pb powerbunch



SAMPLE

Governance Starter Kit for the Microsoft Power Platform

Set up rules, roles, and environments for Power Automate, Power Apps, and Copilot Studio in your organization

54 assessment questions | 15 decision points | 60 steps | Policy | Forms | Workbook

Original pages from the 64-page handbook: contents and chapters 01, 03, and 05. The other pages are omitted, and the page numbers refer to the full handbook.

Version 1.0 · As of November 15, 2026 · Reiner Keller, powerbunch GmbH

Contents

01	**Welcome**	3
02	**The kit at a glance**	4
03	**Governance in five steps**	5
04	**Current status of Microsoft tools**	7
05	**Zones and environments**	9
06	**Data policies and connectors**	11
07	**Sharing and access**	12
08	**Solution lifecycle**	13
09	**Roles and responsibilities**	14
10	**AI features and agents**	15
11	**Security, logging, and data protection**	16
12	**Decisions: The 15 decision points**	17
13	**The 54 assessment questions**	20
	Tenant and roles	20
	Default environment	24
	Environments	27
	Data policies	31
	Sharing and access	35
	Lifecycle	38
	Security and logging	41
	AI and agents	44
14	**The rollout plan**	47
15	**Working with the workbook**	51
16	**Common mistakes and questions**	53
17	**Handbook terms and Microsoft labels**	54
18	**If you would like support**	55
A	**Appendix: Welcome content for makers (template)**	56
B	**Appendix: License terms**	58

01

Welcome

In almost every company, the Power Platform grows faster than the rules for it. First a flow to organize your own files, then an app for the team, soon an agent for questions from sales. I have been helping companies with this since 2018, and the questions are almost always the same: Who may build what, where does it belong, which data may flow where, and what happens when someone leaves the company?

This starter kit helps you establish Power Platform governance without starting from scratch. Use 54 assessment questions to assess your current position, choose how strict your rules should be at 15 decision points, and adapt a ready-to-use policy. The workbook, forms, and 60-step rollout plan help put the rules into everyday practice.

2026 is a good time for this, and for some companies an urgent one. Microsoft no longer maintains the CoE Starter Kit and has moved its tasks into the Power Platform admin center. Unmanaged developer environments and Dataverse for Teams are deprecated, and from February 2027 Microsoft begins enforcing license requirements for Managed Environments. This kit builds on the current state and tells you where each recommendation comes from.

Wishing you a successful rollout,

Reiner Keller
Microsoft Power Platform Expert, powerbunch GmbH

Who it is for

For IT management, Microsoft 365 or Power Platform administration, information security, and anyone setting up a Center of Excellence (CoE) for the Power Platform. Suitable for midsize companies as well as for departments of larger enterprises.

Prior knowledge

You know Power Automate and Power Apps from a user or maker perspective and have access to the Power Platform admin center or work with the person who has it.

Access

Read access is enough for the assessment. To change settings, you need the Power Platform Administrator role, and for some steps also access to Microsoft Entra and Microsoft Purview.

Time required

The time needed for the assessment depends on the number of environments and solutions. The rollout plan allows about nine weeks for decisions, formal policy adoption, and configuration.

03

Governance in five steps

From the current state to ongoing operations in about nine weeks. The steps correspond to the phases in the Rollout plan sheet.

1	2	3	4	5
Time-critical items first	Assess the current state	Decide	Adopt	Configure and operate

1 Time-critical items first

Rollout plan, Phase 0

Three Microsoft deadlines will not wait for your policy. Unmanaged developer environments will be suspended from December 15, 2026, and deleted from January 15, 2027. From February 2027, apps in Managed Environments open only for people with an appropriate license. Dataverse for Teams environments that have not been upgraded to Dataverse will be suspended from September 15, 2027.

Check these three items first. Assessment questions B18, B20, and B21 and steps E01 to E03 tell you where to look in the admin center and what to do.

2 Assess the current state

Assessment, Environment plan, Inventory

Appoint a small core team representing administration, the Center of Excellence, information security, and data protection. Inventory and analytics also show who built and used what. Before exporting or analyzing this data, work with your data protection team and, where applicable, the works council to verify and document whether existing arrangements cover the purpose, scope, access, retention, and deletion (E05, B48).

Then work through all 54 assessment questions. For a question linked to a decision point, rate whether the adopted option has been implemented, regardless of whether it is the recommended option. Add all environments to the Environment plan sheet. Download the inventory only after completing the checks described above. Export only the data you need and store it with restricted access. The Results sheet shows your current position, and the Action plan sheet shows what to address first.

3 Decide

Decisions, Connectors, Roles, Risk assessment

Define the zones, select an option at each decision point, classify connectors, assign roles, and confirm risk classes. The workbook is prefilled with recommendations suitable for many companies. The “Decisions” chapter explains the consequences of each option.

4 Adopt

Policy, forms, quick reference

Transfer your decisions into the policy, replace the placeholders, and have the policy formally adopted. Provide the forms and the quick reference where makers will find them, and announce new rules with some lead time.

5 Configure and operate

Rollout plan, Phases 3 and 4

Apply the settings in the admin center in the order of the plan: first the tenant and the default environment, then environments, groups, and rules, and finally routing and the allowlist. Test strict data policies in a test environment beforehand.

Once configuration is complete, establish a review routine. Review recommendations, inventory, and licenses monthly. Review new connectors and the default environment quarterly, and review the policy annually. The workbook highlights validation messages and overdue dates.

Schedule

Phase	Time frame	Steps
0 Time-critical	immediately	E01 to E03 (3)
1 Assessment	weeks 1 and 2	E04 to E13 (10)
2 Decide and adopt	weeks 3 to 5	E14 to E23 (10)
3 Configure	weeks 6 to 9	E24 to E50 (27)
4 Operations	ongoing	E51 to E60 (10)

05

Zones and environments

The environment strategy is the foundation: It defines where each solution is built and which rules apply there.

Zones instead of individual cases. Microsoft recommends organizing environments into zones and mapping each zone to an environment group with rules. The kit proposes three zones: Zone 1 for personal productivity, Zone 2 for teams and departments, Zone 3 for business-critical solutions. In addition, there are special environments, e.g. for SharePoint forms. The risk assessment determines which solution belongs in which zone.

The default environment. Every tenant has exactly one, all employees have access to it, and it can be neither turned off nor replaced. Microsoft recommends treating it as a space for personal productivity: Rename it, apply a strict data policy, limit sharing, and use routing to direct makers to their own environments. Important solutions move to Zone 2 or 3.

Personal developer environments. From November 15, 2026, only managed developer environments are created, at most one per person. Environment routing creates them automatically when a person opens Power Automate, Power Apps, or Copilot Studio, and assigns them to an environment group. Building and previewing do not require a Premium license, but running does. Personal developer environments are disabled after 60 days without activity and deleted 15 days later.

Managed Environments. They provide practical governance controls, including sharing limits, usage insights, environment group rules, solution checker enforcement, and maker welcome content. Each use requires an appropriate licensing model. Depending on the scenario, this may be a Premium license, qualifying Dynamics 365 rights, per-app or per-flow plans assigned to the environment, or pay-as-you-go billing. This makes W03 an important decision. Before enabling Managed Environments, download the licensing report from the admin center.

Environment groups and rules. A group combines Managed Environments with Dataverse, and each environment belongs to exactly one group. Published rules apply in all environments of the group and cannot be turned off there. Caution: When you add an environment, the rules overwrite its existing settings, e.g. custom welcome content for makers.

> **Environment group rules (selection)**
>
> Sharing of canvas apps, flows, and agents, solution checker, welcome content for makers, usage insights, backup retention, generative AI, knowledge sources and external models for agents, access to conversation transcripts, advanced connector policies, unmanaged customizations, and the release channel. The full list of 28 rules is on Microsoft Learn under “Rules for environment groups.”

The zone model

	Zone 1: Personal	Zone 2: Team	Zone 3: Business-critical	Special environments
Purpose	Low-risk personal productivity in the default environment, developing and testing in personal developer environments. Sharing is allowed only within the limits of W06 and W07.	Solutions for a team or a department with manageable risk (risk class low or medium).	Business-critical solutions and solutions spanning several departments (risk class high).	Special purposes, e.g. SharePoint forms, a pilot for new AI features, an environment for child flows.
Environments	Default environment and personal developer environments through environment routing	One production environment per department, plus a sandbox for development if needed	Separate development, test, and production environments per solution or solution family	As needed
Managed Environments	Personal developer environments always, default environment according to decision point W03	According to decision point W03 (recommended: Yes)	Yes	Depending on purpose
Data policy	Strictly according to decision point W04: non-blockable connectors Business, all others Blocked or individually approved	Microsoft 365 connectors and approved standard connectors, others on request	Allowlist (advanced connector policies) according to decision point W05, custom connectors only on request	Depending on purpose
Sharing	Very restricted (decision points W06 and W07)	With the security group of the department	As needed, documented	Depending on purpose
Requirements	Low-risk solutions only. Anything a team needs or a business process depends on belongs in Zone 2 or 3. Developer environments are for development and testing only.	Owner and deputy, inventory, review according to risk class.	Same as Zone 2, plus production only through solutions, service accounts according to decision point W13, documentation, short review intervals.	Purpose and owners in the environment plan.