Workforce Identity and Access Management (IdAM)

Statement of Direction

for the Victorian Public Service

May 2017

VICTORIA State Government | Premier and Cabinet

Contents

Vision, purpose and document details

VISION	To provide the right people, with the right access, to the right ICT systems and resources regardless of hosting location, at the right time, for the right amount of time.		
PURPOSE	To ensure consistent identity and access services for the Victorian Government that enables efficient and effective management and secure, simple user access to department ICT systems and resources[1] for staff[2], business partners[3] and service providers[4], referred to collectively as 'workforce' throughout this document. In support of the Victorian Government IT strategic aim to be an 'employer of choice with robust, industrial strength back-end components that enable personal productivity systems and easy use of contemporary tools'.		
APPLIES TO	All Departments, Victoria Police & VPS as appropriate	**AUTHORITY**	Victorian Secretaries Board
PERIOD	2017 to 2020	**ADVISED BY**	DPC, in consultation with IdAM Working Group and CIO Leadership Group
ISSUE DATE	August 2017	**DOCUMENT ID**	SOD IDAM 01 - TRIM 17/216264
REVIEW DATE	August 2020	**VERSION**	1.0

[1] Department ICT Systems and Resources – includes department ICT applications, ICT systems, ICT assets (e.g. portable devices such as mobile phone, tablets, laptops) and physical security (e.g. buildings, computer rooms)

[2] Staff – a permanent or temporary employee, contractor, casual or volunteer. Note that contractors and volunteers are not currently stored in the majority of HR systems and the best approach for managing their access will be further assessed during development of the IdAM Strategy.

[3] Business Partner – Entity that performs business on behalf of government e.g. VicRoads car dealers, DHHS Community Service Organisations

[4] Service Provider – Entity that provides services to government including consultants e.g. Telstra network agent, HP data centre hosting operator, KPMG professional services consultant

Scope and context

Scope

The following departments and agencies, referred to collectively as ‘departments’, are formally in scope and the Statement of Direction is applicable to the Victorian Public Service as appropriate:

- Department of Economic Development, Jobs, Transport and Resources
- Department of Education and Training
- Department of Environment, Land, Water and Planning
- Department of Health and Human Services
- Department of Justice and Regulation
- Department of Premier and Cabinet
- Department of Treasury and Finance
- Victoria Police
- CenITex
- Court Services Victoria
- VicRoads

Related Documents

- *Information Technology Strategy, Victorian Government, 2016 to 2020,* DPC
- *ICT Network and Cyber Security Statement of Direction,* DPC, August 2016
- *Workplace Environment Statement of Direction,* DPC, *September 2015*
- *Human Resources Systems Statement of Direction,* DPC, August 2016
- *Finance Systems Statement of Direction,* DPC, August 2016
- *Victorian Protective Data Security Framework (VPDSF),* CPDP, July 2016

Introduction

Priority 3 of the *Victorian Government Information Technology Strategy 2016-20* (the IT Strategy) calls for technology reform so that 'Government employees should not be hindered in their effectiveness and responsiveness because of outdated tools, poor systems or a proliferation of different corporate systems trying to achieve the same outcome.'

Action 15 of the IT Strategy requires DPC to 'Develop a statement of direction for staff/contractor identity management, with a supporting implementation roadmap and business case to enable workplace, shared services and network standardisation'

What is IdAM

Identity and Access Management (IdAM) enables and manages access to Information and Communication Technology (ICT) systems and resources and is essential for protecting the confidentiality, integrity and availability of information held, used and shared.

IdAM achieves this by integrating authoritative sources of identity data, providing automated approval workflow for user on-boarding, movement and off-boarding, delivering simple, secure login services and enforcing authorised role-based access to ICT systems and resources.

IdAM is the trusted eco-system (see Figure 1) that ensures the right people, get the right access, to the right ICT systems and resources regardless of hosting location, at the right time and for the right amount of time.

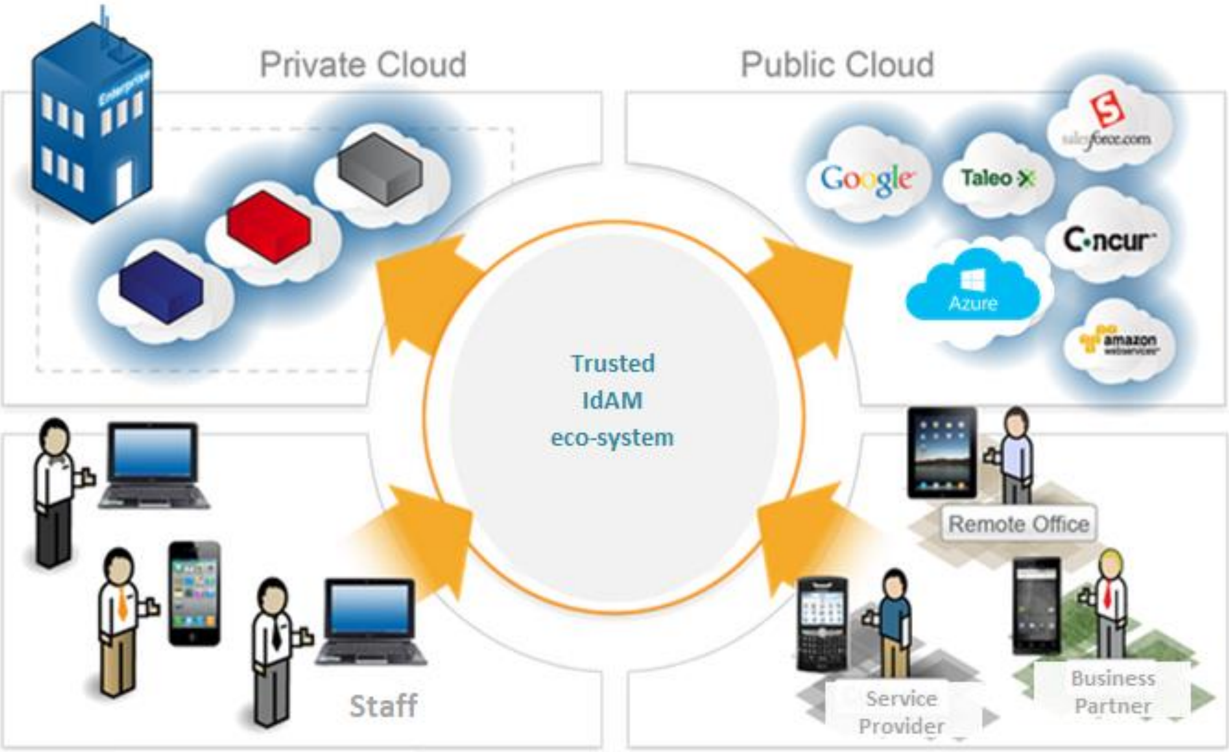


Figure 1 - Trusted IdAM eco-system

A simplistic depiction of the core components of an IdAM eco-system in the context of this Statement of Direction (SoD) are illustrated in figure 2 to assist reader understanding. Note that components 2, 3, 4 and 5 continually change and mature over time.

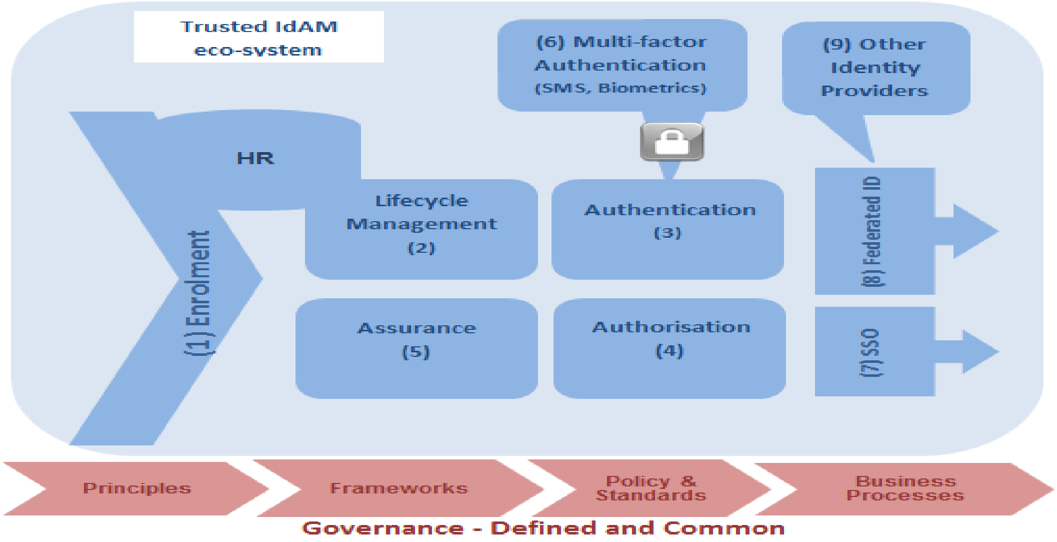


Figure 2 – Core components of trusted IdAM eco-system

Component	Description
1. Enrolment	Initial registration process and associated online interface and approval workflow for requesting access to ICT systems and resources. Includes on-boarding of identities into the IdAM and identity matching (process of linking identity records that relate to the same person).
2. Lifecycle Management	Automated provisioning of identities and entitlements into downstream ICT systems and resources, and online interface for the ongoing management of identities as they require changes to their access or exit an organisation.
3. Authentication	The initial component of access management that requires a user to demonstrate possession and/or control of a digital credential in order to establish confidence that the user is who they say they are (e.g. a login service that verifies a user when accessing a system).
4. Authorisation	The secondary component of access management that determines what a user can do with a particular system or resource based on entitlements of the identity, typically via group/roles and attributes, after successful authentication.
5. Assurance	Processes and activities to validate that predefined requirements are satisfied and give confidence that safeguards are functioning as intended.
6. Multi-factor Authentication	Method of access to ICT systems where a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following: knowledge (something they know, e.g. password), possession (something they have, e.g. token or SMS to mobile), or inherence (something they are, e.g. biometrics).
7. Single Sign-On (SSO)	Real-time authentication of a user to multiple applications using a single digital credential, typically their network logon, either without needing to present the digital credential again or representing the same digital credential.
8. Federated Identity	Arrangement made among multiple organisations that lets participants use the same identification data and digital credential to obtain access to multiple systems across the participating organisations.
9. Identity Provider	An system that has been accredited to participate in a federated identity management system to provide identity authentication services (e.g. login, tokens/assertions, logout).

Background

A decade ago, the Victorian Government implemented a hub and spoke identity management system that integrated, to varying degrees, the ten departments at that time. That Whole of Victorian Government (WoVG) IdAM established a central identity store, staff directory and a staff on-boarding application with automatic approval workflow for provisioning staff to nominated department applications. Some agencies integrated with Human Resources (HR) as their authoritative source of staff identity, but not all. The concept of a single WoVG identifier was introduced for identity tracking and facilitated by an online identity matching function, however a WoVG authentication capability was not established at that time.

Since then, some departments have expanded their local spokes to provision additional applications and provide authentication (login services). This has been implemented without strong governance to ensure interoperability, resulting in multiple point solutions and hindering secure cross-agency data sharing. Collectively this represents a significant cost across departments.

Four years ago, the shared services provider (CenITex) modernised and enhanced the staff on-boarding application and consolidated some of the hub and spoke infrastructure. Works are underway to expand use of the on-boarding application to more department and agencies. There is also opportunity to integrate the WoVG IdAM with WoVG Office365 / Sharepoint services to support automated provisioning of staff, and trial federated single sign-on services to department ICT systems in the cloud.

The Problem

Today, there are still a number of in-scope departments that do not participate in the WoVG IdAM system and, as such, cannot readily take up WoVG offerings. In response to critical services initiatives such as family violence recommendations, departments continue to plan and progress siloed solutions to meet pressing needs for access to sensitive ICT systems and data managed by other agencies.

A key contributor to the proliferation of multiple point solutions and high investment costs is the absence of a governing body, mandated policies, standards, frameworks and a lack of defined, common, streamlined business processes/practices.

In addition, the Victorian Government has a strong reliance on non-government organisations for provision of services to the community that require access to sensitive department systems and information. Departments to date have developed siloed IdAM solutions for these external users (referred hereafter as business partners) and are indicating that these solutions are in need of enhancement and/or replacement. An opportunity exists to take a more efficient and cost effective approach by providing a solution once across departments and standardising business partner processes.

Parallel to this, there has been significant development of new online systems and, with the 'Cloud First' policy, increasing leverage of cloud-based infrastructure-as-a-service (IaaS), software- as-a-service (SaaS) and platform-as-a-service (PaaS). Many of these implementations hold sensitive information and staff now have to access numerous applications and remember many logins and passwords. Single sign-on and multi-factor secure access is significantly lacking in most departments for on premise, legacy and cloud-based applications; contributing to poor user experience, reduced staff productivity and increased risk of compromise to the security of ICT systems and information.

The *Victorian Government IT Strategy 2016-2020* is also progressing a number of whole of government initiatives, including but not limited to, a strategic Human Capital Management (HCM) platform, Finance Platform, Application Programming Interface (API) Gateway and automated Briefing System. Each of these require government-wide identity and access management services and would benefit significantly from a single authoritative source of Victorian Government identities.

An environment scan of IdAM industry analysts (refer Appendix A – IdAM environment scan) reinforces the importance of:

1. protecting identity information and credentials as identity theft continues to be a popular past time for hackers
2. the significant role that a mature approach to IdAM has in preventing data breaches
3. the contribution that poorly managed and secured privileged access accounts play in security breaches.

There is opportunity to better manage privileged access across departments, both operationally and in terms of best practice standards and guidance. In line with cyber-security recommended controls, this domain warrants a stronger focus going forward.

These requirements support the need for a governed, consistent, efficient, and effective IdAM eco-system. A system that can deliver increased productivity for department users with single sign-on and protection of our identities/credentials/ICT systems and resources with authoritative and up-to-date user lifecycle management.

Key objectives and benefits

Key Objectives

- Establish a trusted, governed, managed, integrated and secure IdAM eco-system to manage workforce access to Victorian Government department ICT systems and resources.
- Establish Workforce IdAM as the authoritative source of truth for electronic identity.
- Stand up a governance body, policies, standards, frameworks and procedures that ensure a trusted, managed, cohesive and secure IdAM eco-system.
- Creation, verification and matching of staff identity performed by HR as the authoritative source.
- Improve quality of identity data to enable trusted IdAM services across departments.
- Develop common business processes and automate in online solution for staff enrolment and lifecycle management (access requests, moves and exits).
- Develop common business processes and automate in online solution for business partner and service provider enrolment and lifecycle management.
- Extend online enrolment and lifecycle management of workforce access to other department ICT systems and resources.
- Simplify user login experience with single sign-on and federated identity.
- Easy, secure login for access to sensitive ICT systems and resources eg. SMS, biometrics.
- Uplift access practices to satisfy separation of duty and just-in-time principles and ensure that information confidentiality and integrity is maintained.
- Facilitate compliance assurance through timely and up-to-date monitoring, tracking, audit, reporting and dashboard functions.
- Proactive security incident management and forensic analysis through accurate, real-time logging, monitoring, detection and alerting (Security Incident & Event Management - SIEM).

Benefits

- Re-use of trusted identity across departments, business partners and service providers.
- Staff identity tracking to support improved employee screening processes.
- Streamlined, automated business processes that drive business efficiency and effectiveness for workforce lifecycle management and machinery of government changes.
- Improved provisioning of access to all types of ICT applications - legacy, web and cloud.
- Cost-effective IdAM investment, avoiding multiple procurements and point solutions.
- Improved efficiency and effectiveness of managing access to ICT systems and resources for greater workforce productivity.
- Improved user experience to support being an employer of choice.
- Reduced risk of data breaches and compromised ICT systems from external and insider threat through improved privileged access management and security incident management.
- Improved compliance and assurance of legislation and industry regulations.
- Improved investment and decision making.

Direction

The Victorian Government Workforce IdAM Statement of Direction defines the vision for a trusted, managed, governed, integrated and compliant IdAM for its workforce.

Figure 3 illustrates a high level reference model for IdAM as the provider of seamless access for users to ICT systems and resources by capabilities, delivered through an eco-system, that is managed by strong governance.

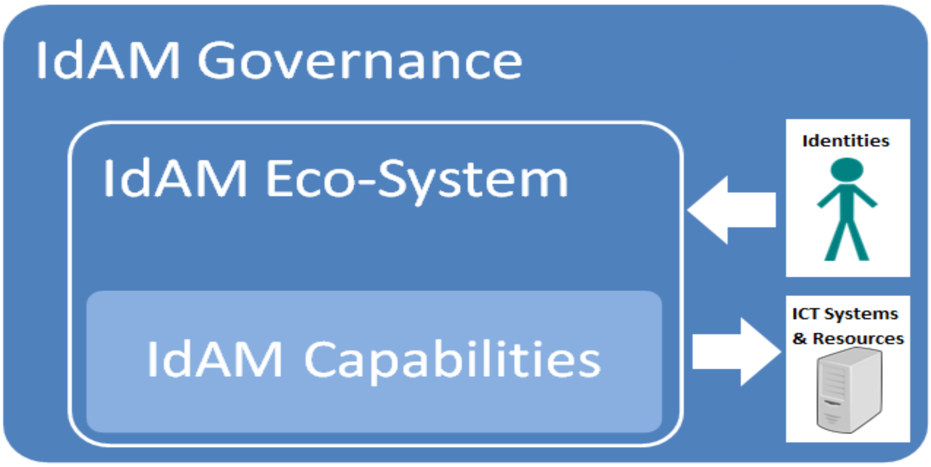


Figure 3 - High Level IdAM Reference Model

Identity scope

Users

The scope of user identities addressed by this Statement of Direction is workforce users of department ICT systems and resources that includes departmental staff, business partners and service providers (see Figure 4). Staff includes full and part-time employees, contractors, casuals and volunteers. Customers (consumers and citizens) are not in scope. Refer to the glossary for definitions of these user types.

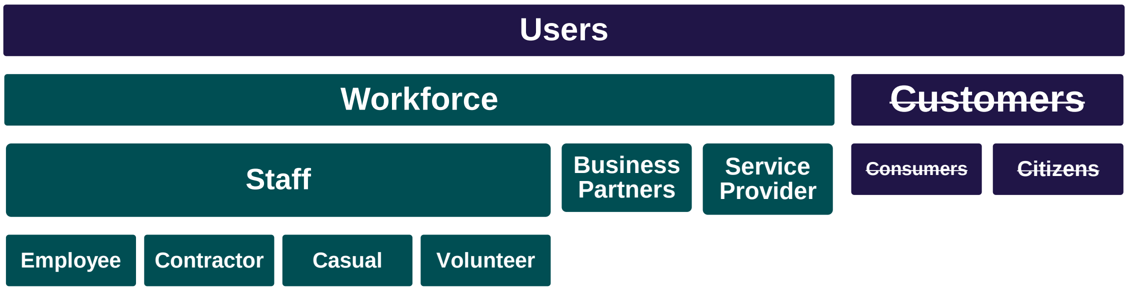


Figure 4 - User scope

Note that contractors and volunteers have been grouped in the staff category and as such, over time they will be stored in and supplied by authoritative HR systems. This does not reflect current practice for many departments and may not be feasible for some in the future. A department's definition of volunteer is also likely to be a factor.

Further assessment will be undertaken during the IdAM Strategy phase to understand how these identities are managed across departments, validate requirements, and consider impact on HR business processes and costs. They may warrant being treated separately or more closely aligned with Business Partner or Service Provider processes.

Non-Users

Non-user accounts are also in scope and will be addressed as part of the Privileged Access capability. They include:

- system, network, database administrator accounts
- software development lifecycle (SDLC) accounts including development, testing, user acceptance testing (UAT) and training
- service accounts e.g. SFTP
- application accounts e.g. WebAPI
- device accounts.

ICT systems & resources scope

ICT systems and resources (Figure 5) includes all department ICT systems regardless of hosting location, including but not limited to: on premise; web-based; private-cloud and public-cloud applications. Resources include access to physical assets such as buildings, computer rooms and portable devices e.g. mobile phones, laptops and printers.

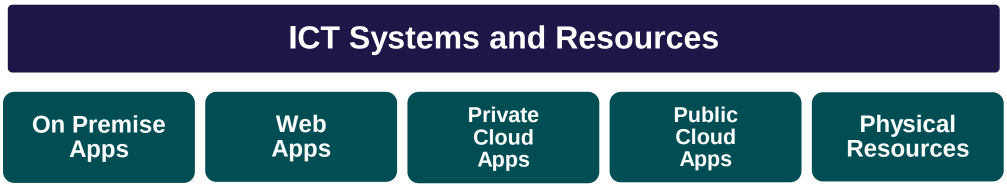


Figure 5 - ICT systems and resources scope

A detailed Workforce IdAM reference model (see Figure 6 below) articulates the scope and key components of the Workforce IdAM described in this Statement of Direction, and guides the structure of the next section of the Direction Statements.

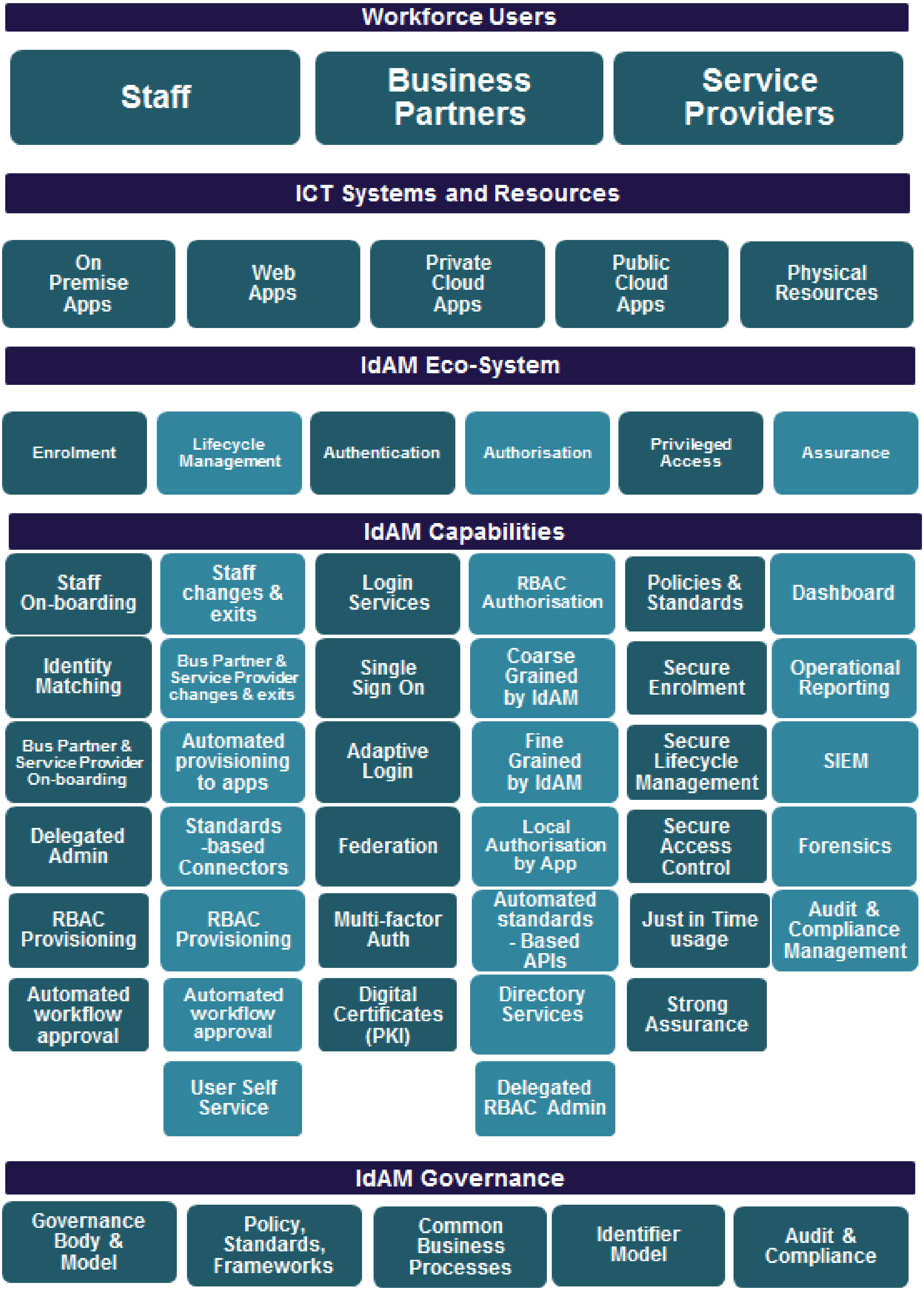


Figure 6 - Workforce IdAM Reference Model

Direction statements

The following direction statements, along with Figure 7 below, set out the requirements for a trusted, managed, governed, integrated and compliant IdAM eco-system for the Victorian Government workforce.

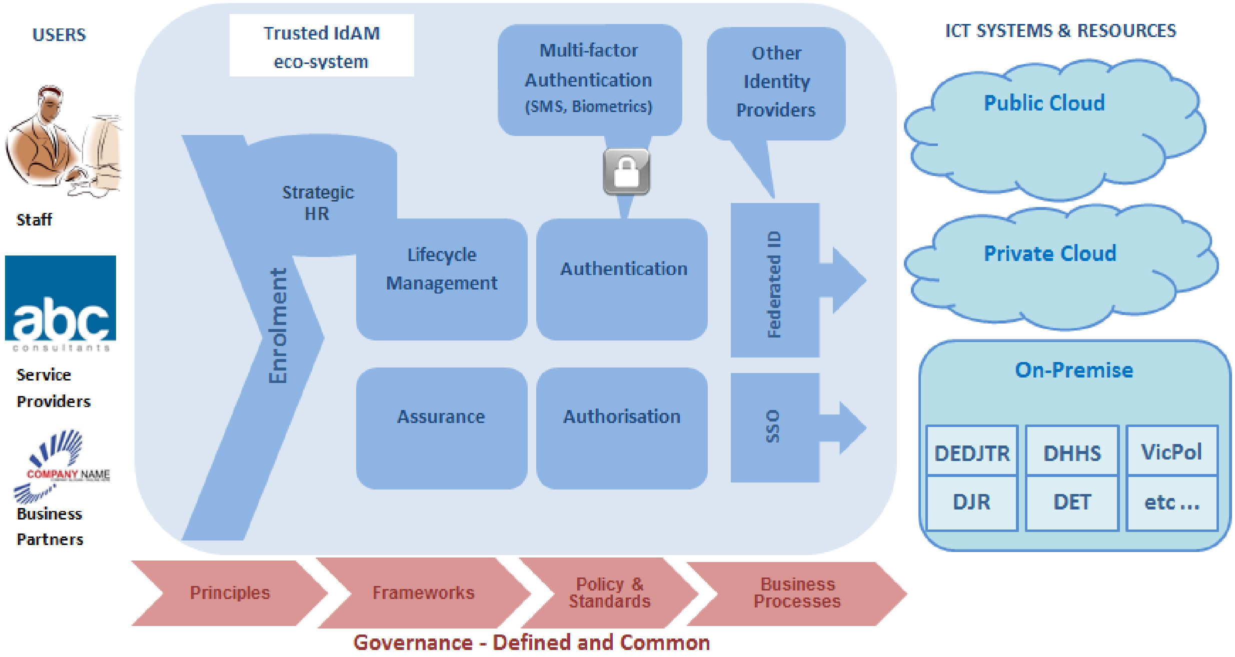


Figure 7 - WoVG Workforce IdAM eco-system

Over time, HR systems will become the authoritative source for all staff identities and HR services will be responsible for staff identity matching.

Staff will have single sign-on access to department ICT systems and resources, internal and cross-agency, regardless of location on premise or in the cloud.

Business partners and service providers will have efficient enrolment services and federated identity to support easy login and controlled access to department ICT systems and resources.

Automated role-based access provisioning and de-provisioning to legacy, on premise and cloud applications for streamlined user access management and improved security

Secure multi-factor authentication methods such as SMS and biometrics, combined with best-practice privileged access management, will protect sensitive information and critical systems.

All of this will be assured by the strong governance of a responsible body, defined frameworks, policies and standards, and audit and compliance functions and tools.

Supported by an approach that leverages and extends fit-for-purpose existing government infrastructure and capability, is aligned with department and CenITex strategic directions, and embraces industry advances in federated identity, biometrics and cloud-based offerings.

IdAM Principles

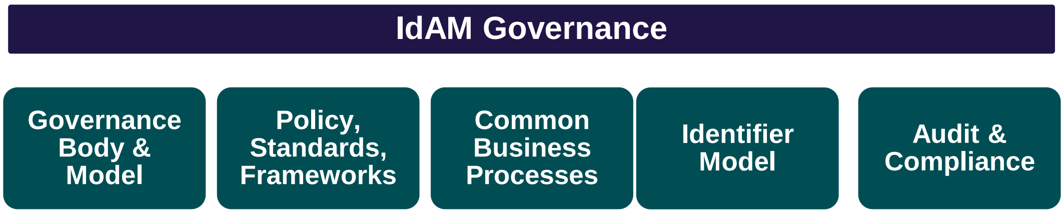
Objective

Ability to uniquely identify and manage a person's access rights to Victorian department ICT systems and resources.

Reference	Direction	Purpose
ID-01	One persistent IdAM Identifier for staff across Victorian Government (the VGID)	• To create a unique identifier for use across the Victorian Government ICT systems (the VGID). • The unique identifier is reused. For example, upon re-engagement i.e. persistence. • Informed by and associated with the unique employee identifier from strategic or department HR system to support staff employment tracking, competency tracking and entitlement changes. • Ability to associate multiple identity records relating to the same staff user via an identity matching function to enable robust and timely off-boarding. • Enables efficient Machinery Of Government changes • Validated 'Level of Assurance' assigned to identity in line with identity trust framework.
ID-02	A persistent, unique department network logon for staff	• To establish a department network logon for staff that can be used to access enterprise, line-of-business and common (shared) department ICT systems, regardless of hosting location, and resources. • Is unique within and across Victorian Government departments. • Is used for the purpose of engagement of the hiring department. • Users working in more than one department at a time may be issued separate network logons for each engagement. • Is reused on staff re-hire within same department. • Is associated with the persistent VGID. • Is of a common derivation and format across departments. • Can be used for single sign-on to ICT systems and resources.
ID-03	A persistent, unique department email address for staff	• To establish a department email address that can be used to access enterprise, line-of-business and shared department ICT systems, regardless of hosting location, and resources. • Is unique within and across Victorian Government departments. • Is used for the purpose of engagement of the hiring department. • Users working in more than one department at a time may be issued separate email addresses for each engagement. • Is reused on re-hire with same department. • Is associated with the persistent VGID. • Is of the common format *first.last.[id]@[dept/agency].vic.gov.au.* • May be used as a username for logging in to applications.
ID-04	External (non-staff) identities issued by the Workforce IdAM will not be identity matched	• Multiple identity records that belong to the same person will not be linked for external (non-staff) identities such as Business Partners or Service Provider users that are generated by the Workforce IdAM. • Compliance with Privacy. • So legal obligation or requirement to do so.
ID-05	Credentials issued for external identities (non-staff) by the Workforce IdAM will have a defined format	• External (non-staff) identities such as Business Partner and Service Provider identities that are generated by the Workforce IdAM will be issued with a defined format user name and secure compliant password. • Assists with easy user type identification. • Increased security with secure compliant passwords.

Reference	Direction	Purpose
ID-06	Mandate ICT applications integrate with WoVG IdAM centralised directory or federated identity service.	- Mandate departments to develop/procure and implement solutions that use an external authentication service i.e. not their own local store. - Ensures use of trusted electronic identity that is managed and store once. - Return on investment for WoVG IdAM. - Reduced IdAM capability costs and operational overheads for ICT applications .
ID-07	Identity is controlled by the hiring organisation	- The owners of the identity are responsible for lifecycle management. - Ability to readily apply relevant policies in line with risk profile. - Allows for separation between internal (staff) and external users (business partner/ service provider) identities for reduced risk of compromise to staff (internal) identities.

IdAM Governance



IdAM Governance

Governance Body & Model

Policy, Standards, Frameworks

Common Business Processes

Identifier Model

Audit & Compliance

Objective

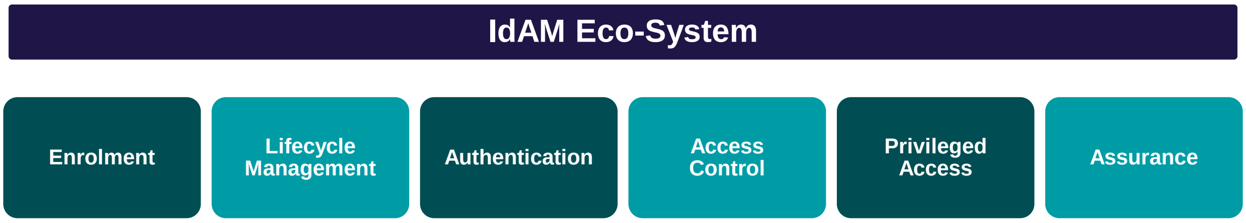
Strong governance and compliance for managing a trusted, governed, managed, integrated, efficient, effective and shared identity and access management eco-system for workforce identity.

Reference	Direction	Purpose
GV-01	**Governance Body & Model** Defined and established governance model and responsible body	- Clear ownership of identities that access department ICT systems and resources. - Body with clear accountability for governance, risk and compliance of identity and access management service and data. - Ensure necessary frameworks, policies and standards are developed, approved and adopted. - Clear department roles and responsibilities ensuring mandatory processes are embedded, adhered to and realigned as needed - Identity matching function is mandated with defined ownership, roles and responsibilities. - Advisory groups and user forums to ensure ongoing fitness-for-purpose and quality of service. - Agreements with participating departments for data sharing and federation of identities e.g. MOU, IPA.
GV-02	**Policy, Standards, Frameworks** Defined and agreed Identity Trust Framework	- Provides structure, rules and controls to govern participants in a federated identity eco-system. - Defines a ‘Level of Assurance’ model to support secure federated identity for use by applications. - Facilitates entitlement based access to ICT systems and resources. - Aligned with Federal Trusted Identity Framework (DTA/DTO), and the NeAF and NIPG guidelines as required by VPDSS.

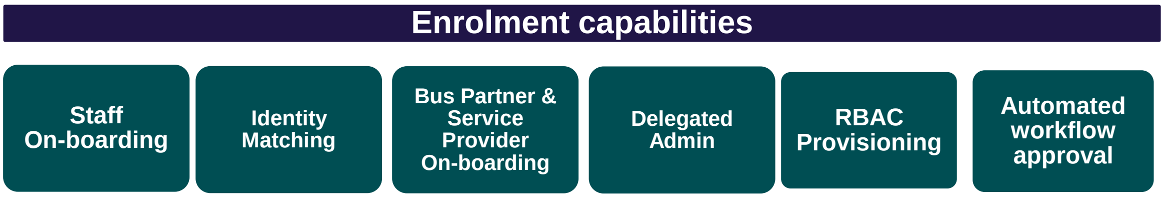
Reference	Direction	Purpose
GV-03	**Policy, Standards, Frameworks** Developed and published policies, standards and guidelines	• Agreed rules for use of a shared IdAM capability to ensure quality and integrity of identity data and access. • Aligned with federal and state government standards and practices e.g. Information Security Manual (ISM). • Privacy is ensured by compliance with the Privacy Data Protection Act 2014 and associated Victorian Protective Data Security Protection Framework and Standards (VPDSF/VPDSS). • Drives consistency of employee screening practices for staff and external identities accessing department ICT systems. • Drive good identity and access management practices and continual improvement across departments. • Drive consistency and interoperability of IdAM systems and applications through procurement and operational standards.
GV-04	**Common Business Processes** Defined, agreed and embedded common business processes	• Consistent business practices across departments making user provisioning easier when IdAM and HR staff change. departments (Victorian government has an active secondment culture). • Consistent business practices for external identities accessing department ICT systems & resources. • Low maintenance, efficient and effective on-boarding and off-boarding of identities (user & non-user) that can be more readily refined and matured over time. • Safeguards more readily embedded into business practice across departments.
GV-05	**Identifier Model** Defined and agreed identifier model	• Defines who, when, how and where participants in the IdAM eco-system can generate, store and use unique identifiers, including but not limited to, the VGID, HR Employee identifier and business partner / service provider identifiers. • Ability to associate multiple identity records relating to the same person for access control and timely off-boarding. • Determine position on username formats determined by federated Identity Providers.
GV-06	**Identifier Model** Defined, agreed, comprehensive identity schema	• Standardised identity data fields and associated formats and content to ensure system integrity and interoperability. • Improved analytics and reporting capability. • Enable automated system and application integration via exposed web interfaces and APIs. • Support of Action 5 Master Data Sets.
GV-07	**Audit & Compliance** Operational Audit and compliance function	• A nominated WoVG business area responsible for ensuring operational compliance of IdAM service and participating agencies. • Ensure ability to demonstrate control over who has access to what and contextual, continuous user access monitoring in place. • Organise, facilitate and progress recommendations of internal audits. • Facilitate response to and progress recommendations from external audits. • Facilitate WoVG and agency risk attestation.
GV-08	**Audit & Compliance** WoVG identity support services	• Department support in the event of a breach of workforce, business partner or service provider identity e.g. ID-Care. • Identity incident response planning assistance. • Access to industry forums to keep up-to-date and for knowledge sharing e.g. Biometrics Institute. • Reduced membership/subscription costs by sharing across departments or sponsored by DPC.

IdAM Eco-system and Capabilities

The high level core capabilities of an IdAM eco-system that are in scope for this statement of direction, as per Workforce IdAM reference model (refer to Figure 6), are repeated in the diagram below and guide the structure of the following section.



Enrolment



Objective

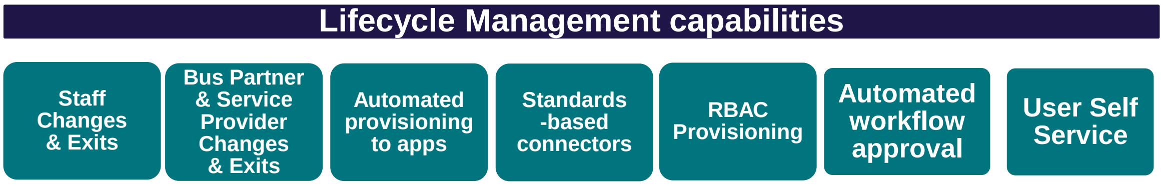
Deliver a defined, fit-for-purpose and efficient identity onboarding and matching capability to ensure accurate and authorised access to ICT systems and resources.

Reference	Direction	Purpose
EN-01	**Staff On-boarding** A trusted, governed, managed and easy-to-use online on-boarding capability for staff access requests to ICT systems and resources.	• Automated, repeatable, robust, efficient and effective implementation of business process. • Improved turn-around of access requests. • Assurance that the right people have the right access to the right systems at the right time. • Reduced number of data breaches due to mature and robust on-boarding approval processes and timely off-boarding.
EN-02	**Staff On-boarding** The Strategic HR (HCM) system, or department equivalent system, to become the authoritative source of staff identities for on-boarding and provider of a unique, persistent HR employee identifier.	• HR system to become the authoritative source for employees, contractors, casuals and volunteers*. • Accurate, timely and authoritative granting and removal of access to ICT systems and resources. • Consistent provisioning based on robust, compliant, repeatable processes. • Unique, persistent employee identifier provided by HR for association with the VGID. * This will have business process and cost implications for People and Culture (HR) that requires further consultation and evaluation as part of the IdAM strategy, solution design and implementation.

Reference	Direction	Purpose
EN-03	**Identity Matching** HR will manage and perform the staff identity matching function. • *Short-Term:* maintain status quo - staff identity matching capability provided by WoVG IdAM and performed in the line of business (e.g. by line managers, on-boarding champions, EAs) • *Medium-Term:* staff identity matching capability provided by WoVG IdAM but function is performed by HR • *Long-Term:* staff identity matching capability provided by strategic HR platform and performed by HR.	• Identity verification performed by responsible and authoritative area with access to all the necessary staff identity information to perform the match e.g. Date of birth. • Facilitates workforce tracking. • Facilitates improved alignment between employee screening, ICT access compliance requirements and determination of a level of identity assurance for workforce users.
EN-04	**Identity Matching** A common flexible staff identity matching capability that allows • matching during or post on-boarding • configurable nominated responsible officer(s)	• Low impact identity reconciliation function to facilitate streamlined staff enrolment. • Enable responsible officers to have choice when identity matching is performed. • Nominated responsible party is configurable to support transition of identity matching function to HR over time. • Improved data quality and identity reconciliation outcomes.
EN-05	**Business Partner & Service Provider On-boarding** A trusted, governed, managed and easy-to-use online on-boarding capability for business partner and service provider access requests to ICT systems and resources.	• Automated, repeatable, robust, efficient and effective implementation of business process. • Improved turn-around of access requests. • Assurance that the right people have the right access to the right systems at the right time. • Reduced number of data breaches due to mature and robust on-boarding approval processes and timely off-boarding.
EN-06	**Delegated Admin** A delegated administration capability to support business partner and service provider on-boarding	• Enable external organisations to locally manage and authorise access requests. • Further improved turn-around of access requests. • Reduced administration burden for departments.
EN-08	**Role-Based Access Control (RBAC) Provisioning** Establish access based on position titles, attributes roles, etc (RBAC/ABAC)	• Low maintenance, consistent, repeatable and accurate enrolment to ICT systems and resources based on role rather than the individual. • Initial access is aligned with the authoritative source (HR).
EN-09	**Automated workflow approval** A common approval workflow capability that facilitates • Line Manager approval • determination of a level of identity assurance • identity assurance step-up escalation management	• Low maintenance, consistent, repeatable and robust user provisioning practices. • Instantiation of an identity trust framework to support secure federated identity across departments and external identity providers. • Ability to increase level of assurance of an identity (step-up) for access to more sensitive ICT systems and information. • Robust approval processes with follow up for process closure.

Reference	Direction	Purpose
EN-10	**Other** A fit-for-purpose administration interface to manage workforce access, run reports and troubleshoot issues.	• Customised to meet administrator needs. • Reports to facilitate data cleansing activities. • Ability to override workflow constraints and issues with approval. • Reduced demand on IdAM technical specialists to resolve operational problems.

Lifecycle Management


Lifecycle Management capabilities

Staff Changes & Exits

Bus Partner & Service Provider Changes & Exits

Automated provisioning to apps

Standards -based connectors

RBAC Provisioning

Automated workflow approval

User Self Service

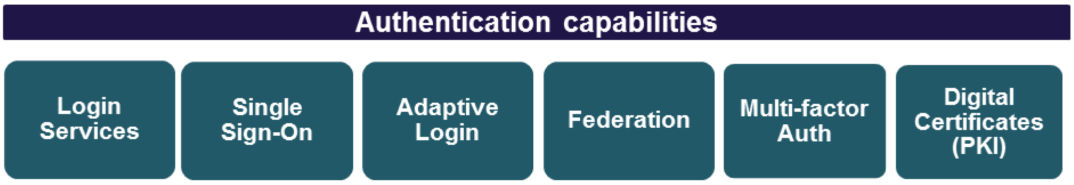
Objective

Deliver common, fit-for-purpose and efficient identity lifecycle management and provisioning of access to ICT systems and resources.

Reference	Direction	Purpose
LM-01	**Staff Changes & Exits** A trusted, governed and managed online lifecycle management capability for changing and revoking staff access to department ICT systems and resources.	• Automated, repeatable, robust, efficient and effective implementation of business process. • Improved turn-around of access changes and revocation. • Assurance that the right people have the right access to the right systems at the right time. • Reduced number of data breaches due to mature and robust on-boarding approval processes and timely off-boarding.
LM-02	**Staff Changes & Exits** The Strategic HR (HCM) system, or department equivalent system, will be the authoritative source for movement and revocation of staff access on exit.	• Accurate, timely and authoritative changes to staff access to ICT systems and resources when staff move. • Accurate, timely and authoritative removal of staff access to ICT systems and resources when staff exit. • Consistent data clean up on staff exit based on robust, compliant, repeatable processes. • Reduced risk of compromise to sensitive information and critical ICT systems and resources. • Enabled by integration with HR and association between HR employee identifier and the VGID.
LM-03	**Business Partner & Service Provider Changes & Exits** A trusted, governed and managed online lifecycle management capability for changing and revoking business partner and service provider access to department ICT systems and resources.	• Automated, repeatable, robust, efficient and effective implementation of business process. • Improved turn-around of access changes and revocation. • Assurance that the right people have the right access to the right systems at the right time. • Reduced number of data breaches due to mature and robust on-boarding approval processes and timely off-boarding.

Reference	Direction	Purpose
LM-04	**Automated provisioning to apps** Automated provisioning of user access and attributes to ICT systems and resources	• User identity and attributes populated in local application stores/databases for local authorisation. • Consistent, robust, efficient and effective implementation of time-consuming business process and complex technology activities. • Real-time turn-around of access requests, changes and revocation when staff exit.
LM-05	**Standards-based Connectors** Provisioning connectors based on industry standards	• Reusable, interoperable interfaces. • Continued support of legacy systems. • Supports pattern-based development. • Reducing SDLC costs.
LM-06	**RBAC Provisioning** Ongoing access based on position titles, attributes roles, etc (RBAC/ABAC)	• Low maintenance, consistent, repeatable and up-to-date granting or removal of access to ICT systems and resources based on role rather than the individual. • Access is aligned with the authoritative source (HR) and readily updated as position title, role or other attributes change.
LM-07	**Automated workflow approval** A common approval workflow capability that facilitates • Line Manager approval • determination of a level of identity assurance • identity assurance step-up escalation management	• Low maintenance, consistent, repeatable and robust user provisioning practices. • Instantiation of an identity trust framework to support secure federated identity across departments and external identity providers. • Ability to increase level of assurance of an identity (step-up) for access to more sensitive ICT systems and information. • Robust approval processes with follow up for process closure.
LM-08	**User Self Service** A common user self-service capability to perform simple administration tasks e.g. maintain contact details and password reset	• Timely resolution of low-risk, low impact user problems i.e. not privileged accounts. • Reduced demand on Service Desk (level 1 support). • Improved quality and accuracy of identity data.

Authentication



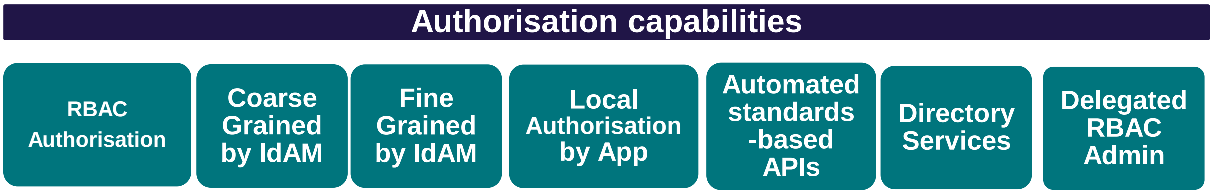
Objective

Deliver a defined, fit-for-purpose, secure and easy-to-use authentication capability that enables single sign-on and federated identity for sharing across participating departments and external organisations.

Reference	Direction	Purpose
AU-01	**Login Services** Authentication services for workforce users to ICT systems and resources that are capable of directory authentication, regardless of hosting location and device type (Refer statement ID-04)	• Improved staff, business partner and service provider productivity with easy login to applications. • Re-use of trusted electronic identity. • Facilitates cross-department system access and information sharing. • Consistent user login experience for legacy, web and cloud applications, regardless of hosting location. • Provide mobile and other portable device authentication.
AU-02	**Login Services** Authentication services based on secure, open or de facto industry standards	• Supports store-once and re-use of electronic identity. • Cost-effective, reusable, secure identity data exchange services. • Ready integration with web applications, on premise or cloud. • Enables cross-domain authentication. • Consider commonly-used standards such as Microsoft Azure AD, LDAP, SAML 2, OAuth, OpenID. • Support for other WoVG IT Strategy initiatives such as API Gateway for cross-agency data sharing, strategic HR, Finance and the App Store.
AU-03	**Single Sign-On** Single Sign On (SSO) to department ICT systems and resources	• Improved employee, business partner and service provider productivity with easy login to applications using network or email login. • Improved security as users no longer need to write down or share login details. • Reduced IdAM administration and support desk overheads with fewer credentials to maintain.
AU-04	**Adaptive Login** Adaptive (risk-based) login to ICT systems and resources based on environment and other variables	• Configurable access based on environmental circumstances and other aspects such as device type, location, time of day, etc. • Impacts user login experience only when necessary. • Reduced risk of compromise to protected sensitive information and critical systems.
AU-05	**Federation** Federated Identity Provider services for staff access to department ICT systems and resources	• Users, typically staff, can log in to cloud applications that participate in the federated eco-system using their network login or email address (single sign-on) application dependent. • Improved security by containing identity access and management data in the home security domain e.g. passwords. • Improved privacy by sharing minimal identity information and only at the time it is needed e.g. date of birth.
AU-06	**Federation** Federated Relying Party services for business partner and service provider access to department ICT systems and resources	• Users, typically business partners and service providers, can log in to department ICT applications using their own organisation's nominated login (application dependent). • Ability to leverage other trusted identity sources. • Reduced identity administration for departments. • Improved privacy by consuming only necessary identity information at the time it is needed.

Reference	Direction	Purpose
AU-07	**Multi-factor Authentication** Multi-factor secure authentication services and step-up facility based on common data classification scheme and levels of identity assurance e.g. SMS, biometrics	• Improved security for sensitive information and critical systems. • Access based on agreed risk profiles that comply with VPDSS data classification scheme (issued by Commissioner for Privacy and Data Protection). • Access based on agreed levels of identity assurance that align with federal identity trust frameworks from the Digital Transformation Agency. • Expensive, complex technologies such as biometrics invested in once.
AU-08	**Digital Certificates (PKI)** Public Key Infrastructure (PKI) and certificate management capability for issuing, managing and revoking digital certificates	• Secure, trusted, seamless authentication to, and between, applications and device-based authentication. • Provide public key cryptography to protect privacy and data. • Support secure digital signing of documents and transactions. • Improved security for sensitive information and critical systems. • Expensive, complex technologies invested in once.

Authorisation


Authorisation capabilities
RBAC Authorisation
Coarse Grained by IdAM
Fine Grained by IdAM
Local Authorisation by App
Automated standards-based APIs
Directory Services
Delegated RBAC Admin

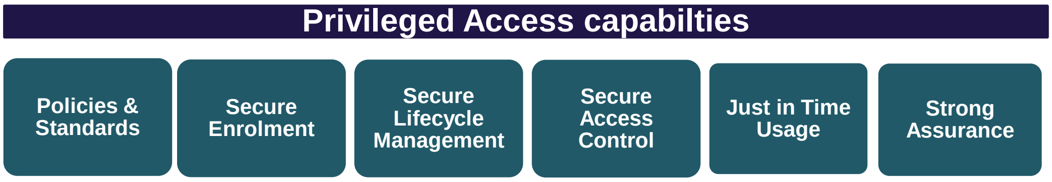
Objective

Deliver a defined, fit-for-purpose, role based authorisation capability that supports centralised coarse and fine grained access control and allows authorisation to be performed locally by applications as appropriate.

Reference	Direction	Purpose
AC-01	**RBAC Authorisation** Authorisation model based on position titles, attribute, roles etc.	• Provide entitlements management to control who has access to what. • Low maintenance, consistent, repeatable and up-to-date control of access to ICT systems and resources based on role rather than the individual. • Access is aligned with the authoritative source (HR) for staff and can be readily updated when position title, role or other attributes change.
AC-02	**Coarse grained by IdAM** Coarse-grained authorisation provided by IdAM at time of granting access to an ICT system or resource	• Simple, consistent, centrally managed, low maintenance access control. • Ability to easily control and change entry to an application based on role or group (supports RBAC). • Access aligned with the authoritative source of electronic identity.

Reference	Direction	Purpose
AC-03	**Fine grained by IdAM** Fine-grained authorisation provided by IdAM once a user has been granted access to an ICT system or resource	• Consistent, centrally managed, access control. • Ability to control access within an application based on a variety of attributes of the user such as position title, building, floor, etc (supports RBAC). • High degree of control over what a user can do in an application or with a resource. • Increased security aligned with 'need to know' and relative to functions being performed in the application.
AC-04	**Local Authorisation by App** Authorisation by application against own local store	• Allows fine grained access control within an application. • Support legacy and off-the-shelf applications.
AC-05	**Automated Standards-Based APIs** Authorisation services, based on secure, open or de facto industry standards that facilitate automation of access management	• Cost-effective, reusable, secure identity data exchange services. • Ready integration with web applications, on premise or cloud. • Enables cross-domain authentication and authorisation. • Consider commonly used standards such as Microsoft Azure AD, LDAP, SAML 2, OAuth, OpenID. • Support for other Victorian Government IT Strategy initiatives such as API Gateway for cross-agency data sharing, strategic HR, Finance and the App Store.
AC-06	**Directory Services** A Victorian Government staff listing	• An authoritative listing of all staff to facilitate easy communications within and across departments. • Up-to-date data maintained by the user via a self-service interface . Refer LM-08 User Self Service.
AC-07	**Delegated RBAC Admin** A delegated administration capability to support external role management	• Enables business partner administrators to manage roles where role based access details are being asserted from an external directory. • Improved turn-around of access control changes. • Reduced administration overhead for departments.

Privileged Access



Privileged Access capabilties

Policies & Standards

Secure Enrolment

Secure Lifecycle Management

Secure Access Control

Just in Time Usage

Strong Assurance

Objective

Defined and agreed strategic and operational management of identity and access for privileged access across departments to ensure processes and controls are in place to protect ICT systems and resources from deliberate and inadvertent misuse of privileged accounts.

Scope

Privileged Access scope includes

- System, network, database administrator accounts
- Software development lifecycle (SDLC) accounts including development, test, UAT and training
- Service accounts e.g. SFTP
- Application accounts e.g. WebAPI
- Device accounts.

Reference	Direction	Purpose
PA-01	**Policies & Standards** Policies, standards, and frameworks for privileged identity and access management	• Facilitate compliance with federal and state government standards and practices e.g. Victorian Protective Data Security Standards (VPDSS), Information Security Manual (ISM). • Consistent, secure privileged access management across departments based on least privilege, segregation of duties and just-in-time control. • Common, more secure SDLC account practices. • Managed and secured service accounts. • Streamlined policy development and maintenance, once across departments.
PA-02	**Secure Enrolment** Common, secure online enrolment for approval and creation of privileged access	• Enforced strong verification processes aligned with NeAF identity verification standards e.g. police checks, employment history checks, for improved assurance. • Robust and enforced approval processes. • Least privilege for reduced risk of compromise of sensitive information and critical business systems.
PA-03	**Secure Lifecycle Management** Common, secure online lifecycle management for maintaining and revoking privileged access	• Robust and enforced strong approval processes for improved assurance. • Reduction in orphan privileged accounts for reduced risk of compromise to sensitive information and critical business systems. • Least-privilege entitlement approach for reduced risk of compromise to sensitive information and critical business systems. • Allow IT administrator access without exposing administrator passwords or root-account credentials
PA-04	**Secure Access Control** Multi-factor authentication services and step-up facility for privileged accounts e.g. SMS, biometrics	• Improved security at time of use of privileged account for reduced risk of compromise of sensitive information and critical systems. • Authentication based on agreed risk profiles. • Expensive, complex technologies procured and invested in once. • Manage, control and record privileged account activities for all authenticated systems across physical and virtual environments.
PA-05	**Just in Time usage** Tools for enforcement of just-in-time use of privileged accounts	• Time restricted use of privileged access for reduced risk of compromise to sensitive information and business critical systems. • Enforced segregation of duties. • Expensive, complex technology procured and invested in once. • Robust tracking of privileged access use.

Reference	Direction	Purpose
PA-06	**Strong Assurance** Operational Reporting capability	• Improved visibility of privileged access abuse to reduce risk of compromise to sensitive information and critical business systems • Low maintenance • Provide assurance on privileged access • Facilitate improved compliance • Support audit activities • Facilitate improved data quality.

Assurance

Assurance capabilities

Dashboard

Operational Reporting

SIEM

Forensics

Audit & Compliance

Objective

Robust, timely incident and event management logging, monitoring, alerting and reporting capability for incident prevention and response, and facilitation of legislative and regulatory audit and compliance obligations.

Reference	Direction	Purpose
AS-01	**Dashboard** IdAM Service Dashboard	• High level, real-time status of IdAM service for Help Desk. • Improved visibility for senior and executive management.
AS-02	**Operational Reporting** Operational Reporting capability for usage, capacity and quality management	• Inform identity lifecycle management to ensure timely change and removal of access. • Reporting on identity lifecycle and entitlements management to demonstrate who has access to what. • Enable implementation of a usage charge-back model. • Provide performance reporting to aid capacity planning. • Facilitate improved identity data quality.
AS-03	**SIEM** Security Incident and Event Management capability	• Provide continual, contextual, identity access information and monitoring. • Log, monitor, detect, alert and report IdAM security events. • Enable forensic data analysis to support investigations. • Facilitate proactive breach/threat detection through governance and analytics. • Improved reporting to support strategic security capability planning. • Reduce risk of compromise to workforce identity and department ICT systems and resources.
AS-04	**Forensics** Forensic Data Analysis capability	• Support identity breach and fraud investigations. • Discover and analyse patterns of inappropriate behaviour. • Reduce risk of compromise to workforce identity and department ICT systems and resources.

Reference	Direction	Purpose
AS-05	**Audit and Compliance Management** Audit and compliance management capability (tools)	• Efficient, consistent, easy-to-use, standardised, timely compliance reporting. • Demonstrate control over who has access to what. • Provide contextual, continuous user access reporting. • Provide detailed, real-time governance reports for auditors. • Enable risk and information security attestation. • Enable improved compliance against government regulation and industry standards. • Improved reporting for strategic IdAM capability and service planning.

Implementation

Planning will commence with the development of a Victorian Government Workforce IdAM strategy and implementation plan that will align with the *Victorian Government Information Technology Strategy 2016 to 2020* and the broad principles of governance and implementation set out in the *Business Support Services Strategic Review.*

To progress this, DPC will establish a working group of stakeholders to assist with the development of a business case for seed funding to perform a maturity assessment and develop the strategy and detailed implementation plan.

Approach

Reference	Direction	Purpose
AP-01	Roadmap of IdAM Capabilities	• Provide high level timeline for delivery of IdAM capabilities. • To follow completed IdAM Statement of Direction.
AP-02	Business case for procurement of services to develop the Workforce IdAM Strategy and Implementation Plan	• Request for seed funding. • Independent, expert guidance on identity and access management. • Provide the necessary resources to gather all departments and CenITex requirements. • Obtain the necessary skills and expertise to perform a maturity assessment across departments to determine elements for re-use.
AP-03	The Victorian Government will have a Workforce IdAM Strategy	• Defines the future state based on good practice and federal, state and industry standards. • Based on maturity assessment of current department and CenITex IdAM capability. • Is aligned with department and CenITex strategic IdAM directions. • Deliverables based on department priorities. • Designed to be usable by all in-scope departments.
AP-04	The Victorian Government will have a Workforce IdAM Implementation Plan	• 5 year implementation plan with detail of next 2 years and key priorities for subsequent years. • Based on department priorities. • Includes all in-scope departments. • Incorporates planned department and CenITex programs of work.

Document control

Approval

This document was approved by the Victorian Secretaries Board on 23 August 2017 and applies from the date of issue (see cover).

Version history

Version	Date	Comments
0.1	09/02/2017	Preliminary draft to CenITex and ESB stakeholders
0.2	01/03/2017	Second draft to IdAM Working Group (IdWG) – partial release
0.3	03/03/2017	Third draft to IdAM Working Group (IdWG) – full release
0.4	27/03/2017	Forth draft to IdAM Working Group (IdWG)
0.5	29/03/2017	Fifth draft to IdAM Working Group (IdWG)
0.6	31/03/2017	Sixth draft to IdAM Working Group (IdWG)
0.7	05/04/2017	FINAL draft for CIO LG – discussed at IdWG (5 April)
0.8	01/05/2017	Final version endorsed by CIO LG as recommended by IdWG
0.91	29/05/2017	Final version for endorsement by Deputy Secretaries' Integrity and Corporate Reform Subcommittee (ICRS)
0.92	23/06/2017	Resubmitted to Tony Bates (DPC Deputy Secretary) and ICRS (Deputy Secretaries) with broadening of scope to VPS.
0.93	02/08/2017	Final version for VSB approval with reference model correction noted by Department of Justice and Regulation.
1.0	23/08/2017	Approved by VSB

Glossary

Term	Definition
Business Partner	Entities that perform business on behalf of Departments e.g. Automotive dealers for VicRoads, DHHS Client Service Organisations such as Berry St.
Casual	A person hired to the Victorian Government on a casual basis in an ongoing capacity but without fixed hours that is likely to have restricted access requirements
Coarse-grained authorisation	Coarse-grained authorisation essentially focuses on controlling access in to the ICT system or resource based on role/groups.
Contractor	A person hired to the Victorian Government for a fixed period of time with minimum hours that is likely to have restricted access requirements.
Customer	Consumers of government services, citizens.

Digital Certificates	An electronic ‘passport’ that verifies a user sending a message is who he or she claims to be, and provides the receiver with the means to encode a reply.
Employee	A person hired on a full time or part time basis in an ongoing capacity with fixed hours and typically has minimum standard access requirements.
Federated Identity	Means of linking a person’s electronic identity and attributes that are stored across multiple distinct identity management systems to obtain access to ICT systems. Common purpose is to provide single sign-on experience for users across organisations.
Fine-grained authorisation	Fine-grained authorisation focuses on securing the ICT system or resource after access has been granted based on attributes of the user.
IdAM	Identity and Access Management.
Level of Assurance	A level of confidence in a claim, assertion, credential or service. The four levels of assurance typically recognised in Government policies are: Level 1 – No or little confidence Level 2 – Some confidence Level 3 – High confidence Level 4 – Very high confidence.
Multi-factor Secure Access	Method of access to ICT systems where a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know, e.g. password), possession (something they have, e.g. token or SMS to mobile), and inherence (something they are, e.g. biometrics).
Privileged Accounts	Accounts with ability to view, modify or delete sensitive information or manage ICT systems and resources, including but not limited to, system, network and database administrators, service (system-to-system), development, testing, training, application and WebAPI accounts. Can be staff, business partner or service provider users.
Role Based Access Control (RBAC)	A method of regulating access (e.g. view, create or modify) to ICT systems and resources based on the roles of individual users within an organisation.
Service Provider	Provider of services to Victorian Government including consultants e.g. Telstra network agent, HP data centre hosting operator, KPMG professional services consultant.
Single Sign On	Real-time authentication of a user to multiple applications using a single digital credential, typically their network logon, either without needing to present the digital credential again or representing the same digital credential.
Staff	A collective term referring to persons hired to the Victorian government as full time or part time employees, contractors, casuals or volunteers.
Trusted Identity Framework	Establishes the accreditation requirements, governance arrangements and interoperability standards that participants of a federated-style IdAM eco-system are required to comply with.
Workforce	Collective term for staff, business partner and service provider users of department ICT systems and resources.
Volunteer	A person performing tasks on behalf of the department on an ad hoc or seasonal basis and requires tightly controlled access.
VPDSS	The Victorian Protective Data Security Standards issued by the Commissioner for Privacy and Data Protection (CPDP).

Appendix A – IdAM environment scan

Consistent, efficient, and effective IdAM services are needed to deliver increased productivity for users with single sign-on and protection of our identities, credentials and information systems with authoritative and up-to-date user lifecycle management.

The Breach Level Index (BLI) report released for 2016 financial year states that 'hackers have continued to go after both low hanging fruit and unprotected sensitive personal data that can be used to steal identities'[5].

In article 'IAM Maturity Means Half the Breaches'[6], it states that Forrester Research conclude 83% of organisations do not have a mature approach to identity and access management resulting in two times more breaches and $5 million more in costs than those that do. Also that 80% of security breaches involve privileged credentials that typically belong to the IT professionals who administer the systems, databases and networks of an organization.'

The Queensland Crime and Corruption Commission further indicates unlawful access to government systems, including police databases, makes up 11.5 percent of all its complaints and is on the rise.

The continuing rapid migration of business applications to the cloud is also a consideration.

Forrester and Gartner advise that 'enterprise-wide adoption of SaaS is widespread and has reached a tipping point. 62% of enterprises have multiple SaaS apps today, and that number is growing quickly'.

Forrester reports that 91% of organizations with the most mature IdAM instances gravitate toward integrated IdAM platforms, rather than relying on multiple point solutions, and spend 40% less on technology. A more mature IdAM approach showed direct correlation to reduced security risk, improved productivity, increased privileged activity management and greatly reduced financial loss over their less mature counterparts.

In this environment, consistent, efficient, and effective IdAM services that deliver increased productivity for users with single sign-on and protection of our identities, credentials and information systems with authoritative and up-to-date user lifecycle management is required.

[5] The BLI is a global database produced by Gemalto, a recognised provider in digital security, that tracks data breaches and measures their severity based on multiple dimensions. Refer to …… *http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-first-half-2016-Breach-Level-Index.aspx*

[6] Refer to source *https://www.infosecurity-magazine.com/news/iam-maturity-means-half-the/*