Kickstart your Identity Governance practice in 45 minutes!

Where to start?

V-Platin Sponsor

nwc services
one step ahead

RECAST SOFTWARE

Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja gab

Lenovo

Microsoft

V-Gold Sponsor

scopewyse
we are what's next

sepago®

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors

SD:>_
SwissDev Jobs

About “Pim Jacobs”

Focus

Azure Active Directory

Microsoft Endpoint Manager

From

The Netherlands

My Blog

https://identity-man.eu

Certifications

Microsoft MVP

Hobbies

Blogging, Watching Soccer, (trying) to play soccer myself & spending time with my family.

Contact

https://www.linkedin.com/in/pimjacobs89/

https://twitter.com/pimjacobs89

About “Ronny de Jong”

Focus

Microsoft Endpoint Manager

Azure Active Directory

From

Netherlands

My Blog

https://ronnydejong.com

Certifications

Microsoft MVP

Hobbies

Relaxing, Fishing, BBQ, CrossFit

Contact

https://www.linkedin.com/in/ronnydejong/
https://twitter.com/ronnydejong

Agenda

Introduction of Identity Governance

Key features and importance

Account Lifecycle Management

For regular & guest accounts with demo

Access Lifecycle Management

Access packages & reviews with demo

How & where to start tomorrow?

Simple tips & tricks for quick wins

Q & A

Let us know if you have any questions?

Key takeaways:

- **Create your own strategy!**
- **Start with simple quick wins!**

Introduction of Identity Governance

Introduction of Identity Governance

www.wpninjas.eu

01

Identity Lifecycle Management

For employees and guests

02

Controlling 3rd party apps

Access and provisioning to 3rd party apps

03

Access Lifecycle Management

Access Packages and Reviews

04

Azure AD PIM

Just in time just enough access

05

Terms of use

For employees and guests

06

Reporting

For generating reports

Introduction of Identity Governance

Define your Identity Governance Strategy by:

- Making sure your identities are **centrally managed** in Azure AD and are **secured**;
- Making the HR department responsible for the identity lifecycle(s), HR data will become the '**source of truth**' in your environment.
- Making sure that user **access & provisioning** to (3rd party) apps is managed from Azure AD;
- Identifying **Access Packages & Access Reviews** which can be created for your organization;
- Implementing the identified **Access Packages and Access Reviews**;
- Implementing **Just in Time permissions** for your administrator accounts with Azure AD PIM;
- Defining and implementing a '**terms of use**' which employees and guests must accept to use organization-data and -applications;
- **Monitoring** the usage and make the necessary enhancements within your setup.

Account Lifecycle Management

For employees and guests

Account Lifecycle Management

Lifecycle management explained

- Lifecycle management is important to be applied to all end user accounts.
- Accounts are therefore provisioned and disabled on time
- Control lies with HR .
- Making HR data the **source of truth** is key here!
- Only supported with SAP / Workday

- Lifecycle management is even **more important** for guest accounts.
- This as you are not the owner of where the account is ‘sourced’ from.
- Therefore, make sure you’ve implemented lifecycle management around guest accounts as well!

SuccessFactors to Active Directory User Provisioning
Microsoft

Workday to Active Directory User Provisioning
Microsoft

SuccessFactors to Azure AD User Provisioning
Microsoft

Workday to Azure AD User Provisioning
Microsoft

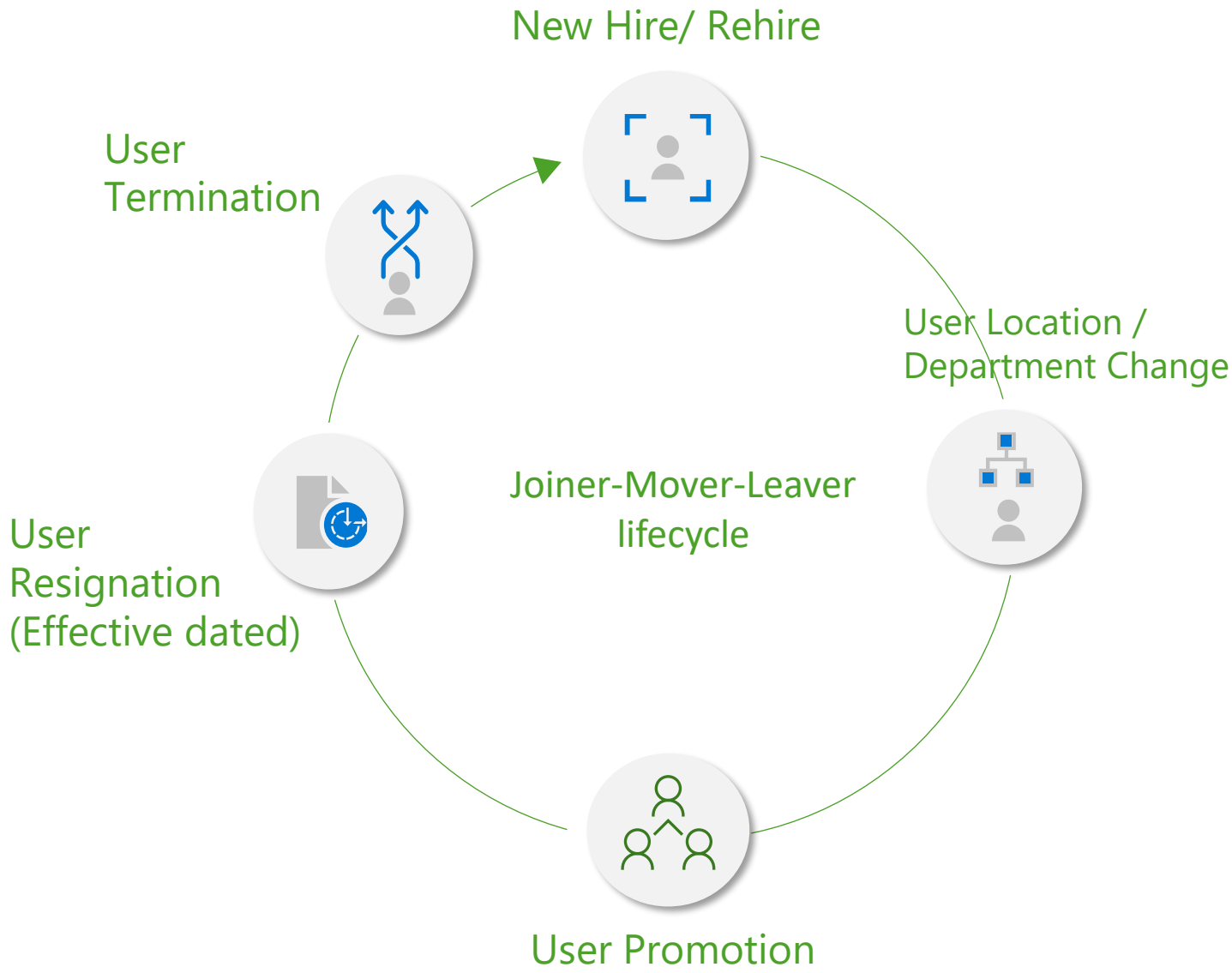
Account Lifecycle Management

Lifecycle management for employees

- HR provisions the user in the HR system.
- Provisioning will start automatically from the HR system to AD/AAD.
- AD/AAD account will be created.
- Updates are applied during promotions/ job changes.
- When the user terminates his/her contract the account will be disabled as well.

NOTE: Start with automated provisioning to 3rd party applications which support SCIM as a next step.

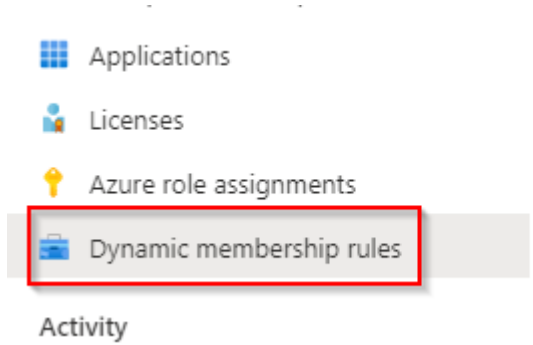
Result: Automated process and an improved security posture.

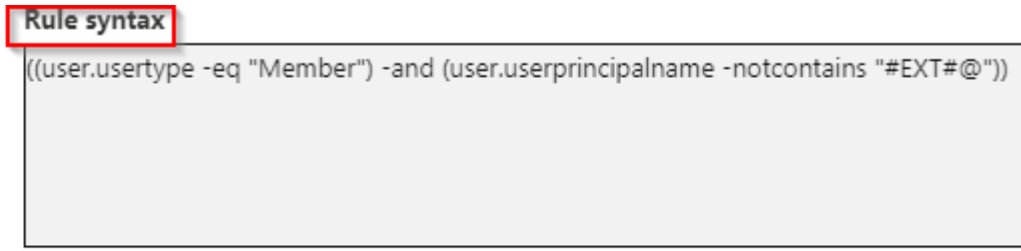


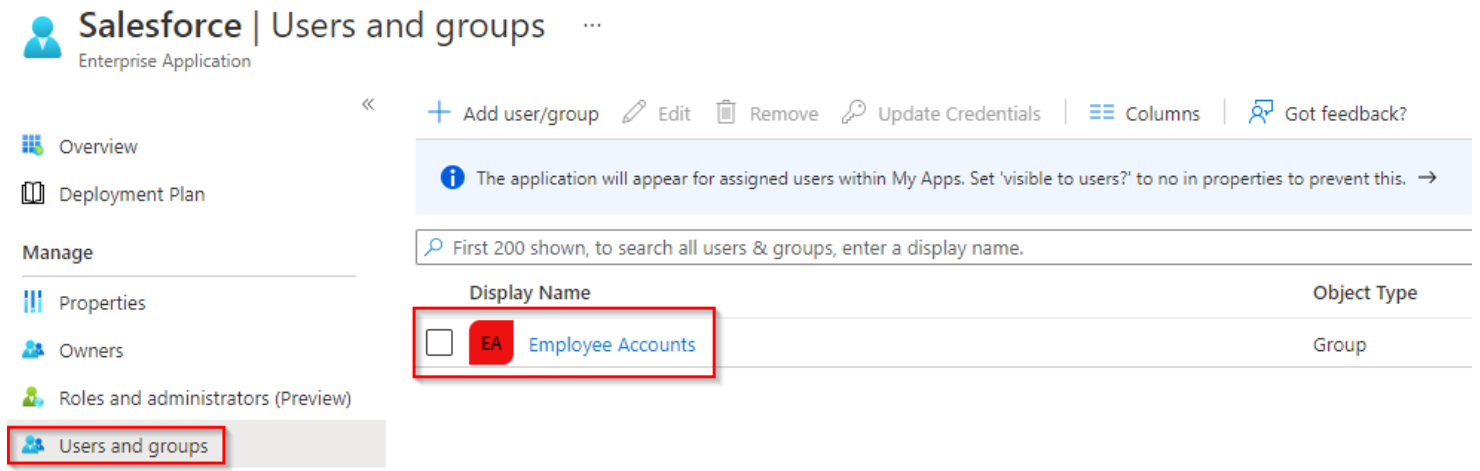
Account Lifecycle Management

Lifecycle management for guest users

- First start with the basics:
  - Create a group which ONLY contains employees.
  - Assign it to apps which are only required for your employees.
  - Make sure Assignment is required.







Account Lifecycle Management

Lifecycle management for guest users

- Basics continued:
  - Configure the guest user access in AAD.
  - Configure invite settings.
  - Configure collaboration restrictions (if required).

Guest user access

Guest user access restrictions ⓘ

Learn more

- ○ Guest users have the same access as members (most inclusive)
- ◉ Guest users have limited access to properties and memberships of directory objects
- ○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

- ○ ~~Anyone in the organization can invite guest users including guests and non-admins (most inclusive)~~
- ◉ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ○ Only users assigned to specific admin roles can invite guest users
- ○ No one in the organization can invite guest users including admins (most restrictive)

Collaboration restrictions

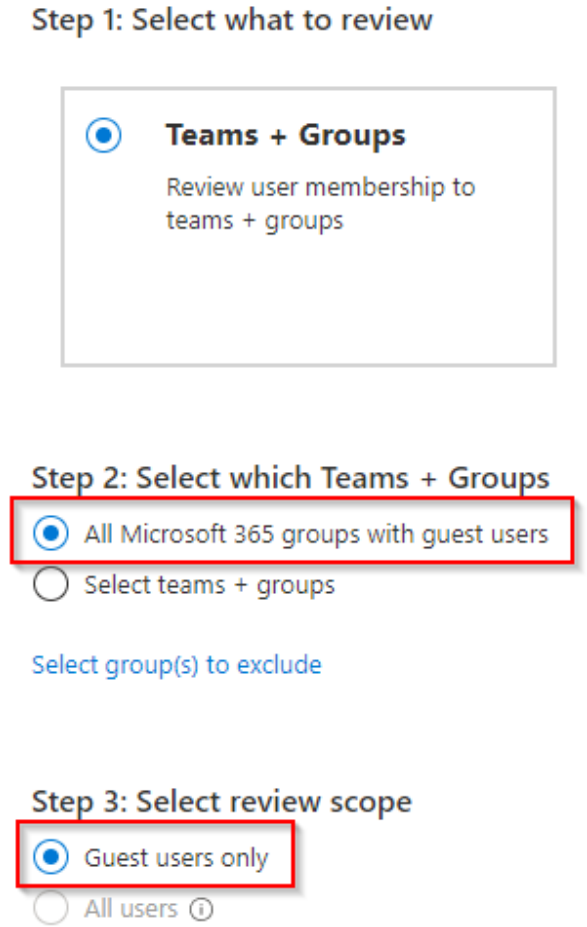
- ◉ Allow invitations to be sent to any domain (most inclusive)
- ○ Deny invitations to the specified domains
- ○ Allow invitations only to the specified domains (most restrictive)

Account Lifecycle Management

Lifecycle management for guest users

- When the basics are implemented start with a global access review for all your guest users.
  - This is only hits guest users who are a member of a Microsoft 365 (MS Teams) group.
  - Security groups aren't included in this feature.

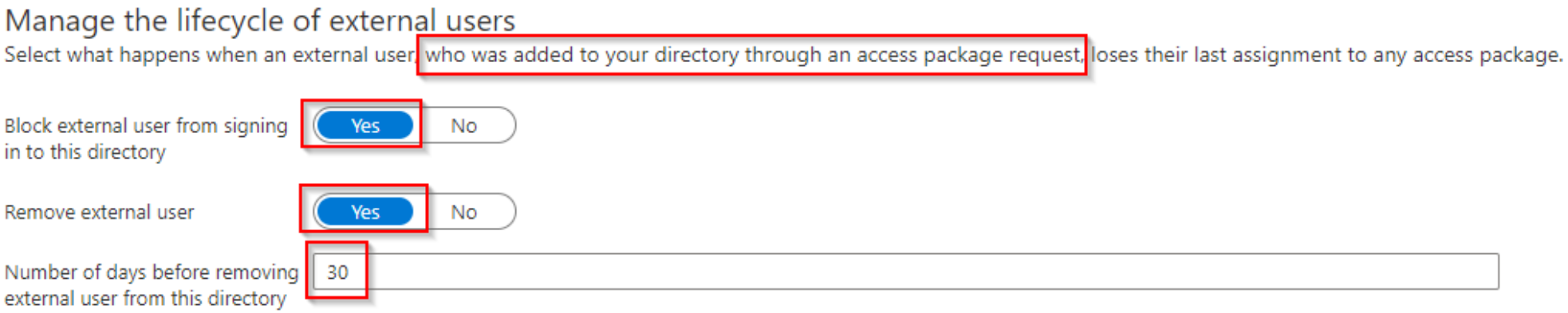
- Guests will then i.e. be challenged for a self-review to examine their own access (to possible sensitive information).



Account Lifecycle Management

Lifecycle management for guest users

- The last step is to configure the global tenant settings within Identity Governance, which exists of:
  - Settings which determine what happens when a users loses their last assignment to an access packages when it was added via an access package.



Code part 1

Lifecycle management for guest users

- Run a script to delete ‘Inactive accounts’ as it’s required for:
  - All existing guest users who are active today lifecycle management must be implemented manually.
  - All users who will be invited in the future (via Teams) outside the Identity Governance process.

```
#Connect to environment

Connect-AzAccount -ServicePrincipal -Tenant ad7aaf9d-e478-4d3f-99aa-ce450535d9cc -ApplicationId f7d7fe08-fd8b-47b0-93a2-ccf47669e74d -CertificateThumbprint *****

Connect-AzureAD -TenantId ad7aaf9d-e478-4d3f-99aa-ce450535d9cc -ApplicationId f7d7fe08-fd8b-47b0-93a2-ccf47669e74d -CertificateThumbprint *****


#Retrieve all user and get todays current date

$GuestUsers = Get-AzureADUser -All $true | where {(($_.usertype -like "guest") -or ($_.userPrincipalName -like "*#EXT#@*")) -and ($_.UserState -eq "Accepted")}

$Today = Get-Date
```

Code part 2


```
Foreach ($GuestUser in $GuestUsers) {

    $UserGroupMembership = Get-AzureADUserMembership -ObjectId $GuestUser.ObjectId

    $UserGroupMembership = $UserGroupMembership.count

    If ($UserGroupMembership -eq '0') {

        $userprincipalname = $GuestUser.mail

        [string]$WorkspaceID = 'd4c05fa0-1652-45e8-9ed0-bda450c81ee2'

        $QuerySignInCount = 'SigninLogs | where TimeGenerated > ago(60d) | where UserPrincipalName == "' + $UserPrincipalName + '" |
order by TimeGenerated desc nulls last | limit 1'

        $ResultsSignInCount = Invoke-AzOperationalInsightsQuery -WorkspaceId $WorkspaceID -Query $QuerySignInCount

        $AADSigninDate = $ResultsSignInCount.Results.TimeGenerated


        if ($AADSigninDate -like "") {

            $AADSigninDate = get-date

            $AADSigninDate = $AADSigninDate.AddDays(-62)

        }
```

Code part 3


```
        #Gather differences
        $DaysInactive = (New-TimeSpan -Start $AADSigninDate -End $Today).Days

        if (($DaysInactive -gt 30) -and ($DaysInactive -lt 60)) {
            write-output "Account $UserPrincipalname is inactive for $DaysInactive days, disabling the account“
            Set-AzureADUser -ObjectId $guestuser.ObjectId -AccountEnabled $false
        }

        if ($DaysInactive -gt 60) {
            write-output "Account $UserPrincipalname is inactive for $DaysInactive days, removing the account“
            Remove-AzureADUser -ObjectId $guestuser.ObjectId
        }
    }
    Else {
        write-output "Account $UserPrincipalname still has group memberships, skipping."
    }
}
```

Demo

Global Access Review for Guests Configuration

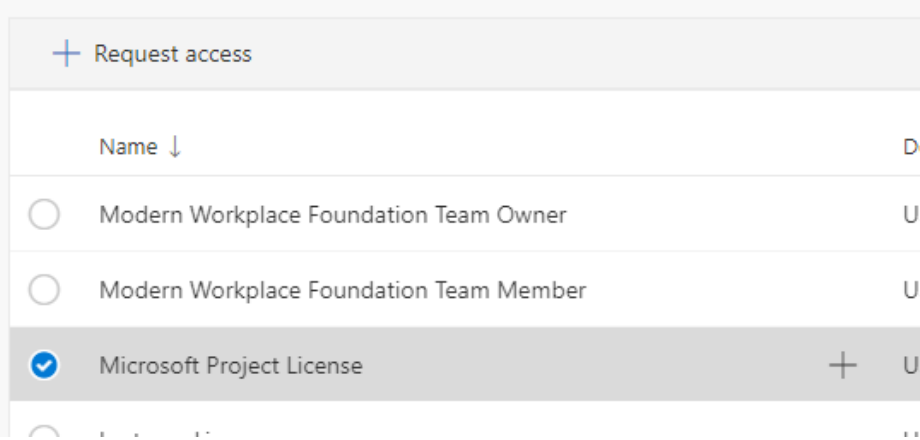
Running the cleanup script to disable / cleanup ‘inactive’ guest accounts.

Access Lifecycle Management

Access Lifecycle Management

How to implement Access Lifecycles?

- Create an access package with access review for access which fits this purpose (Groups & Teams, SharePoint Sites & Applications).
- Start with simple resources for access lifecycle management like:
  - MS Visio Licenses;
  - MS Project Licenses;
  - Other licenses;
  - Offer an opt-in to Insider release for Windows 11;
  - Access to 3rd party licensed SaaS software (Slack, SalesForce);
  - Access to 3rd party software provided within Endpoint Manager;
  - Access to MS Teams team which contains sensitive documents.



- Configure approvals per access package to make sure the request is reviewed.
- Use separation of duties if you have access packages which fit the same purpose but do have different settings attached.
  - Different insider preview rings attached (Slow / Fast).
  - User in sales team North can't be a member as well of Sales team West.

Access Lifecycle Management

How to implement Access Lifecycles?

- Configure connected organizations within Identity Governance so new or existing Guest users can request access packages as well.
  - These are organizations which you often work with, like suppliers.
- Start using access reviews for access already provided.
  - By review all your groups and making on a global scale access reviews where required (including security groups).

Name	Resource
Semi-Annual Access Review	Group Access Review Group Semi-Annualy
Semi-Annual Access Review	Group Global Access Review Group (Semi-Annualy)
Quartarly Access Review	Group Access Review Group Quartarly
Quartarly Access Review	Group Global Access Review Group (Quartarly)
Review guest access across Microsoft 365 groups	All Office Groups

Demo

Configuring Connected Organizations

Implementing and requesting an Access Package

- Microsoft 365 Visio

How & where to start tomorrow?

- Create your own **Identity Governance Strategy**.
- Make sure the **‘Manager’** is configured correctly on all user accounts.
- Make sure the **correct AD Premium licenses** (P2) are in place.
- Make sure to configure the correct **Global Tenant settings** for External Identities.
- Implement a **global access review** for your Guest (B2B) users to review access to Microsoft 365 Groups.
- Implement automated **lifecycle management for your Guest** (B2B) users via a script.
- Implement **‘simple’ access packages** for licensed software (i.e. Visio, Project, SalesForce, Slack & PhotoShop).
- Implement ‘**simple’ access reviews** for groups which provide access to sensitive information or software.
- Identify **other use cases** for the use of access packages & access reviews within your organization.
- Implement **lifecycle management for end user** accounts.

Q&A

Thank You