



Report 12: 2023-24 | 28 March 2024

BETTER PRACTICE GUIDE

Digital Identity and Access Management



Office of the Auditor General for Western Australia

Audit team:

Aloha Morrissey
Kamran Aslam
Michael Chumak
Ben Goodwin
Paul Tilbrook

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

© 2024 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Digital Identity and Access Management

Report 12: 2023-24
28 March 2024

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

DIGITAL IDENTITY AND ACCESS MANAGEMENT

This report has been prepared for submission to Parliament under the provisions of sections 23 and 24 of the *Auditor General Act 2006*.

This better practice guide aims to help Western Australian (WA) public sector entities improve their digital identity and access management. The guide focuses on better practice principles to protect information assets from unauthorised access and has been informed by this Office's recent information systems audit findings and input from other WA government entities.

A handwritten signature in grey ink that reads "Sandra Labuschagne".

Sandra Labuschagne
Acting Auditor General
28 March 2024

Contents

- Auditor General’s overview..... 5
- Part 1: Introduction 6
 - 1.1 About this guide6
 - 1.2 Who should use this guide7
 - 1.3 Background7
- Part 2: Digital identity and access management..... 8
 - 2.1 Governance8
 - 2.2 Workforce management..... 10
 - 2.3 Identity and account management 11
 - 2.4 Standard access management 14
 - 2.5 Privileged access management 16
- Appendix 1: Digital identity and access management checklist..... 18

Auditor General's overview

The complexity and scale of IT environments and rapid expansion of technology poses many security challenges for Western Australian public sector entities. One such challenge regularly highlighted by our General Computer Controls audits, is the management of digital identities and their access to entities' information systems. Strong management is essential to protecting key systems and the information they hold from cyber threats and inappropriate access.



This guide aims to provide public sector entities with vendor-agnostic principles to implement and maintain strong digital identity and access management practices.

I acknowledge the work done in this area by the Australian Cyber Security Centre. I also thank the Department of the Premier and Cabinet's Office of Digital Government, the State Records Office, the Office of the Information Commissioner, the WA Local Government Association and the Department of Local Government, Sport and Cultural Industries for their submissions during the development of this guide.

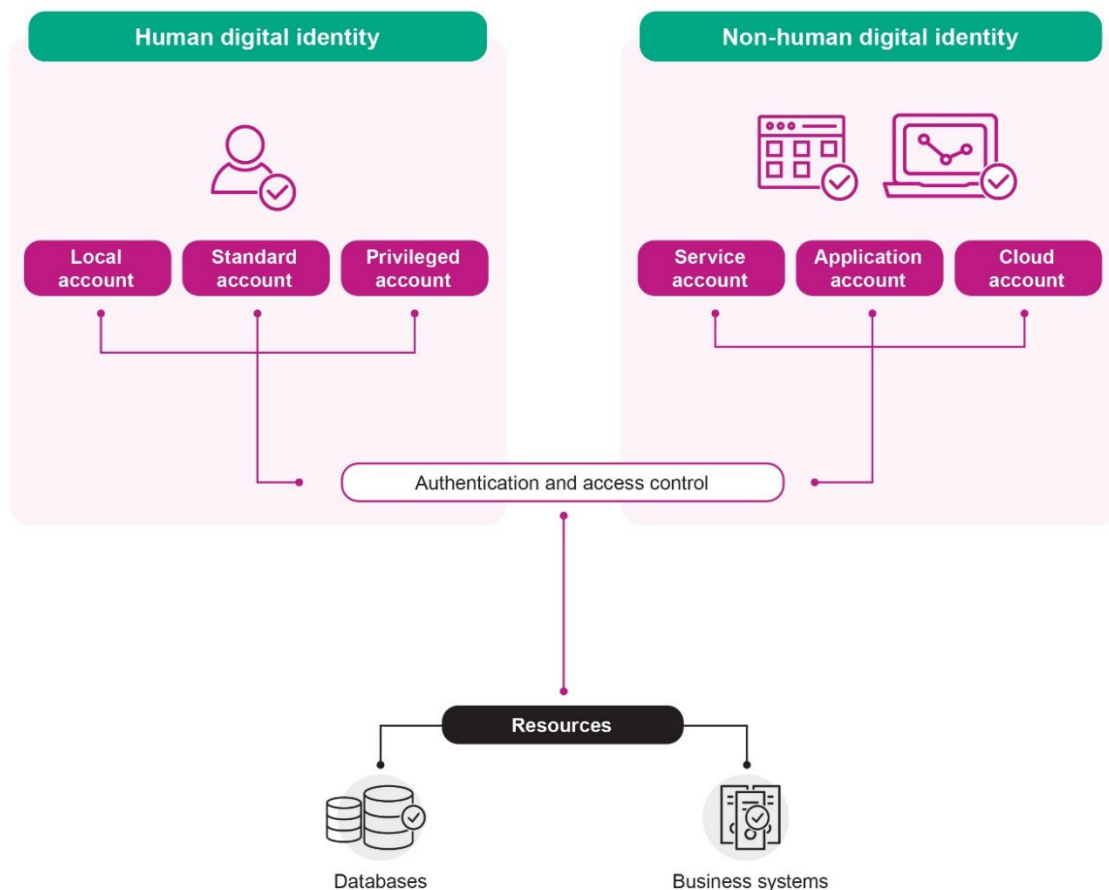
Part 1: Introduction

1.1 About this guide

This better practice guide aims to help Western Australian (WA) public sector entities improve their digital identity and access management (IAM). The guide focuses on better practice principles to protect information assets from unauthorised access and has been informed by this Office’s recent information systems audit findings and input from other WA government entities.

Digital identity and access management¹ consists of the technologies and business processes to help the right identities access the right assets at the right time for the right reasons, while keeping unauthorised access and fraud at bay.²

Identity management in this guide only covers the digital identity of an individual, software application or device, not the physical identity of humans³. Digital identity is represented by unique verified attributes and credentials such as a username, password or email address used to authenticate, define permissions, provide access and monitor activity (Figure 1).



Source: OAG

Figure 1: Simplified overview of identity, accounts and access

This is not intended to be an exhaustive document. Further guidance is available through sources including:

¹ 'Set of practices that enables only permitted individuals the ability to perform an action on a particular resource'. National Institute of Standards and Technology, [Access management – Glossary](#), NIST website, n.d., accessed 7 November 2023.

² Gartner, [Identity and Access Management \(IAM\)](#), Gartner website, n.d., accessed 7 November 2023.

³ This document does not cover protection of human identity information which has additional security and privacy considerations.

- Australian Cyber Security Centre⁴
- Identity Defined Security Alliance⁵
- Identity Management Institute⁶
- IDManagement.gov⁷.

1.2 Who should use this guide

We encourage all public sector entities to adopt the principles in this guide as required in order to better protect their information assets from unauthorised access. A checklist of the better practice principles is also provided at Appendix 1 to assist entities in implementing IAM.

1.3 Background

At the start of an individual's (entity staff and contractors) employment, a digital identity is created for them. This is then linked with accounts that provide access to business systems and information. Digital identities and accounts can also be created for devices and software applications. Over time accounts may accumulate unnecessary privileges. For example, when individuals permanently or temporarily change roles or when devices or software applications are replaced. Ongoing maintenance is required to ensure account privileges do not become excessive and are disabled when no longer required.

Protection of identities and access management is paramount as information systems drive decision-making and delivery of services to the public. Furthermore, the continued growth of remote and flexible work arrangements, underpinned by cloud technology, presents additional challenges for how entities manage digital identities and access. Identities and accounts present an attractive target for nation-state, organised crime, hacktivist and insider threat actors. The Office of the Australian Information Commissioner attributed the majority of notifiable data breaches in the first half of 2023 to compromised identity credentials⁸.

As part of our annual information systems audit program, we continue to find IAM weaknesses which could result in unauthorised access to sensitive information assets. In 2022-23, we found only 21% of State government entities and none of the local government entities audited met our access management benchmark.

The need to secure information assets and only allow authorised⁹ access or changes is also a requirement for State entities under the State Records Commission Standards and associated principles¹⁰. The Department of the Premier and Cabinet's Office of Digital Government has published information to support WA government cyber security activities¹¹ and circulated an authentication guide for WA government entities.

⁴ Australian Cyber Security Centre, [Resources for business and government](#), Cyber.gov.au website, n.d., accessed 25 January 2024.

⁵ Identity Defined Security Alliance, [Identity Defined Security Best Practices](#), Identity Defined Security Alliance website, n.d., accessed 25 January 2024.

⁶ Identity Management Institute, [Identity Management Institute website](#), n.d., accessed 25 January 2024.

⁷ U.S. General Services Administration, [Identity Lifecycle Management Playbook \(idmanagement.gov\)](#), idmanagement.gov website, n.d., accessed 25 January 2024.

⁸ Office of the Australian Information Commissioner, [Notifiable Data Breaches Report: January to June 2023](#), OAIC website, 5 September 2023.

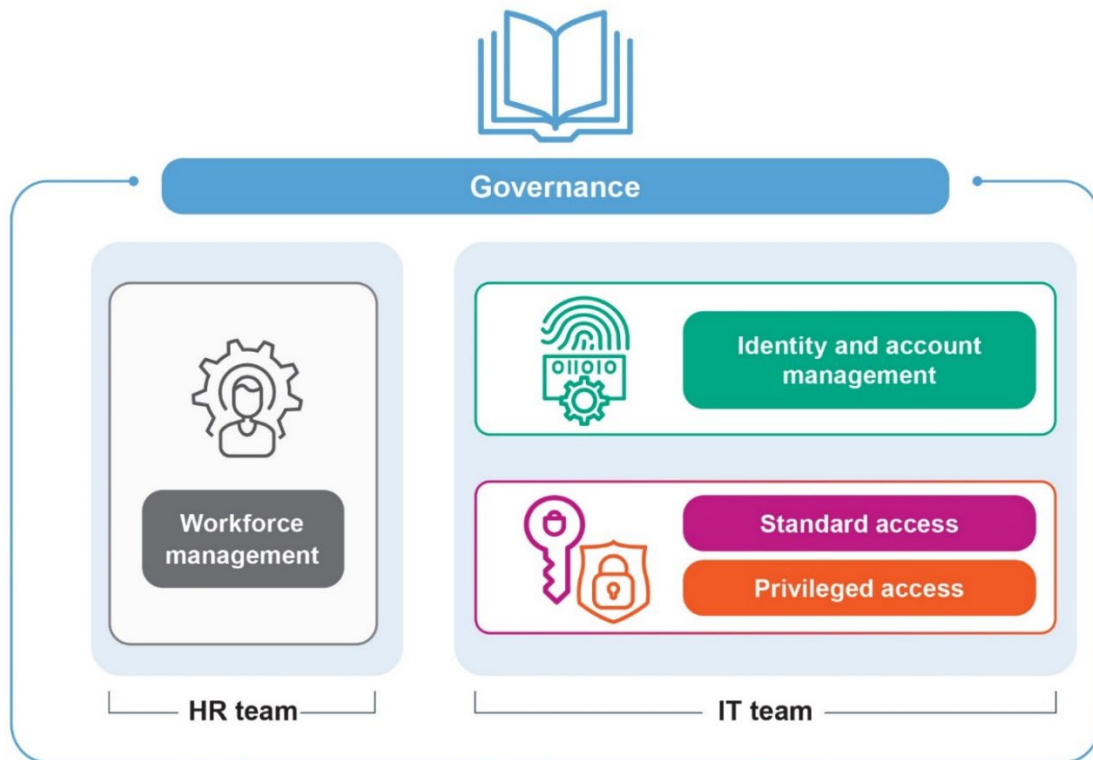
⁹ 'Ensuring that correctly authenticated users can access only those resources for which the asset owner has given them approval'. Gartner, [Authorization](#), Gartner website, n.d., accessed 7 November 2023.

¹⁰ State Records Commission, [State Records Commission Standard 8 – Managing Digital Information \(Principle 3 – Security of Digital Information\)](#), WA.gov.au website, 22 June 2016, accessed 22 November 2023.

¹¹ Office of Digital Government, [WA Cyber Security Unit](#), WA Cyber Security website, accessed 16 February 2024.

Part 2: Digital identity and access management


This guide focuses on the key principles outlined in Figure 2 to help improve the WA public sector's IAM capabilities. We have included case studies to emphasise the importance of principles in this guide. These case studies are based on our information systems audit findings and recommendations to rectify control weaknesses.



Source: OAG

Figure 2: Overview of IAM areas

2.1 Governance



Governance

Governance establishes accountability and responsibility for defining identity and access requirements.

It ensures the necessary visibility over access, privileges and authentication controls to identify deviations from policies, strengthen controls and respond to unauthorised actions.

2.1.1 Establish a framework

Define and document IAM objectives that align with the entity's values, regulatory requirements and risk appetite. Entities should:

- Develop formal policies and procedures covering access controls, authentication standards, account lifecycle, auditing and segregation of duties requirements.
- Identify system owners, who define system access levels and approve access to information systems and data. System owners enforce the principle of least privilege¹²,

¹² The principle that identities/accounts are granted the minimum system resources and authorisations needed to perform its function. National Institute of Standards and Technology, [least privilege – Glossary](#), NIST website, n.d., 7 November 2023.

manage changes and periodically review system access levels against regulatory, policy and role requirements.

- Manage risks associated with trusting third-party and legacy identity providers (e.g. domain trusts¹³).

2.1.2 Centralise IAM

Centralise authentication services with a key focus on critical systems, business applications, devices and supporting infrastructure.

Centralising IAM helps to efficiently grant, revoke, and monitor identities and access over multiple systems. Entities should weigh the benefits of centralisation to determine if it fits their needs. Entities should:

- Document all authentication services in use and include them in disaster recovery plans.
- Where possible, link access levels to pre-defined roles and automatically assign them through IAM software for key business applications and resources.

2.1.3 Log and monitor events

Logging and monitoring provide visibility over system use, data access patterns and indicators of compromise and help support forensic investigations. Entities should:

- configure key systems, applications and infrastructure to generate event logs
- identify key security and transactional events that require logging and monitoring. Logs should provide actionable information to detect attacks and ensure actions are unambiguously attributable to an identity
- monitor access to cloud resources to identify suspicious access
- keep and protect logs.

Automating log collation and monitoring through software tools such as Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) can provide real-time situational awareness and better assist with threat detection. Information and cyber security staff should be appropriately trained to use these tools.

For more details see the Australian Cyber Security Centre (ACSC) *Guidelines for System Monitoring*.¹⁴

2.1.4 Understand how accounts are used

Entities should gain visibility over all human and non-human identities to ensure their account use is well understood. Software tools can assist with the analysis of large numbers of accounts in complex environments. For example, they can be used to identify non-human or service accounts and their use.

2.1.5 Verify the effectiveness of controls

The effectiveness of IAM controls should be assessed to confirm they are implemented and operating effectively to achieve policy objectives. This program can be strengthened through internal and external audits.

¹³ A trust between two domains allows users and groups from one network to access resources in another network domain.

¹⁴ Australian Cyber Security Centre, [Guidelines for System Monitoring](#), ACSC website, 01 December 2023.

Case study 1: Data breach as a result of control weaknesses

An entity we audited recently suffered a data breach when an outdated authentication system that granted access to a key business application was attacked and compromised. The entity took six months to detect the attack and data breach. We had previously recommended the entity improve its logging and monitoring controls, but it was only after the data breach that the entity updated their security policies, defined roles and responsibilities, improved monitoring and hardened authentication mechanisms.

2.2 Workforce management

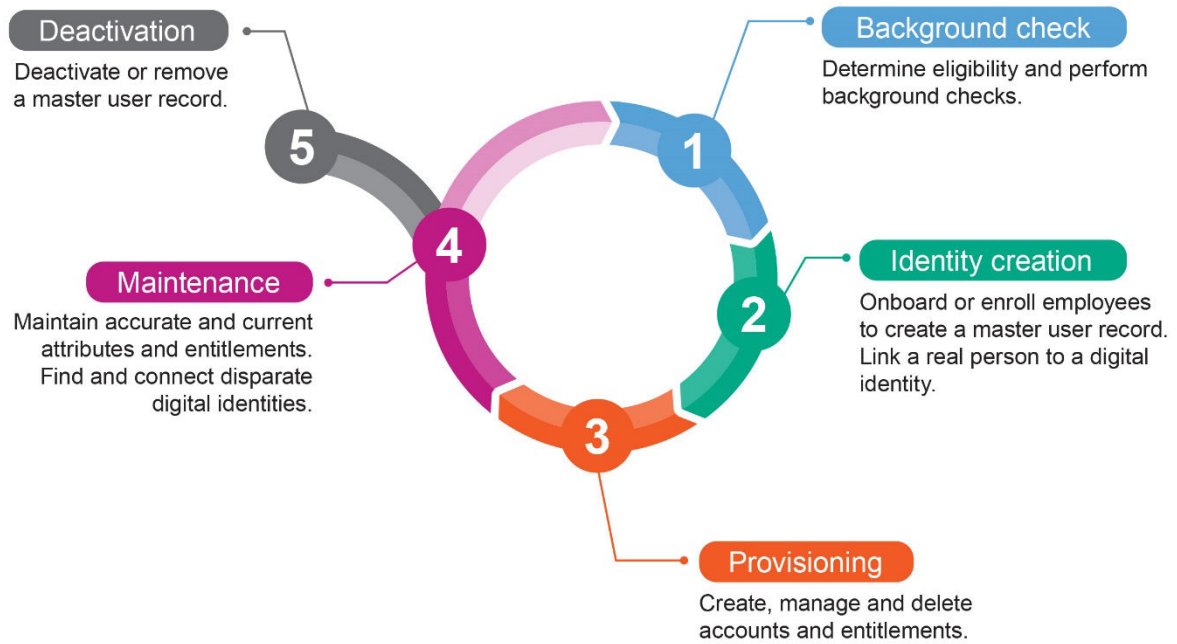
An entity's workforce management practices play an important role in securing human identities and accounts. This guide does not cover the full extent of workforce management but rather the key principles required to properly manage identity and access.

Workforce management systems should maintain appropriate workforce records including a master user record of all individuals employed or contracted.

The following aspects should be considered (Figure 3):

- Background checks – identities and accounts should only be created and access rights (entitlements) assigned after background checks have verified the individual's personal identity.
- Identity creation and provisioning – the creation of identities and accounts, and assignment of access rights can be performed manually or be automated¹⁵ through integration with IAM software.
- Maintenance – workforce records should be maintained and changes communicated to system owners so access rights can be updated. For example, when there are permanent or temporary changes in an individual's role. Individuals may have multiple digital identities due to multiple legacy systems; these should be linked or consolidated.
- Deactivation – an individual's identity and associated accounts should be disabled when they leave an organisation.


¹⁵ IAM software can assist with automating IAM processes.



Source: OAG based on IDManagement.gov

Figure 3: Workforce IAM lifecycle

2.3 Identity and account management



Identity and account management

Managing the digital representation of individuals, applications and devices, including all associated accounts.

Formal processes provide assurance that activity on networks and restricted systems can be reliably attributed to a known identity.

2.3.1 Create identities and accounts

Ensure all human (individuals) and non-human identities (applications, end-user devices, services) and accounts are provisioned through formal, documented and accountable processes. Without formal processes, accounts may be created without authorisation for fraudulent activity. Additionally, dormant accounts could be used by malicious actors. The following principles must be considered:

- For smaller entities, provisioning may be a manual process.
- For larger entities, better practice is to automate provisioning.
- Manual requests and approvals, and automation logs must be retained. These should be periodically reviewed to verify the effectiveness of the process.
- Place a time limit on identities/accounts created for a fixed period. For example, a contractor's identity/account should automatically expire on their last day.
- Create dedicated accounts and do not share accounts between staff, infrastructure, systems and applications.
- Some identities may require more than one account such as for privileged access or access to legacy systems that do not support central authentication. These accounts should be linked so they are all disabled when no longer required.

Case study 2: Request and approve accounts

Our audits in 2022-23 found entities failed to appropriately request and approve accounts for individuals (35%) and services (24%). Examples included:

- At one entity, a data custodian requested and self-approved access to the finance application.
- At another entity, 37% of privileged accounts provided to consultants working on a key business application were not appropriately approved.
- At a third entity, 80% of non-standard accounts, including highly privileged service and administrator accounts, were not appropriately requested and approved.

2.3.2 Manage non-human identities and accounts

Applications and devices need access accounts to operate. These accounts require additional considerations as they support system operations in the background, are less visible and often have higher privileges. Compromise or misuse of these accounts can significantly impact service delivery.

Entities should:

- establish processes to create, maintain and remove non-human identities and accounts
- ensure service and generic accounts for on-premise and cloud-based systems have assigned owners, are clearly labelled and only used for a dedicated purpose
- grant the required rights using a least privilege approach and maintain visibility over non-human accounts with privileged access
- minimise the use of built-in roles and security groups for non-human accounts
- ensure generic and built-in administrator accounts are only used when access to dedicated accounts is not possible
- ensure rights assigned to application identities, services and generic accounts are periodically reviewed by designated system owners to make certain they are still required. Changes should be made using a change control process
- disable and remove non-human identities and accounts when assets are disposed of or applications are no longer required
- protect the application programming interface (API) with strong authentication. Where possible use tokens over API keys
- monitor the activity of non-human identities and accounts.

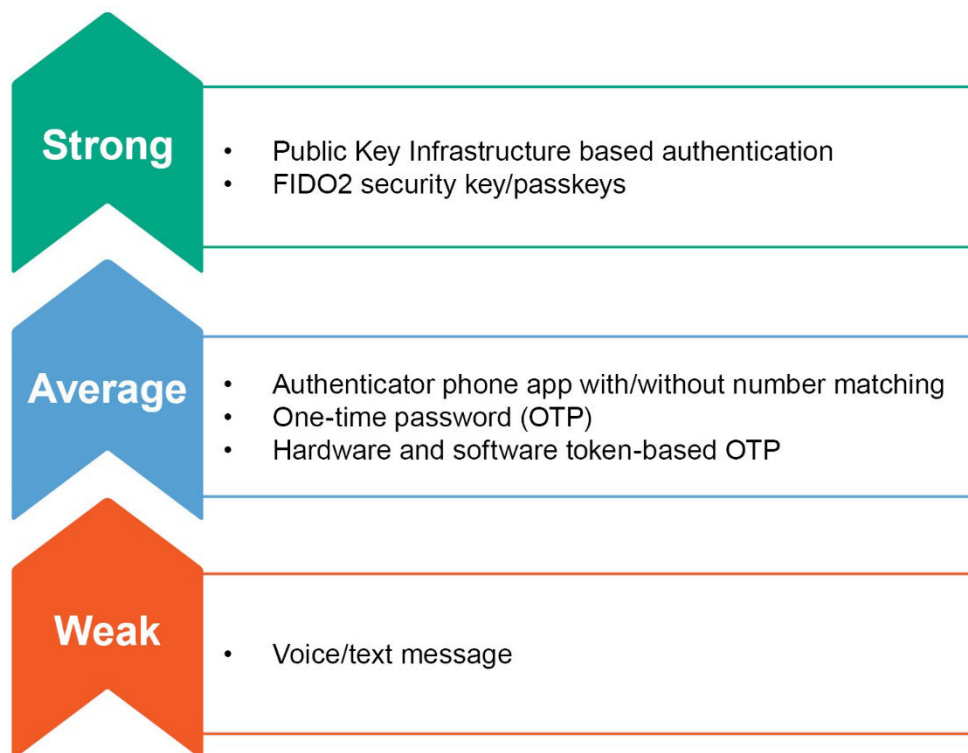
2.3.3 Implement strong authentication controls

Authentication verifies the identity of a person, device or application requesting access. For example, individuals accessing a banking application may need to verify their identity through a username and password or biometrics (face ID, fingerprints). Entities need to select an appropriate authentication method considering factors such as the importance of a system and the information it holds, who uses the system, the location of individuals and devices (office, remote or overseas) and the type of device used (personal or entity-provided).

Entities should:

- strive for password-less authentication. If this is not possible, prevent the use of simple, weak, default and commonly used passwords

- set up long, unique and complex passwords for application identities, service, generic and break glass¹⁶ accounts. Passwords should be changed when someone with access to these identities or accounts leaves the entity or changes roles
- verify individual and device identity whenever risks or context changes (such as location, device type, device health and system use patterns).¹⁷ For example, additional authentication may be required to verify the identity of an individual if they login from an untrusted device or unusual location to access sensitive information
- prioritise multi-factor authentication (MFA) and implement phishing resistant MFA (Figure 4)
- implement entity-wide single sign-on (SSO) to access systems and information.



Source: OAG based on Microsoft¹⁸ and Cybersecurity & Infrastructure Security Agency information¹⁹

Figure 4: MFA methods and strength

2.3.4 Protect credentials

Policies and supporting processes should enforce the secure storage and handling of credentials (username/password) and encryption keys. For example:

- Credentials should be stored in a centrally managed password manager. Individuals should have their own account to access the password manager and this activity should be monitored.
- Actively identify and secure passwords stored in plain-text on shared drives, documents and internet/intranet pages.

¹⁶ A highly privileged account to gain authorised access in an emergency situation.

¹⁷ Identity Management Institute, [Zero Trust Cybersecurity Model](#), IMI website, n.d, accessed 22 November 2023.

¹⁸ Microsoft, [Conditional Access authentication strength](#), Microsoft website, 25 March 2024.

¹⁹ Cybersecurity & Infrastructure Security Agency, [CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication](#), Cybersecurity & Infrastructure Security Agency website, 31 October 2022.

- Perform third-party risk assessments, undertake audits and review assurance reports where cloud services are used for managing credentials or encryption keys.
- Encryption keys for cloud services containing sensitive and mission critical systems should be self-managed instead of being managed by the service providers.

Case study 3: Manage sign-in risks

At an entity we audit, overseas attackers used phishing techniques in 2022-23 to bypass MFA controls designed to protect remote access. The entity had not implemented location-based access restrictions to limit access to staff in WA, had inadequate event logging and did not have a cyber security incident response plan.

Another entity recently experienced a high volume of brute force login attacks against a remote access system. The entity did not monitor its event logs and only became aware of the attacks when our audit identified them. We found:

- A rule implemented within the main firewall for testing purposes had rendered controls intended to limit overseas access ineffective.
- Poor change management and a lack of firewall rule reviews contributed to the issue.

Entity staff observed an improvement in system performance once the firewall rules were updated.

2.4 Standard access management



Standard access

This type of access cannot be used to perform privileged actions such as modification of system configurations.

2.4.1 Grant minimum access

Access should be granted using the principle of least privilege. This means access should only be given to those systems and resources required by the individual, application, device or service accounts. Access may be further restricted based on the context of the access request such as location, device, time of day. Entities should:

- use pre-defined roles and associated privileges instead of copying access from one identity to another
- ensure segregation of duties requirements are maintained
- ensure only standard access accounts are granted remote access and that all remote access requires strong authentication and phishing resistant MFA.

Case study 4: Restrict remote access

Recently at one entity we identified over 30 highly privileged administrator accounts and 150 service accounts with remote access rights.

Entities should follow ACSC recommendations²⁰:

- only grant standard accounts remote access
- administrators should use their standard account for remote access and then use their privileged account to perform administrator tasks.

2.4.2 Verify access rights

Implement processes to regularly verify that identities and accounts belong to individuals currently engaged by the entity and their access is still required and appropriate to their role. This should also occur when an individual's role changes. In addition, entities should regularly review access levels assigned to predefined roles.

Similarly, non-human (e.g. application device and system) accounts should also be reviewed. Where automation is used to assign rights, logs should be monitored and the access rights of active accounts regularly reviewed to verify the effectiveness of automated processes.

Case study 5: Automation failures

Recently at one entity we found automated processes failed to disable more than 65 network and 80 application accounts of individuals that had left the entity.

A misconfigured automated workflow at another entity granted access to its data centre to over 100 unauthorised individuals. The entity's internal reviews had failed to identify this inappropriate access.

2.4.3 Promptly disable access

It is important to revoke access when individuals no longer require it and to keep suitable records of access removal. For example, when individuals (e.g. contract, casual, temporary and permanent staff) take long periods of leave, retire, resign, are terminated or are at the end of an employment contract. A central identity management system can be used to automatically disable access. If access is not revoked promptly, it could be used to access systems and information without authorisation.

Case study 6: Former staff had access to multiple systems

Our audits in 2022-23 found 61% of entities had not disabled access accounts belonging to terminated staff and unknown individuals. We found:

- At one entity, an automation error resulted in 12 staff still having network access for up to six months after they ceased employment. Three of these accounts had privileged access, including access to a firewall, and two other accounts were used after the staff ceased employment.
- At another entity, 17 enabled network accounts belonged to former employees of which six were used after staff ceased employment. Seven of the 17 had remote access still enabled. Another 44 accounts could not be attributed to current staff or contractors. Eleven of these had remote access.

²⁰ Australian Cyber Security Centre, [Secure Administration](#), ACSC website, 6 October 2021, accessed 16 December 2023.

- At another entity, 241 individuals retained building access after they ceased employment. The current employment status of many more could not be confirmed.

2.5 Privileged access management



Privileged access

Process to define and secure accounts with higher access or capabilities beyond standard access.²¹

Privileged individuals, applications, and service and generic accounts require additional controls to reduce the risk of being compromised.²² Effective privileged access management provides an added barrier against attackers.

2.5.1 Elevate rights based on need

Privileged access should be requested based on need and granted only for a short period of time. Approval of this access can be through a delegated officer or automated based on rules. Auditable records of access elevations should be kept.

System administrator accounts usually have a very high level of access. Whilst this provides flexibility, this type of access is only needed for certain tasks every now and then.

Case study 7: Dedicated privileged access accounts

Our audits in 2022-23 found 24% of entities had wrongly granted privileged access to standard accounts. At several entities these privileges allowed individuals to access internal and internet facing servers, cloud configurations and data within key business applications. Attackers can take advantage of privileges granted to normal accounts as these accounts are exposed through activities such as web browsing or the use of email.²³

The ACSC recommends the use of separate accounts for privileged access. Removing privileged access from standard day-to-day accounts helps to prevent threat actors from escalating their attack when an account is compromised.

2.5.2 Use privileged access workstations

Only allow approved/trusted devices (privileged access workstations) administrative access to cloud and on-premise infrastructure and systems. These workstations should not be used for non-privileged tasks.

2.5.3 Secure privileged accounts

Privileged accounts should have the highest level of security as entities can experience significant impacts when these accounts are compromised. The following principles should be considered:

- Highly privileged identities should not be shared between on-premise and cloud environments.

²¹ Yubico, [What is Privileged Access Management](#), Yubico website, n.d., accessed 12 February 2023

²² Identity Management Institute, [Privileged Account Management Best Practices](#), IMI website, n.d., accessed 10 January 2023.

²³ Australian Cyber Security Centre, [Secure Administration](#), Australian Cyber Security Centre website, 6 October 2021, accessed 16 December 2023.

- Always require stronger authentication and phishing resistant MFA for privileged access to cloud services and on-premise infrastructure and systems.
- To reduce the risk of compromise, privileged accounts should not have internet, email or remote access. Where privileged accounts require administrative access to cloud services, this should be restricted through jump hosts²⁴ or privileged access workstations.
- Do not create unnecessary privileged accounts, instead use the principle of least privilege to grant specific privileges needed by the role.

Case study 8: Exposing privileged credentials

Our audits in 2022-23 found 27% of entities were sharing privileged access credentials instead of creating dedicated accounts for each privileged user.

We identified one entity where highly privileged generic accounts were shared amongst various teams. Credentials were shared through a variety of methods including email, end-user documentation and password managers using a single shared password.

At another entity a shared account was used to administer firewalls.

In addition to leaving privileged account credentials vulnerable, if a shared account is used for malicious purposes, it may not be possible to identify the individual responsible and hold them accountable.

2.5.4 Review privileges

Privileged access requires regular revalidation and monitoring to minimise insider threats. Entities should ensure:

- Access rights assigned to privileged staff and contractors are reviewed regularly and monitored. If their duties change, access should be adjusted.
- Reviews are documented and auditable records are maintained.
- Privileged rights expire after 12 months unless revalidated.

Case study 9: Compromised service accounts

In 2022-23 at one entity, we identified multiple service accounts with unrestricted delegation rights²⁵. If an attacker compromised one of these accounts, they would be able to impersonate any individual to access systems on the network.

At another entity, an attack compromised a service account by guessing the password using a dictionary of common passwords. The attacker gained access to a remote desktop service and then compromised servers responsible for authentication and communication. During the attack, logs and backups were deleted and a ransomware attack was performed.

²⁴ A jump host is an intermediary computer used for access between two network zones.

²⁵ Delegations enable a user or device to impersonate another account or service. This can be exploited to gain unauthorised access.

Appendix 1: Digital identity and access management checklist

Digital identity and access management better practice principles		Checked
Governance		
1	Ensure IAM objectives are defined.	
2	Develop and implement formal policies covering access, authentication, account lifecycle and monitoring requirements.	
3	Allocate system owners who will enforce policies.	
4	Understand and mitigate risks associated with third-party and legacy identity providers.	
5	Document all authentication services in use.	
6	Where possible centralise identity management and authentication.	
7	Configure all systems to generate important event logs which can be used to detect suspicious activity.	
8	Monitor event logs for suspicious activity. Retain event logs and protect them from unauthorised access.	
9	Understand the use of all identities and accounts.	
10	Periodically assess controls to ensure they are operating as intended.	
Identity and account management		
11	Ensure all identities and accounts are provisioned through formal processes.	
12	Where possible, automate provisioning processes through IAM software.	
13	Enforce expiry dates on temporary accounts and identities.	
14	Do not share accounts. Create dedicated accounts for individuals and purpose-specific accounts for applications and services.	
15	Where central authentication is not possible, link accounts with access to multiple systems so they can all be disabled when no longer needed.	
16	Where possible, implement password-less authentication. Restrict the use of weak, default or commonly used passwords.	
17	Identify existing weak passwords and change them.	
18	Prioritise phishing resistant multi-factor authentication (MFA).	
19	Re-verify the identity of individuals and devices when context changes. For example, individual or device location, device health and usage patterns.	
20	Implement single sign-on for all entity systems.	
21	Use a centralised password manager to store passwords, codes and encryption keys. Do not store passwords in plain-text.	
22	Self-manage encryption keys for sensitive and mission critical systems.	
23	Where possible use tokens to protect application programming interfaces (APIs) over keys.	

Digital identity and access management better practice principles		Checked
Standard access management		
24	Use pre-defined roles and associated privileges. Do not copy access from one identity to another.	
25	Enforce segregation of duties when granting access.	
26	Ensure only standard user accounts have remote access and require strong authentication and phishing resistant MFA.	
27	Regularly verify and review the appropriateness of access levels and pre-defined roles. Periodically review the effectiveness of automated processes where they are used to grant access.	
28	Disable access promptly when individuals leave.	
Privileged access management		
29	Grant rights using the principle of least privilege.	
30	Elevate access based on need and with appropriate approval. Use privileged access only for those tasks that specifically require elevated access.	
31	Ensure administrative access is only performed through privileged access workstations. Standard accounts should not be allowed to use these workstations.	
32	Do not share accounts between on-premise and cloud environments.	
33	Use stronger authentication and phishing resistant MFA for privileged access.	
34	Ensure privileged accounts do not have internet, email or remote access.	
35	Avoid creating unnecessary privileged accounts.	
36	Do not grant rights to non-human (devices, applications, services) accounts using built-in roles and groups.	
37	Non-human accounts should have assigned owners and their use documented.	
38	Monitor all, especially privileged, non-human accounts.	
39	Generic and built-in administrator accounts should only be used to restore access to dedicated accounts.	
40	Review privileged access regularly.	
41	Privileged rights should expire after 12 months unless revalidated.	
42	Disable privileged accounts when no longer required.	

Source: OAG

This page is intentionally left blank

Auditor General's 2023-24 reports

Number	Title	Date tabled
12	Digital Identity and Access Management – Better Practice Guide	28 March 2024
11	Funding for Community Sport and Recreation	21 March 2024
10	State Government 2022-23 – Financial Audit Results	20 December 2023
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Financial Audit Results – Local Government 2021-22	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

**Office of the Auditor General
for Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500

E: info@audit.wa.gov.au

www.audit.wa.gov.au



@OAG_WA



Office of the Auditor General
for Western Australia