/guidelines.html#other_privacy_guidance

Liability Policy

Service Providers **MUST**:

- Publish their Liability Policy in a prominent position on their website and require customers to acknowledge that they have read it prior to registering for a mailbox/data-vault service.
- Not seek to avoid or exclude liability for any breaches of its core obligations to ensure:
- the security of a customer's data-vault / digital mailbox;
- the prevention of unauthorised access to the information / data that is held within a Customer's data-vault / digital mailbox; and
- the privacy of any personal information that may be collected, used or disclosed by the Service Provider as a result of its service offering.

Consistent with the Guide to Limiting Supplier Liability in Information and Communications Technology (ICT) Contracts with Australian Government Agencies (May 2010 2nd Edition) Service Providers may cap or limit their liability at appropriate levels based on the outcomes of a risk assessment.