­

**Azure Access Models Whitepaper**

**Version 0.2, 2023-11**

**Instructions:**

1. **Arial 11 single space is the standard format**
2. **Delete these instructions**

Contents

[1 Introduction 3](#_Toc151989735)

[1.2 Why use – Access Models 3](#_Toc151989736)

[1.3 What is - Azure Active Directory 3](#_Toc151989737)

[2 Access Models 4](#_Toc151989738)

[2.2 Current state 4](#_Toc151989739)

[2.2.1 New groups are established which overlap existing groups. 4](#_Toc151989740)

[2.2.2 Staff movements 4](#_Toc151989741)

[2.3 Cascading Access 5](#_Toc151989742)

[2.3.1 Downward Cascades 5](#_Toc151989743)

[2.3.2 Upward Cascades 5](#_Toc151989744)

[2.3.3 Requirements 5](#_Toc151989745)

[2.4 Dynamic Access 6](#_Toc151989746)

[2.4.1 Examples of Dynamic groups include: 6](#_Toc151989747)

[2.4.2 Dynamic Access group governance 7](#_Toc151989748)

[3 Challenges 8](#_Toc151989749)

[3.2 Azure Active Directory & Staff movements 8](#_Toc151989750)

[3.2.1 Current State 8](#_Toc151989751)

[3.2.2 Potential state 8](#_Toc151989752)

[4 Supporting materials 10](#_Toc151989753)

[4.2 Acronyms 10](#_Toc151989754)

[4.3 Terms 10](#_Toc151989755)

[5 Document Management 11](#_Toc151989756)

[5.2 Document Currency 11](#_Toc151989757)

[5.3 Document Owner 11](#_Toc151989758)

[5.4 Version Control 11](#_Toc151989759)

[5.5 Document Distribution 11](#_Toc151989760)

# Introduction

Access to Microsoft products can be governed by Microsoft’s integrated Azure Active Directory (*Azure AD / AAD*), which provides a centrally managed system for controlling access and privileges within the Microsoft suite. [Microsoft documentation - Azure RBAC](https://learn.microsoft.com/en-us/azure/role-based-access-control/overview)

While <Your Org> has an ‘Information Access and Control Policy’ (*IACP*), it does not currently have an Access Model providing a framework for how “*all access … based on the requirements of a role or function*” should be provisioned (*IACP 5.1*)

Depending on the use case, there are different approaches to provisioning access. Multiple of these “Access Models” can be utilised within a single organisation concurrently.

## Why use – Access Models

Access Models provide a framework to define employees’ access to files within the organisation, setting out how resources can & cannot be accessed, according to the principle of least privilege (POLP).

The access model sets out the “Why & Why not”, and informs the “How”

From an Access Model, Access Control can be configured to ensure employees (*only*) have access to information and resources related to their roles in the organisation. Having both the Access Control & Access Model enables the organisation to audit employee’s access against the desired state, as set out in the Access Model(s).

## What is - Azure Active Directory

Azure AD can be used for creation of Microsoft Teams channels, provisioning access to restricted folders, provisioning access to reports in PowerBI, and more.

Azure AD is the chosen security management system utilised by <Your Org>

# Access Models

## Current state

<Your Org> does not currently have a formalised access model approach, and provisions access on an ad hoc basic, adding the necessary members to new Azure AD group as requirements emerge. There is no governing procedure for creating, modifying, maintaining or deleting these groups, nor are they widely known resulting in access often provisioned on a per-user basis. As such, groups are created once, and not reviewed, and access is complex to audit, provide and remove.

[Microsoft documentation - Azure RBAC best practices](https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices#assign-roles-to-groups-not-users)

Azure AD groups as implemented have thus far are a combination of Cascading access & Dynamic access, without the governance of either.

### New groups are established which overlap existing groups.

Given Azure AD permissions are additive, the overlapping group memberships make it difficult to audit where certain permissions come from, and who has (what level of) access to what.

|  |  |
| --- | --- |
| •chael  -PBl-MH4L-GovemanceCommittee  d Johnson  dle  -PBl-MH4L-ProgramLeaders  ra  anda McNaught  -PBl-MH4L-ManagementCommittee  s  lee  rin  Rajan | Weatherston  •chele Romeo  Fic  em  - BI-MH4  Raja n  rin Eisele  entCommittee  -PBl-MH4L-P  mLeade  ß"ddle  'k Fokas  a da cNaug  -PBl-MH4L-SeniorLeadership  thy Leftwich  e Hawes |

Figure : Examples of <A Program> access groups

### Staff movements

Where staff movements are not communicated to IT, or IT are unaware staff have held group membership, access remains long after it should have been removed.

1. For internal movements, this can mean staff have access to records, documents and reports they should no longer have access to.
2. For external movements, this means their accounts retain access after staff have left.

## Cascading Access

Cascading access models mirror an organisation’s structure and are used to provide persistent access to assets, such as Teams channels, SharePoint files and reports, based on anticipated use cases. *i.e., Finance teams & the Finance managers should have access to the finance reports.*

There are two sub-types of cascading access, downward cascades and upward cascades, each with different use cases:

### Downward Cascades

Downward cascades are useful if you want to do something related to everyone in a group of connected (*sub*)divisions with one action, but you don’t want to affect people above a node in the chain, or those in other divisions.

|  |  |
| --- | --- |
| Use case: Mailing list Sending the Media group Christmas party invite to all media staff at a company "Autocar"  This will go to all staff in Media, but not to the group executive or to other divisions, such as Sales or Engineering. | Figure : Example - Downward Cascade |

### Upward Cascades

Upward cascades are useful if you want everyone in a team & their management chain to see something, but not other people in adjacent (*sub*)divisions.

|  |  |
| --- | --- |
| Use case: Access permissions Reports on Facebook ad engagement are available for all members of the Facebook media team at Autocar, and their managers.  These reports are not available to the Internal Comms team within Media, or to other Divisions like Sales or Engineering. | Figure : Example - Upward Cascade |

The advantage of an upward cascade model is the access flows upwards through worker-manager pairs to provide all staff in the value chain access to selected material. These people don’t have to be added individually, nor is material exposed to whole management teams where only one member is responsible.

### Requirements

As cascading access models are built to replicate organisational structures it requires accurate and persistent data to support it.

This is discussed more in [Challenges](#_Challenges)

## Dynamic Access

Recognising not all business functions are delivered by groups within the same team, there is need to provide groups which have members from across the organisation and which do not consist of whole teams or cascades, rather they’re composed of members from multiple workgroups who share common responsibilities.

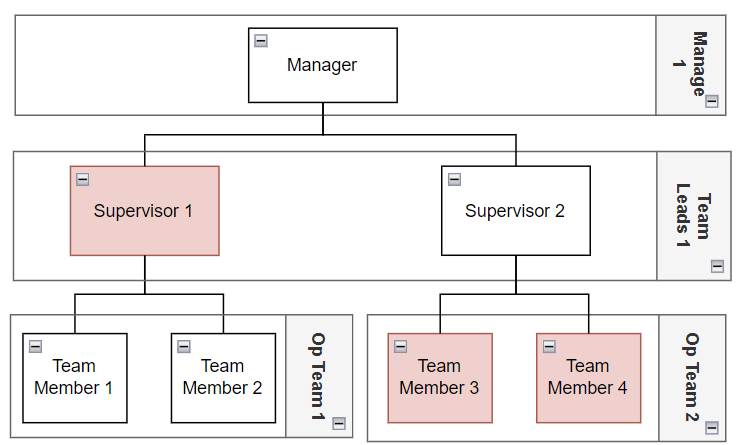


Figure : Dynamic Access - example

A Dynamic Access model approach allows the organisation to remain agile, standing-up temporary teams to meet functional needs as required, without restructuring the organisation. These groups should have a fix short-medium lifecycle, and access should be removed (*archived*) or renewed once this lifecycle is complete.

Using dynamic groups to provide persistent access over long time periods produces a messy difficult to audit and maintain environment that is equivalent to our current state. As such, the majority of content should be shared via (*Upward*) Hierarchical groups, keeping core functions centrally governed, and keeping the use of Dynamic Access models to a required minimum. Dynamic groups should be provided on an as needed-based basis, and according to pre-set guidelines.

Being an all of Microsoft product, Azure AD groups can be used to provision access to Teams Channels, SharePoint directories, as well as access to reporting. Utilising these for projects is a key tool behind agile and scalable workflows.

### Examples of Dynamic groups include:

* Working Groups
* IT project groups
* Governance Committees

### Dynamic Access group governance

Creation of dynamic groups should be challenged by default, such that creation of a dynamic access group requires approval by IT. This is to prevent an overwhelming number of dynamic groups where not required.

#### The creation of a dynamic group should include a record of the following parameters:

|  |  |
| --- | --- |
| **Requirement** | **Reason** |
| Group name | What the group is - identifier |
| Group members |  |
| *Group Owner* | Person accountable for adding / removing members, extending / archiving the group |
| *Group Members* | Contributors & consumers of group resources / outcomes |
| Group purpose | Purpose statement  Why can't this group be serviced by standard Azure access groups *(top down or bottom up)*  *i.e., it requires people from different work units* |
| Group duration | Expiration date  *Defines the retention policy for the group – when it’ll be automatically archived if not renewed / extended* |
| Microsoft services to be utilised | Which applications / tools this group is intended to underpin   * *MS Teams* * *PowerBI* * *HaloITSM* * *Other* |
|  |  |

# Challenges

## Azure Active Directory & Staff movements

When applied at scale, the Azure Active Directory system requires information about organisational structures to ensure privileges are correctly allocated. This information needs to be maintained as organisations grow and change, presenting a challenge for technical administrators: IT administrators have to maintain a parallel Organisational structure model inside AAD.

### Current State

Currently in <Your Org>, Azure AD isn’t synced against external systems. As such, there is additional workload to maintain synchronisation, changes take time to flow through as changes have to be manually applied, human error becomes a factor, accounts get forgotten, and access is left open where it should have lapsed...

Replicating existing structural information creates two sources of truth, introduces possibility of human error, creates desynchronisation and duplicates data. Additionally, there is now a requirement to update records across two systems whenever staff movements occur;

1. HR needs to update their system(*s*)
2. IT needs to update theirs

Microsoft Azure 
Hame > Diabetes Australia I Users > Users > Jack MacCormick > 
Jack MacCormick 
P Search resources. servi 
Properties 
CD Refresh 
Identity 
Got feedback? 
Job Information 
Contact Information 
Parental controls 
Settings 
On-premise± 
This view only contains properties that can be updated. Learn mare CZ 
P Search "Job Information" 
Showing g results under "Jab Information" 
Job title 
Company name 
Department 
Employee ID 
Employee type 
Employee hire date 
Office location 
Manager 
Sponsors (preview) 
Data Analyst 
Operations QLD 
Nik Fakas Edit 
+ Add sponsors 

Figure : Desynchronised Org structure w/in MS Azure

### Potential state

Ideally, adding / removing members from access groups is not done by IT, rather the AAD system in-loads the organisational structure from HR applications / data.

This would allow user profiles and Azure AD groups to be automatically created / deleted / updated, in line with changes to the organisational structure

An integration between HR systems and IT’s Azure AD removes human error, ensures synchronisation of records, and reduces the number of systems that need to be updates to one. Changes made inside the HR system are read by the automated processes, and carried across into IT’s user profiles.

#### Downward cascades

The group creation rules are straightforward; the members are all staff under a manager of a specified node when [member – manager] chains are expanded recursively [Use case: Mailing list](#_Use_case:_Mailing).

*Find staff belonging to X.*

#### Upward cascades

The group creation occurs at each node in the organisational chart, and includes all members of that node, plus a recursively expanded [member – manager] chain [Use case: Access permissions](#_Use_case:_Access)

*Find managers of X*

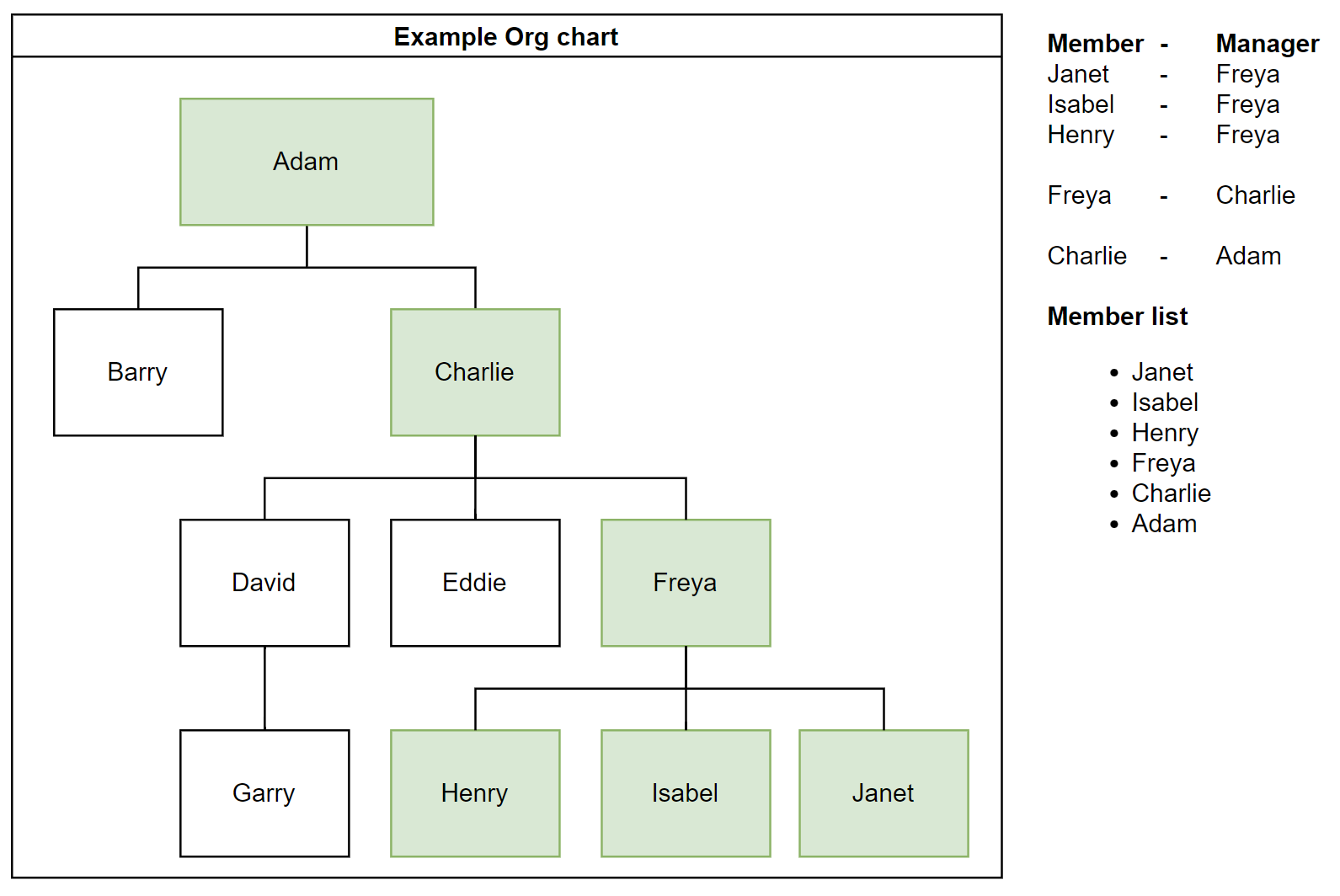


Figure : Example - Upward Cascade members

# Supporting materials

## Acronyms

|  |  |  |
| --- | --- | --- |
| **Term** | **Acronym** | **Context / Use** |
| <Your Org> | XX |  |
| Human Resources | HR |  |
| Information technology | IT | Primarily used to refer to the IT service team within XX |
| Microsoft | MS |  |
| Active Directory | AD |  |
| Azure Active Directory | AAD / Azure AD |  |
| (Microsoft) PowerBI | PBI |  |
| Information Access and Control Policy | IACP |  |
| <A Program> | <A PROGRAM ACRONYM> | An initiative delivered by ‘The Healthier Queensland Alliance’, led by <Your Org> |
|  |  |  |

## Terms

|  |  |
| --- | --- |
| **Term** | **Context / Use** |
| Group | A “group” as created in Azure Active Directory |
| Team | A collection of staff all reporting into the same manager,  *i.e., the media & marketing “team”* |
| (Sub) division / Department | A collection of multiple teams, all working to deliver the same function.  *i.e., the IT Division / Department is made up of multiple “teams”* |
| Cascade | A set of linked entities, with a defined sequence.  *i.e., multiple teams within a single reporting line* |
| Access Model | A framework / guiding principle for how access to resources should be provided. |
| Dynamic / Agile | A business methodology focused on the ability to scale, refocus and respond within short timeframes, typically involving multiple skillsets and parallel bodies of work, enabled by technology. |
|  |  |

# Document Management

## Document Currency

| Document CURRENT as of: | Document due for REVIEW on: | Review Owner |
| --- | --- | --- |
|  |  |  |

## Document Owner

| Name | Position | Email |
| --- | --- | --- |
| Jack MacCormick | Data Analyst | My email |

## Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Position | Description |
| 2023-11-27 | 0.2 | Data Analyst | Refined draft |
|  |  |  |  |

## Document Distribution

| Date | Version | Agency/Stakeholder organisation and members |
| --- | --- | --- |
|  |  |  |
|  |  |  |