

# Best-practices for Power Platform Governance



Toni Pohl | Microsoft MVP | CTO atwork  
toni.pohl@atwork.at | [www.atwork-it.com](http://www.atwork-it.com)  
@atwork



[thriveconf.com](http://thriveconf.com)

# Governance...

“Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization.

It includes the mechanisms required to balance the powers of the members (with the associated accountability), and their primary duty of enhancing the prosperity and viability of the organization.”

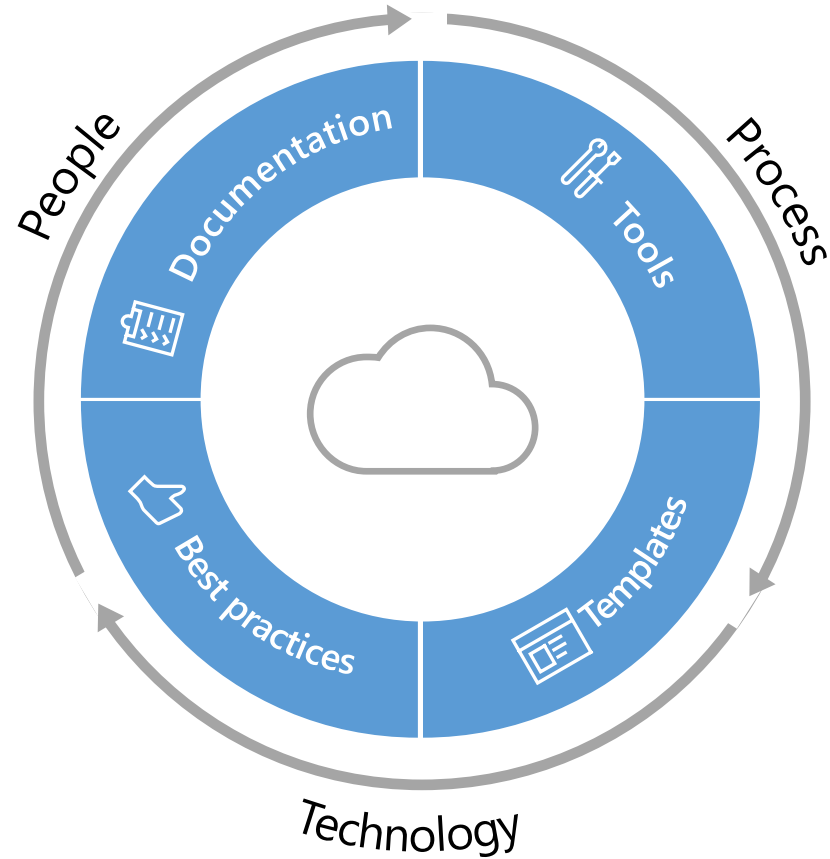
Business Dictionary

# Governance...

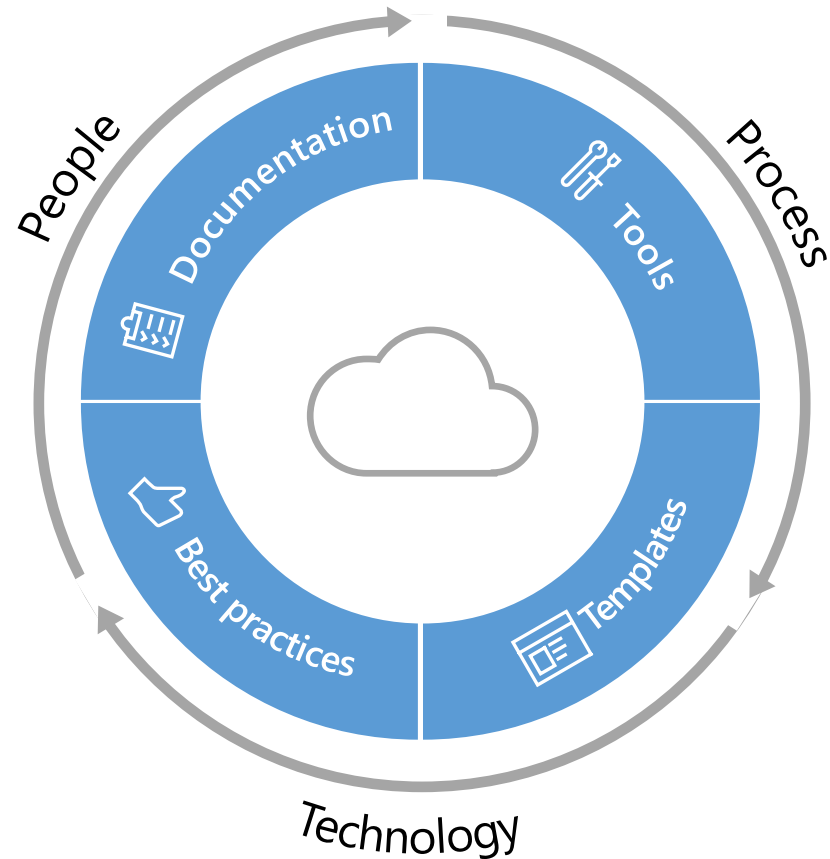
“Who can do what, when and under which conditions.”

(my simplified version)

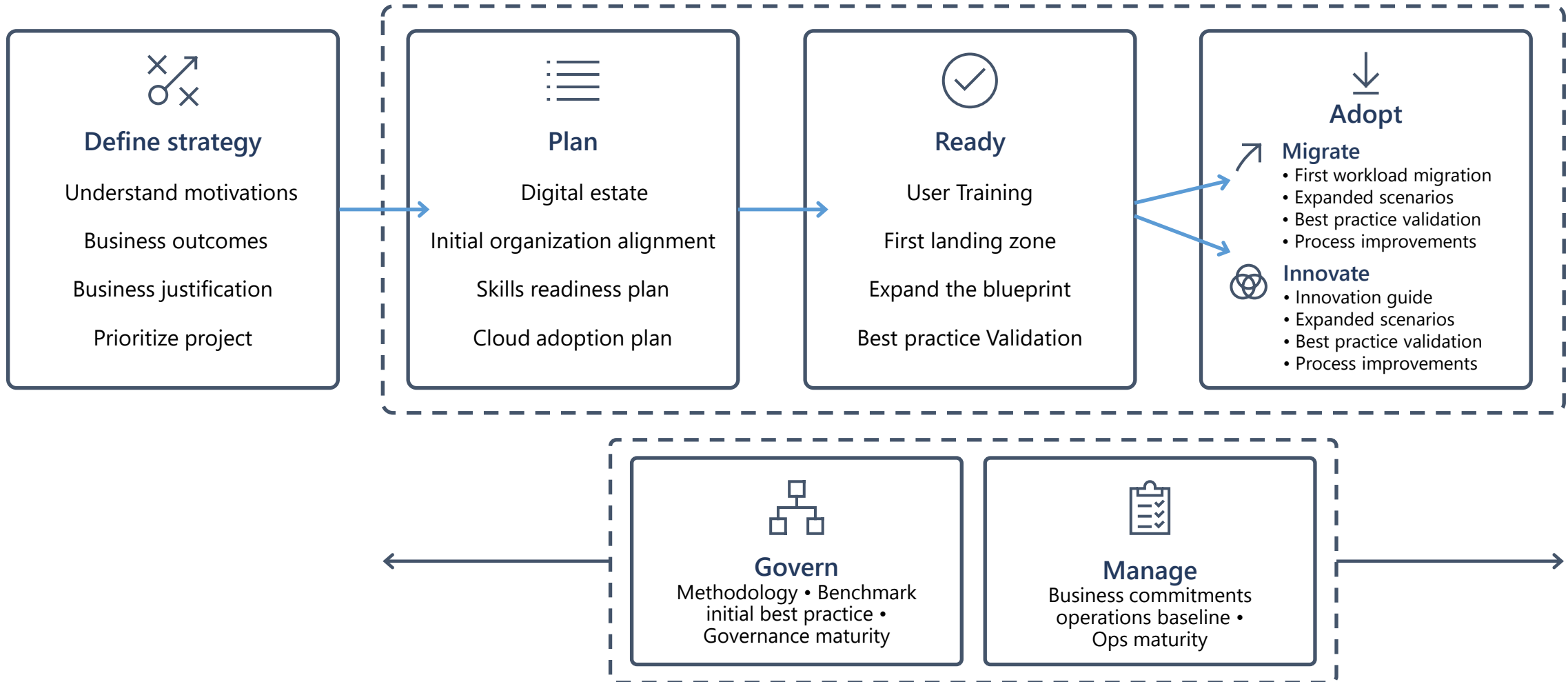
# The Governance principle



# The Governance principle



# Governance principles (for all technologies)



# **Governance for the Power Platform**

# Microsoft Power Platform

The low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications



## Power BI

Business analytics



## Power Apps

Application development



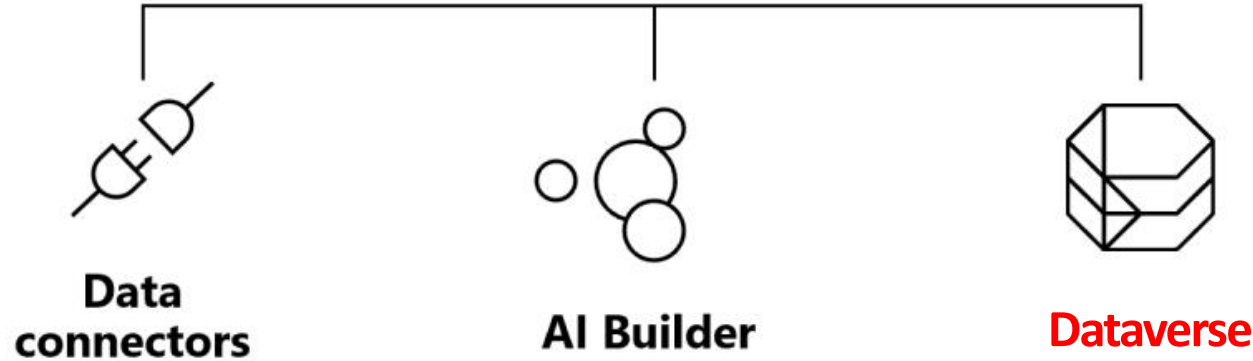
## Power Automate

Process automation



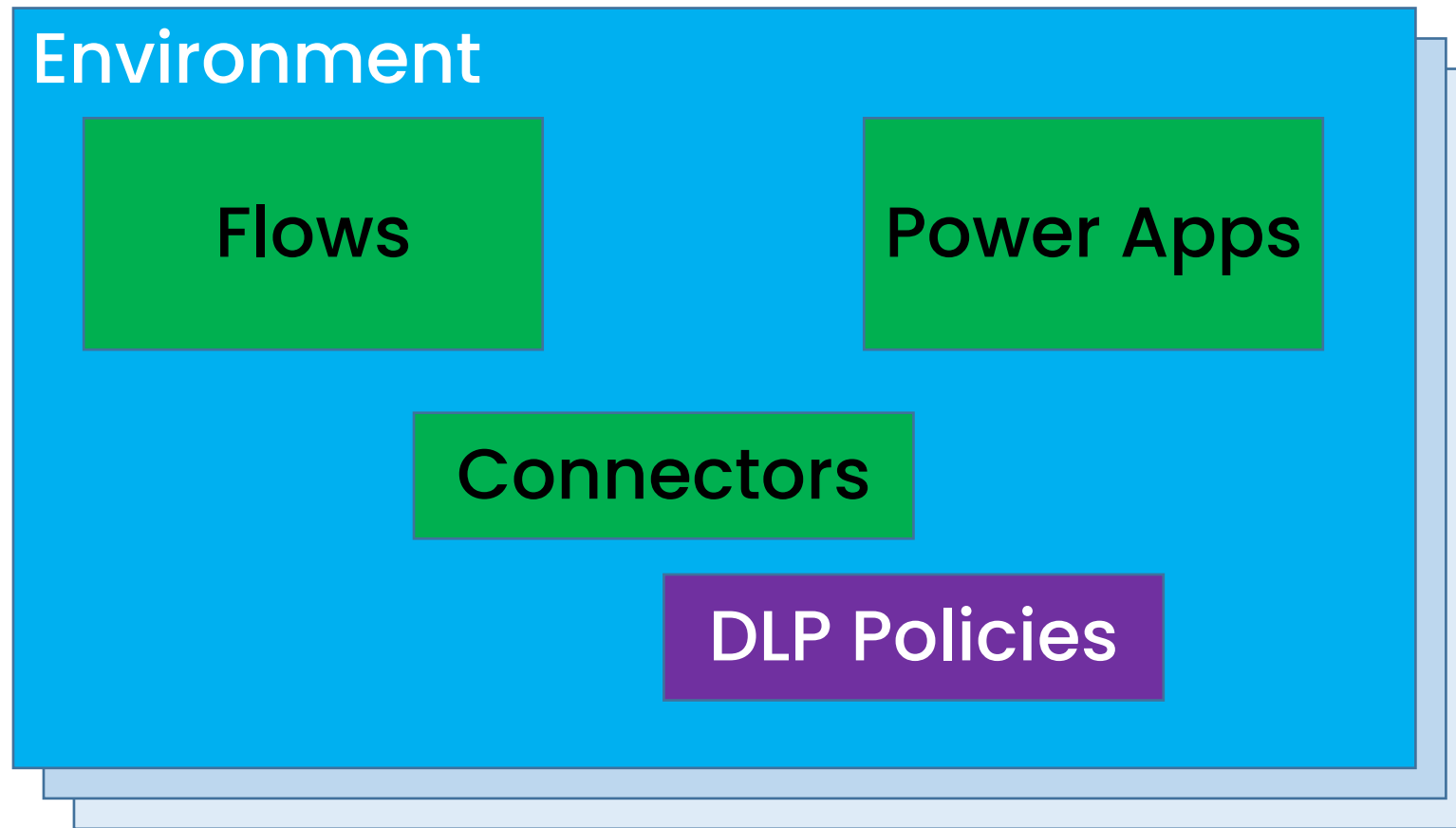
## Power Virtual Agents

Intelligent virtual agents





# The Power Platform management architecture



# Best practices #1

- Organize environments
- Use Admin-roles only for actual admins (use PIM)
- Assign User Licenses (later, not by default)
- aka.ms/ppac
- <https://app.powerbi.com/admin-portal>

atwork

Power Platform admin center

Environments

Analytics

Common Data Service

Power Automate

Power Apps

Resources

Capacity

Dynamics 365 apps

Portals

Help + support

Data integration

Data gateways (preview)

Data policies

Admin centers

Power BI

+ New ↺ Refresh

Environments

Environment	Type	State	Region	Created on ↓
CoE	Sandbox	Ready	Europe	08/24/2020 6:40 PM
Dev Environment	Sandbox	Ready	Europe	08/29/2019 8:35 AM
atwork deutschland gmbh	Production	Ready	Europe	03/20/2018 8:56 AM
TP Demo Environment	Sandbox	Ready	Europe	12/26/2016 10:33 AM
CW environment	Sandbox	None	United States	10/24/2016 11:28 PM
atwork (default)	Default	Ready	Europe	10/08/2016 6:08 PM
atwork (Upgrade, US)	Production	Ready	United States	10/08/2016 6:08 PM

Power Platform settings

These settings are applicable across your organization. [Learn more](#)

Governance

Enable features across environments.

Who can create production and sandbox environments

☒ Everyone

☐ Only specific admins ⓘ

Who can create trial environments

☒ Everyone

☐ Only specific admins ⓘ

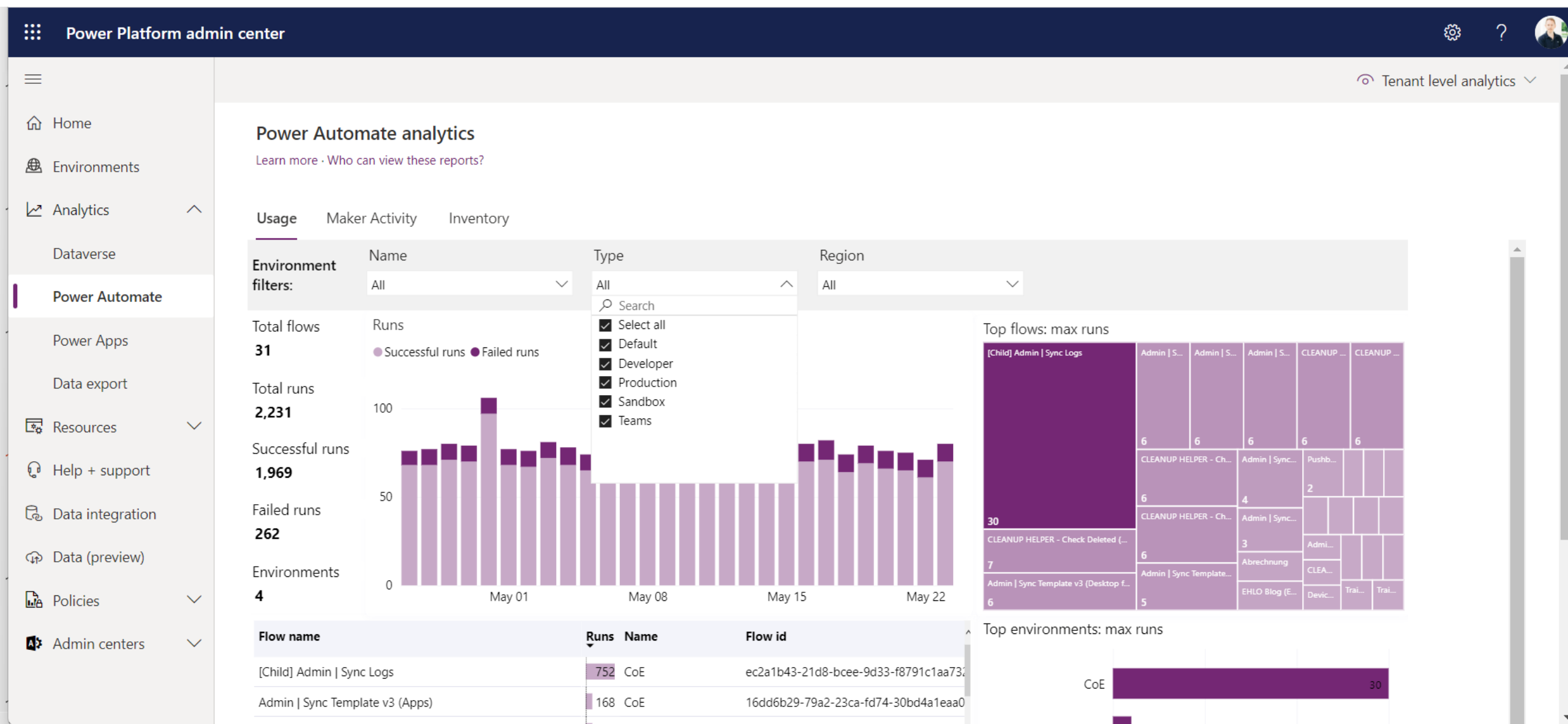
Save

Cancel

# Data governance in Power Platform

- Power Platform environments protect data using encryption at rest
- Define general and group-based environments permissions
- Define allowable / restricted connectors
- Define DLP policies

# Tenant level analytics





- Home
- Favorites >
- Recent >
- Create
- Datasets
- Goals
- Apps
- Shared with me
- Learn
- Workspaces >
- My workspace v

## Admin portal

## Tenant settings

- Usage metrics
- Users
- Premium Per User
- Audit logs
- Capacity settings
  - Refresh summary
- Embed Codes
- Organizational visuals
- Azure connections
- Workspaces
- Custom branding
- Protection metrics
- Featured content

## Workspace settings

## Create workspaces (new workspace experience)

*Unapplied changes*

Users in the organization can create app workspaces to collaborate on dashboards, reports, and other content. Even if this setting is disabled, an upgraded workspace will be created when a template app is installed.

☒ Enabled

The permission to create workspaces in the new workspaces experience preview is currently controlled by the permission to create groups in Office 365. By clicking Apply, the values below will control which users can create workspaces in the new workspaces experience preview. [Learn more.](#)

Apply to:

- ☐ The entire organization
- ☒ Specific security groups

 X Enter security groups☐ Except specific security groups

Apply

Cancel

## Use datasets across workspaces

*Enabled for the entire organization*

## Block classic workspace creation

*Enabled for the entire organization*

# **Power Apps & Automate When to use what?**

Best practices #2

# What is a Power App

 Microsoft.PowerApps

 manifest.json

Governance Toolkit 365 - Antrag Team erstellen (v1.1) admin@M365x029176.OnMicrosoft.com

**Eine neues Team erstellen**

Geben Sie hier die Daten des neuen Teams ein. Ihr Manager erhält Ihren Antrag zur Genehmigung. Sie erhalten eine Bestätigung per E-Mail und eine Benachrichtigung über den Status.

Projekt Typ\* Team

Name des neuen Teams\*

Der Name wird automatisch mit dem Projektnamen als Präfix ergänzt.  
**Team Name ist ein Mussfeld.**

Generierter Name

Begründung\*

**Begründung ist ein Mussfeld.**

Team ☒ Ja

Ja erstellt ein Teams Team. Bei Nein wird nur eine Microsoft 365 Gruppe erstellt, die nicht in Teams sichtbar ist.

Besitzer 1\* MOD Administrator

**Besitzer 1 ist ein Mussfeld.**

Besitzer 2\* Find items

**Besitzer 2 ist ein Mussfeld.**

Speichern Formular zurücksetzen



# When to use Power Apps



## Access

Work account or MSA  
Every user must have a license

## Standard Connectors

SharePoint, OneDrive, Excel, Outlook, Azure AD, etc.  
Records < 500

## Simple apps

Not too much screens & controls  
Not too complex: dependencies ...  
**Offline scenarios!**

## Guidance

Support your users with rules, training & best practices



HP  
**EliteBook**

1049



HP  
**ProBook**

499



Samsung  
**Series 9**

1599.99



Microsoft  
**Surface Pro**

999

[Order](#)[Back](#)

# When NOT to use Power Apps



## Access

External users  
No license

## Premium Connectors (key users)

HTTP, Azure SQL, SAP, Custom Connectors, Third party,...  
Records > 500

## Complex apps

Many screens & controls  
Dependencies, Permissions

## Performance

Power Apps are no native apps...

Project

Phase 1: Basic Information

Progress:

Overview

Project

Phase 1: Basic Information

Basic Information

Ownership

Timing

Execution

Why (Reason)

Why (Strategy)

Add Attachments

Submit

Phase 2: Detailed Information

SWOT Analysis

## HISTORY - 77 - TEST A

### PROJECT STATIONS

### BASIC INFORMATION

### PROJECT OWNERSHIP

### TIMING

### EXECUTIVE SUMMARY

DATE	USER	
2020-10-06 09:21:00	Toni Pohl	
2020-10-06 09:21:00	Toni Pohl	
2020-10-06 09:21:00	Toni Pohl	
2020-09-15 06:04:00	Andreas	

### WHY (REASON)

### WHY (STRATEGY)

### ADD ATTACHMENTS

## PROGRESS REPORT

Please add a short report on the most important results achieved and the progress of the project, referring to the defined outputs, outcomes and the impact. Please don't forget to mention the time period you are referring to.







### OUTCOMES

OUTCOME	CATEGORY	TARGET GROUP(S)	INDICATOR(S)	
Outcome 1	Long-Term	Target Group(s) 1	Indicator(s) 1	<input type="checkbox"/>
Outcome 2	Long-Term	Target 2	Indicator 2	<input type="checkbox"/>

### OUTPUTS

OUTPUT	TARGET GROUP(S)	INDICATOR(S)
Output 1	Target 1	
Output 2	Target 2	

### SHORT REPORT ON THE MOST IMPORTANT RESULTS (OPTIONAL)

**B** U       default 3

Please fill in text here...

Custom controls  
Complex workflows  
Permissions  
Additional functionality  
Reporting, Export, PDF, ...

# When to use Power Automate



## Usage

Users have a license coming with their "Ex" license assignment  
Using the M365 connectors

## Personal scenarios

Get data from another source into M365 or vice versa  
Automate personal workflows

# When NOT to use Power Automate



## Licenses

No Power Automate licenses  
HTTP & enterprise connectors

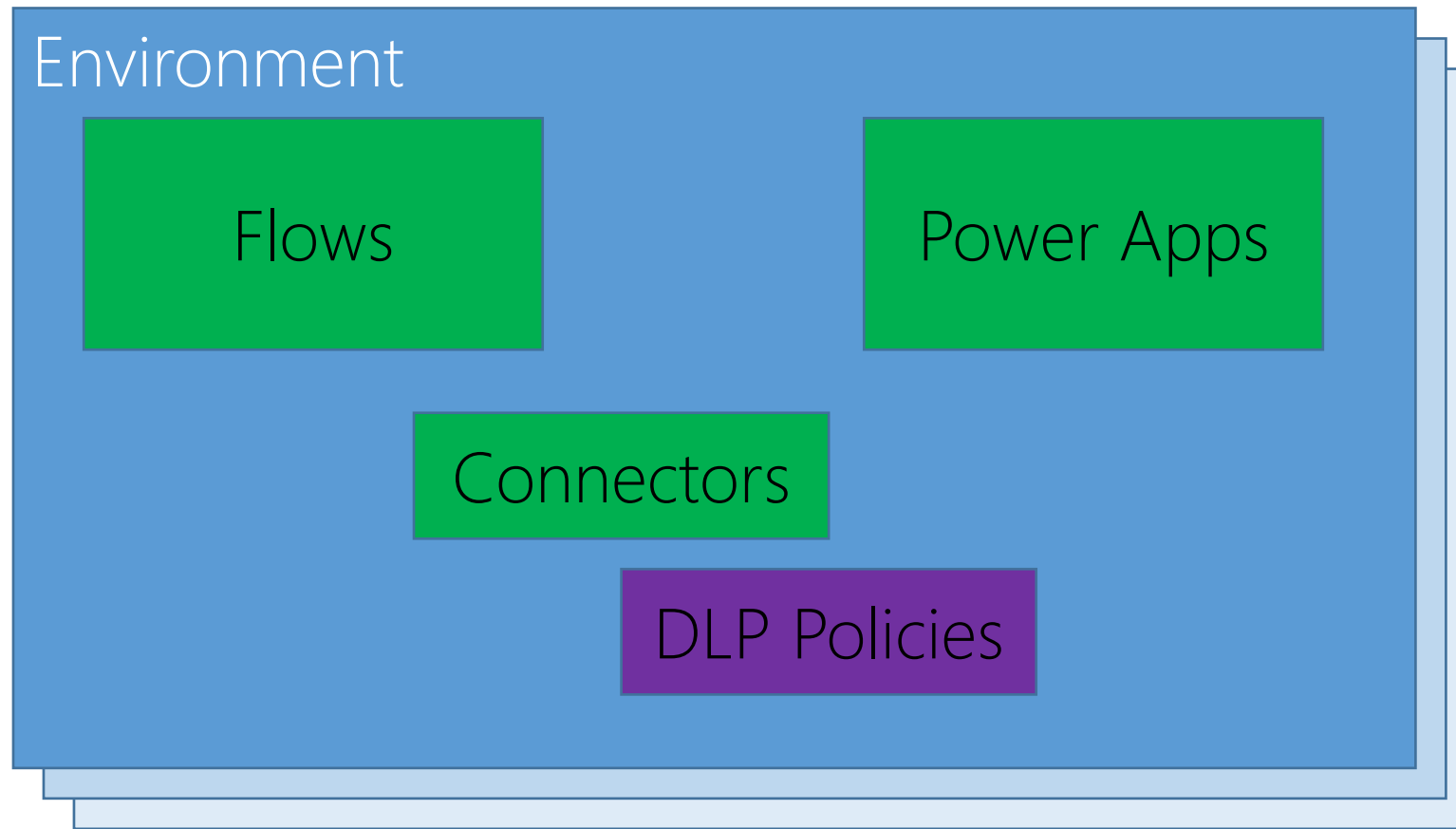
## Organization or Department scenarios

Use Azure Logic Apps for "organization" tasks  
Require HTTP connections  
Pay per use in Azure = leave budget for personal flows

# Best practice #3

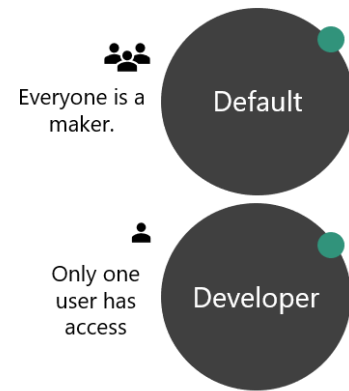
Plan your environments

# The Power Platform management architecture



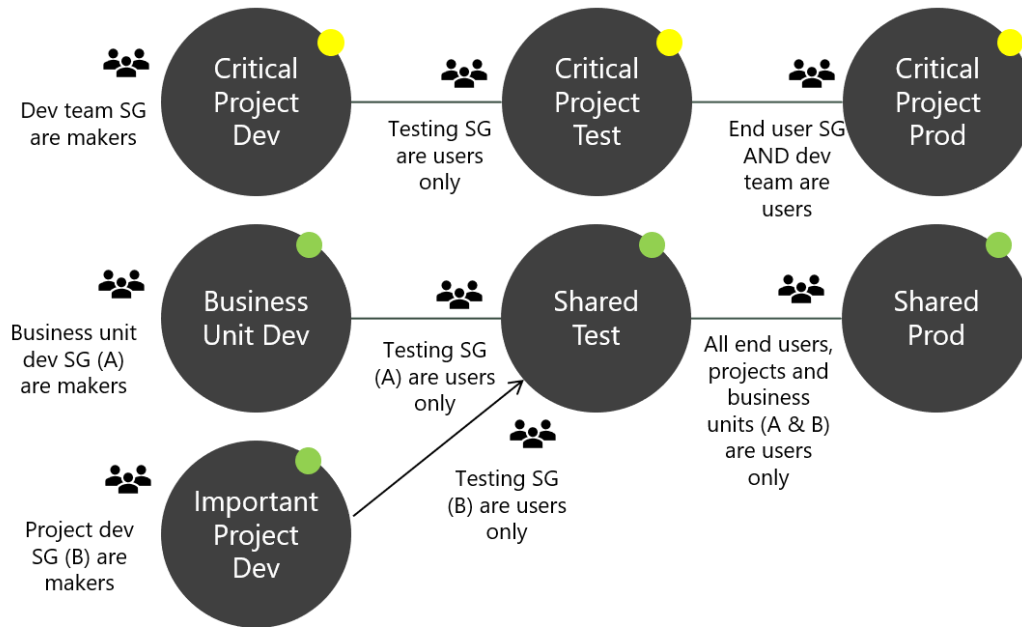


# Example environment strategy diagram



Communicate with everyone that **Default** is not for development of critical apps.

**Developer** environments are completely locked for any other user except the user who subscribed to the community plan. Applications can be moved out of the environment if needed.



**Dedicated** dev/test/prod environments for each critical application. Developers have Environment Maker access in the dev environment, but only user access in test and prod. End users only have end user access to the production solution so no one can modify the applications.

**Shared** test/prod environments for important but medium complex apps can be shared between multiple projects or business units. Individual projects and business units should always have their own development environment to protect data. End users only have basic user access to solutions and data in production environments.

- Critical project
- Individual project
- Personal productivity apps

SG = Security Group

# Best practices #4 – Configure Data loss prevention policies (DLP)

## DLP

- DLP policies enforce rules for which connectors can be used together by classifying connectors as either **Business** or **Non-Business**.

## Business

- If you put a connector in the **Business** group, it can only be used with other connectors from that group in any given app or flow.

## Block

- Sometimes you might want to block the usage of certain connectors altogether by classifying them as **Blocked**.

# Best practices #5 (Must Have)

- Center of Excellence (CoE)
- [aka.ms/coestarterkitdownload](https://aka.ms/coestarterkitdownload)
- [aka.ms/coestarterkit](https://aka.ms/coestarterkit)

# Center of Excellence (CoE)

[aka.ms/coestarterkitdownload](https://aka.ms/coestarterkitdownload)

[aka.ms/coestarterkit](https://aka.ms/coestarterkit)

# CoE Starter Kit



## Overview

Define goals and expected outcomes of your CoE

- [Overview](#)
- [Motivation](#)
- [Download](#)



## Admin

Gain insights into your Microsoft Power Platform adoption

- [Set up](#)
- [Use](#)
- [Deep dive](#)



## Govern

Establish audit and compliance processes

- [Set up](#)
- [Use](#)
- [Deep dive](#)



## Nurture

Accelerate your adoption by thriving with a community of makers

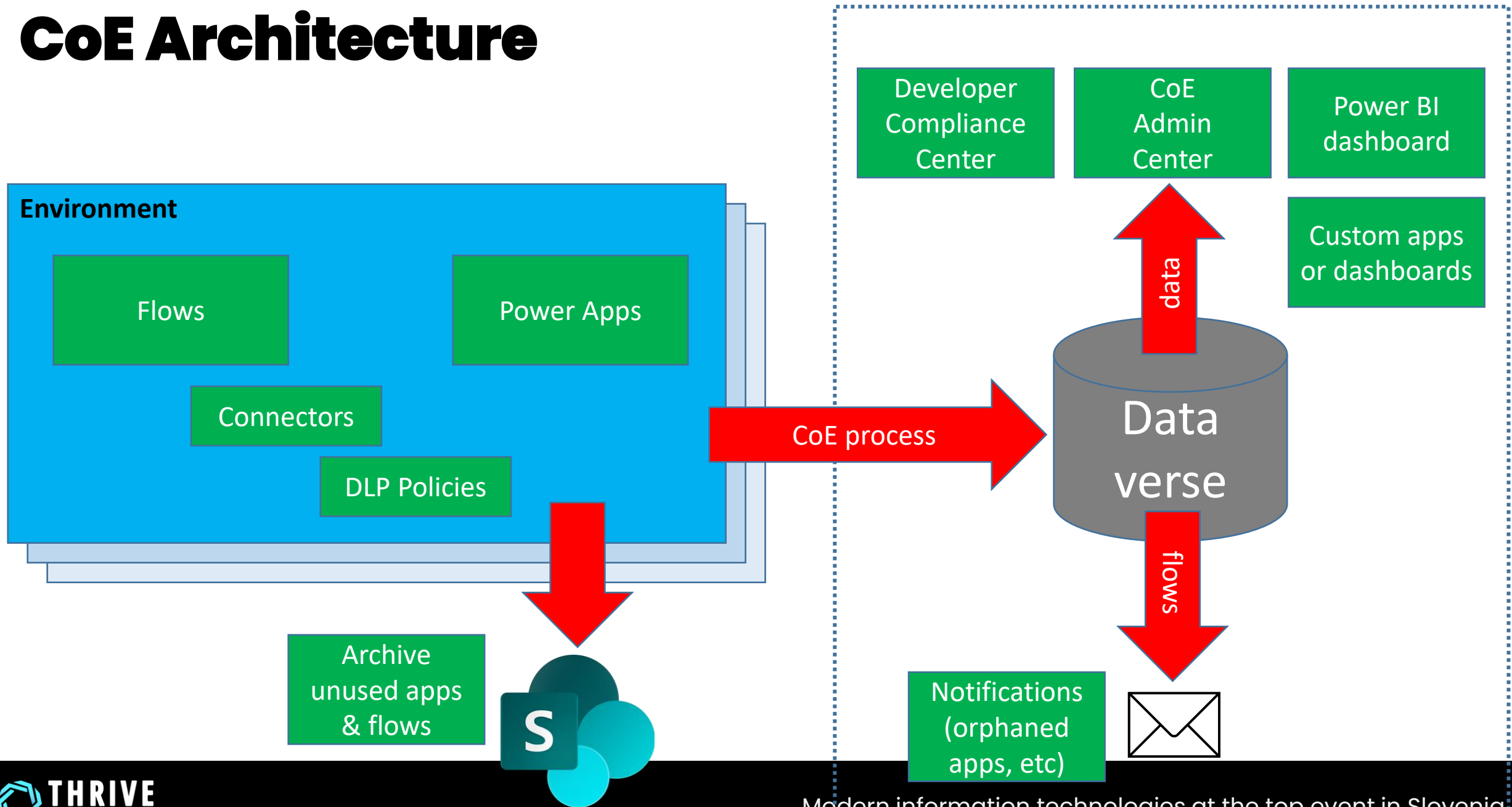
- [Set up](#)
- [Use](#)

...a collection of components and tools for adopting and supporting Microsoft Power Platform, with a focus on Power Apps, Power Automate, and Power Virtual Agents.

# Install CoE requirements

- <https://aka.ms/CoeStarterKitDownload>
- Microsoft Power Platform service admin, global tenant admin (or Dynamics 365 service admin)
- Power Apps Per User license (non-trial) and Microsoft 365 license
- Power Automate Per User or Per Flow license (non-trial)
- The identity must be email-enabled
- If you'd like to collect telemetry information, such as app launches and unique users per app, the identity must have access to the Microsoft 365 audit log

# CoE Architecture



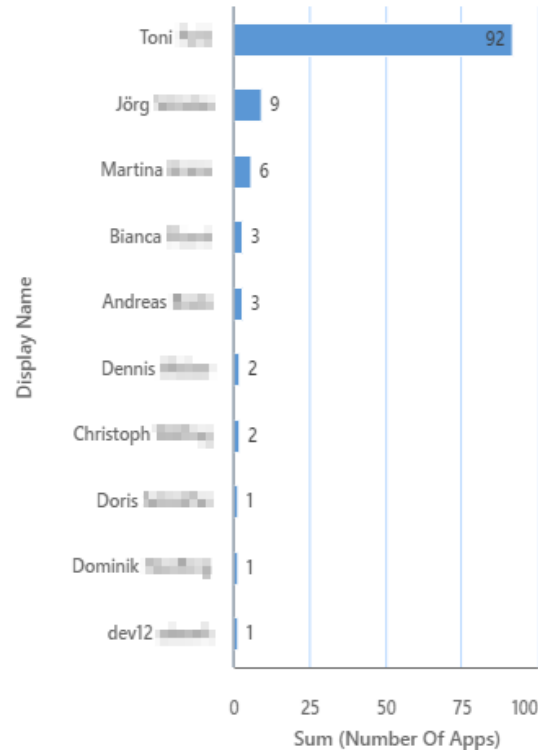
Save As + New ▼ ✓ Set As Default Refresh All

## Power Platform Dashboard ▼

### Active Makers

Expand Chart ⋮

#### Makers

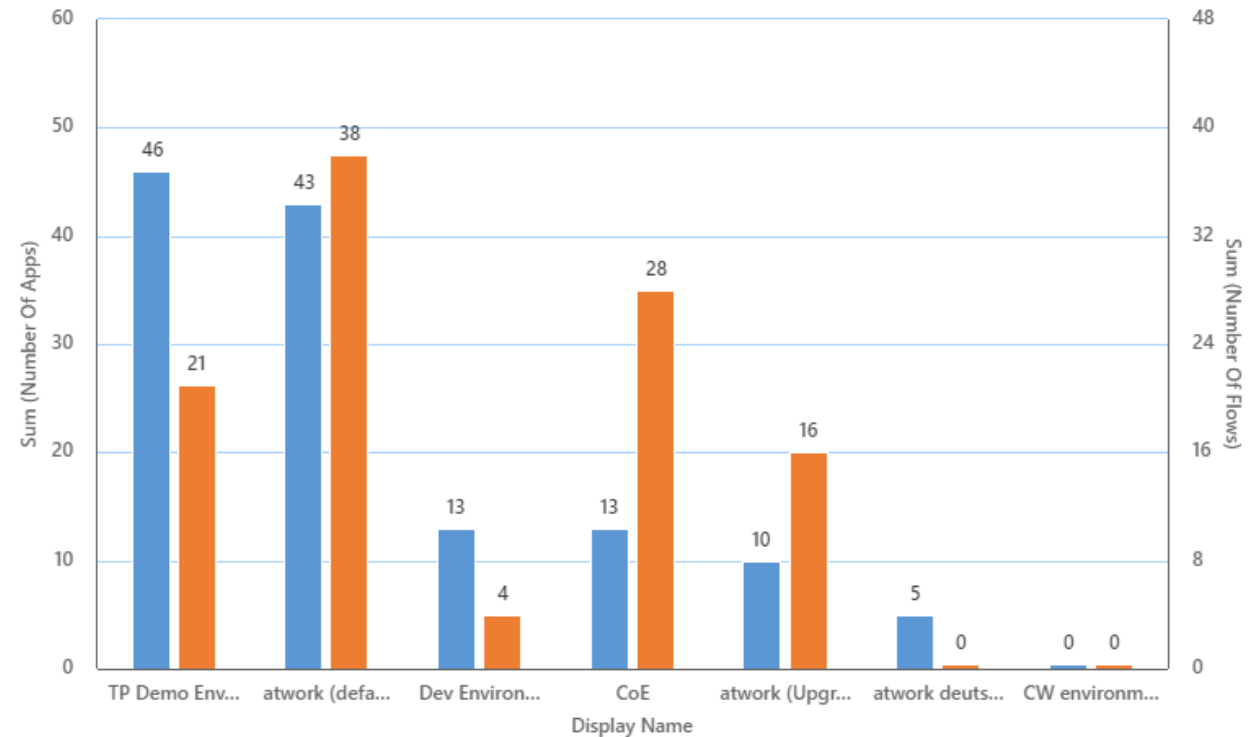


### Active Environments

Expand Chart ⋮

#### Environments

● Sum (Number Of Apps) ● Sum (Number Of Flows)



### Active Makers

Expand Chart ⋮

Delete ▼ ⋮



[← Back to dashboard](#) [⚙ App Settings](#) [↶ Re-publish](#) [🚀 Launch](#) [✉ Email users](#) [🗑 Delete App](#)

## App overview

**Drivers Logbook**

TP Demo Environment

### DETAILS

Created

January 22, 2017

Modified

January 22, 2017

Last published

0 days

App Type

Canvas

Description



To Add Description: Go to the App Settings > Edit the App > Settings > Add Description > Save and Publish. Then return here and click the refresh button below.

### APP COMPLIANCE

- Submitted Support Details
- Filled out app description
- Published within 60 days

### SUPPORT DETAILS

#### Maker Requirement - Business Justification

Collect drivers data directly on a mobile phone

#### Maker Requirement - Access Management

#### Maker Requirement - Dependencies

#### Maker Requirement - Business Impact

Important



#### Maker Requirement - Data Classification

Confidential



#### Mitigation Plan Provided

No



#### Category

Human Resources



#### Attachments

There is nothing attached.

 Attach file[Submit](#)

### PERMISSIONS (3)

ROLE

TYPE



Toni

Owner

User



Jörg

CanEdit

User



Everyone in the organization

CanView

Tenant

# CoE Power BI

- <https://docs.microsoft.com/en-us/power-platform/guidance/coe/setup-powerbi>
- Use the **Production\_CoEDashboard\_MMMYY.pbix** file if you have installed the CoE Starter Kit in a Production environment.
- Use the **Teams\_CoEDashboard\_MMMYY.pbix** if you have installed the CoE Starter Kit in a Dataverse for Teams environment. This version connects to Microsoft Dataverse using the TDS endpoint, therefore the TDS Endpoint has to be enabled for the environment: Manage feature settings.

# Connect Power BI to the CoE environment

<https://docs.microsoft.com/en-us/power-platform/guidance/coe/setup-powerbi>

The screenshot displays the Power Platform admin center interface. On the left, the navigation pane includes 'Home', 'Environments', 'Analytics', 'Resources', 'Help + support', 'Data integration', 'Data (preview)', and 'Policies'. The 'Environments' section is selected, showing a list of environments. The 'CoE' environment is highlighted, and its details are shown in a panel on the right. A red arrow points from the 'Environment URL' field in the details panel to the 'OrgUrl' field in a modal dialog box titled 'Production\_CoEDashboard\_March2022'. This dialog box contains the text 'CoE Power BI Dashboard', the 'OrgUrl' field with the value 'https://org[redacted].crm4.dynamics.com/', and 'Load' and 'Cancel' buttons. Below this, another modal dialog box titled 'Cds' is visible, showing the same 'OrgUrl' and a 'Sign in as different user' button. The 'Cds' dialog also has 'Connect' and 'Cancel' buttons at the bottom.

Power Platform admin center

Open environment Settings

Environments > CoE

Details

Environment URL  
org[redacted].crm4.dynamics.com

Refresh cadence  
Frequent

Organization ID  
88f85[redacted]

Production\_CoEDashboard\_March2022

CoE Power BI Dashboard

OrgUrl  
https://org[redacted].crm4.dynamics.com/

Load Cancel

Cds

Organizational account

https://org[redacted].crm4.dynamics.com/

You are currently signed in.

Sign in as different user

Connect Cancel

# CoE Upgrade

- <https://docs.microsoft.com/en-us/power-platform/guidance/coe/after-setup>
- „We recommend upgrading at least every three months.“
- <https://github.com/microsoft/coe-starter-kit>

# Automation of the Power Platform with PowerShell

Best practices #6

Automation of the Power Platform & Power BI governance is possible with PowerShell (& API)

**Note:** Power BI is not covered in the CoE

modify-app-roles.ps1 > ...

```

1  #-----
2  # modify-app-roles.ps1
3  #-----
4  Get-AdminPowerAppEnvironment | ft
5
6  # $environment = Get-AdminPowerAppEnvironment -Default
7  $environment = Get-AdminPowerAppEnvironment -EnvironmentName 'a19c40e9-731d-4338-aa9e-c83c502185d8'
8  $environment
9
10 # $environmentid = $environment.Internal.id
11 # We need to extract the ID only from
12 # "/providers/Microsoft.BusinessAppPlatform/scopes/admin/environments/Default-<someid>"
13 $environmentid = $environment.Internal.id.split("/")[1]
14 Write-Output "Environment ID: $environmentid"
15
16 $apps = Get-AdminPowerApp | Where-Object {$_.EnvironmentName -eq $environmentid }
17 # $apps | Format-Table -Property DisplayName, CreatedTime, EnvironmentName
18 $apps | ft
19 $apps | export-csv .\apps.csv -Delimiter "," -Encoding UTF8 -NoTypeInformation
20 $apps.count
21
22 # AppName
23 $myapp = $apps | Where {$_.DisplayName -eq "DeviceOrder2" }
24 $myapp.AppName
25
26 # Get the permissions for a specific app
27 # Get-AdminPowerAppRoleAssignment (previously Get-AdminAppRoleAssignment)
28 Get-AdminPowerApp -AppName $myapp.AppName -EnvironmentName $environmentid `
29 | Get-AdminPowerAppRoleAssignment `
30 | Select PrincipalDisplayname, PrincipalObjectId, RoleType, AppName, EnvironmentName `
31 | ft
32
33 # Add a user. We need the UserID from Azure AD.
34 # BiancaP
35 $userid = "ffc33f12-5f31-4fff-a1c1-60ddd3d617d3"
36

```

TERMINAL PROBLEMS 7 OUTPUT DEBUG CONSOLE











2: PowerShell Integrat...


```

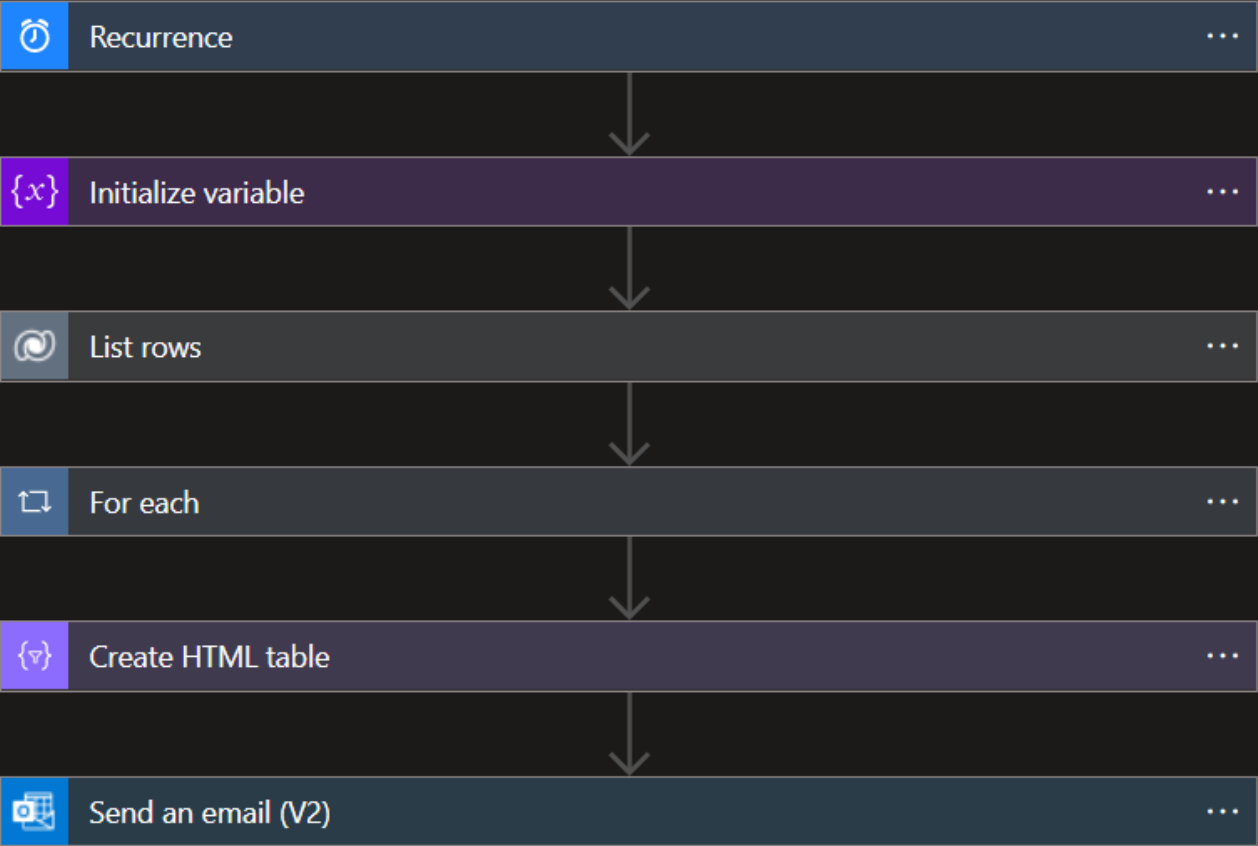
PS C:\TFSRepo\Session\CoE> Write-Output "Environment ID: $environmentid"
Environment ID: a19c40e9-731d-4338-aa9e-c83c502185d8
PS C:\TFSRepo\Session\CoE>

```

# Logic Apps Designer

 Save  Discard  Run Trigger  Designer  Code view  Parameters  Templates  Connectors  Help  Info

 100%



# Summary: Plan your governance



## Phase 1: Analyse, Planning , Controlling

- Monitor Power Apps and control new solutions
- Architecture, License and Security
- ppac, Environments, Connectors, Common Data Services, Data Loss Prevention (DLP)
- **Define roles and responsibilities**



## Phase 2: Use tools

- Tools like PowerShell, CoE, or 3rd party solutions: [governancetoolkit365.com](https://governancetoolkit365.com), etc
- Monitoring, Alerts and Deployment (DevOps)
- Monitor Power Apps and control new solutions



## Phase 3: End User Adoption

- Let your users transform into Makers
- Listen and learn about the Business Requirements (app life cycle)



# References

- SharePoint PnP
- Microsoft 365 Groups creation
- Microsoft 365 Groups Governance
- Techcommunity: Governance Plan with Teams
- Susan Hanley: Governance Questions for SharePoint
- Governance Toolkit
- Microsoft 365 Governance Resources
- CloudHub
- Training: Microsoft Teams Governance
- Groups Architecture Poster
- Excel Sheet
- [www.GovernanceToolkit365.com](http://www.GovernanceToolkit365.com)

# THANK YOU



Sponsors



INTELLITY

