Governance Zones in Copilot Studio

Build the same agent across three governance zones (Green, Yellow, Red) to experience firsthand how DLP policies and environment settings control knowledge access in Microsoft Copilot Studio.

🧭 Lab Details

Level	Persona	Duration	Purpose
300	Maker / Admin	30 minutes	After completing this lab, participants will be able to explain the differences between Green, Yellow, and Red governance zones, understand how DLP policies restrict knowledge sources, build agents that comply with organizational governance requirements, and evaluate the trade-offs between access and control across environments.

📚 Table of Contents

🤔 Why This Matters

Makers and admins — Ever built a great agent only to discover that a key knowledge source is blocked by your organization's policies? Or deployed an agent to a permissive environment and realized it returned unreliable results?

Think of governance zones like traffic lights: - **Without governance awareness**: You build agents that fail silently because blocked knowledge sources produce no results, or you build in wide-open environments that lack quality control. - **With governance awareness**: You choose the right environment for the right use case, set proper expectations with stakeholders, and design agents that thrive within policy boundaries.

Common challenges solved by this lab: - "Why can't my agent access this website in production?" - "I built my agent in a developer environment and it broke when I moved it to the corporate environment." - "How do I get the best of both worlds — full access and governed quality?" - "What is the actual difference between our dev, staging, and production environments for Copilot Studio?"

In 30 minutes, you will build the same agent three times and see exactly how governance changes behavior — so you never get surprised in production again.

🌐 Introduction

Organizations adopt governance zones to balance innovation speed with data security. In Microsoft Copilot Studio, Data Loss Prevention (DLP) policies control which connectors and knowledge sources an agent can use. These policies are applied at the environment level, meaning the same agent definition can behave very differently depending on where it is deployed.

Real-world example: A consulting firm creates a “Best Practices Advisor” agent for their consultants. In the personal productivity environment (Green), the agent can only reference internal SharePoint documents. In a project environment (Yellow), it can also pull from Microsoft Learn. In the development sandbox (Red), it has full access to public websites and an MCP server with curated best practices. The governance team uses this tiered approach to protect client data while giving developers room to innovate.

By completing this lab, you will build hands-on intuition for how governance zones affect agent behavior, so you can design agents that work reliably within your organization’s policies.

🎓 Core Concepts Overview

Concept	Why it matters
Governance Zones (Green / Yellow / Red)	Organizations tier environments by risk level. Understanding the tier your environment belongs to determines which knowledge sources and connectors your agent can use.
Data Loss Prevention (DLP) Policies	DLP policies are the enforcement mechanism behind governance zones. They block or allow specific connectors at the environment level, and their effects are only visible at runtime — not during design.
Knowledge Sources	Copilot Studio agents can draw from SharePoint, public websites, files, Dataverse, and more. DLP policies control which of these are available in each environment.
MCP (Model Context Protocol) Servers	MCP servers provide curated, structured, and governed knowledge that can be added as a tool. In permissive environments, MCP offers quality control that open web access alone does not.
Environment Selection	Choosing the right Power Platform environment is the first and most impactful decision when building an agent. It determines your governance boundaries for the entire project.

📄 Documentation and Additional Training

Links

- Data loss prevention policies in Power Platform (https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention)
- Environments overview in Power Platform (https://learn.microsoft.com/en-us/power-platform/admin/environments-overview)
- Knowledge sources in Microsoft Copilot Studio (https://learn.microsoft.com/en-us/microsoft-copilot-studio/knowledge-copilot-studio)
- Model Context Protocol (MCP) in Copilot Studio (https://learn.microsoft.com/en-us/microsoft-copilot-studio/agent-mcp-overview)

✅ Prerequisites

- Access to Microsoft Copilot Studio (https://copilotstudio.microsoft.com).
- Access to the **Bootcamp Green**, **Bootcamp Yellow**, and **Bootcamp Red** environments (pre-provisioned by the facilitator).
- A SharePoint link provided by the facilitator containing the Microsoft Copilot Studio Implementation Guide.
- A list of public website URLs provided by the facilitator for the Red zone exercise.
- A solution pre-created in each environment for your bootcamp session.

🎯 Summary of Targets

In this lab, you'll build the same Copilot Studio agent across three governance zones to compare their behavior side by side. By the end of the lab, you will:

- Create an agent in the Green zone restricted to SharePoint-only knowledge.

- Observe DLP enforcement blocking public website knowledge in a restricted environment.
- Create an agent in the Yellow zone with access to approved Microsoft domains.
- Create an agent in the Red zone with full public website access.
- Explore an MCP server as a governed knowledge tool in a permissive environment.
- Understand the governance trade-offs between safety, capability, and quality control.

🧩 Use Cases Covered

Step	Use Case	Value added	Effort
1	Green and Yellow Zones — DLP-Restricted Agents	Experience how DLP policies progressively restrict or allow knowledge sources across environments	25 min
2	Red Zone — Full Access and MCP Integration	Build an agent with full web access and explore MCP as a governed knowledge layer	20 min

🛠️ Instructions by Use Case

🧱 Use Case #1: Green and Yellow Zones — DLP-Restricted Agents

Build agents in the Green and Yellow governance zones to see how DLP policies progressively allow or block knowledge sources.

Use case	Value added	Estimated effort
Green and Yellow Zones — DLP-Restricted Agents	Experience how DLP policies progressively restrict or allow knowledge sources across environments	25 minutes

Summary of tasks

In this section, you'll learn how to create an agent in a SharePoint-only environment, observe DLP blocking a public website, and then repeat the process in a Yellow zone where approved Microsoft domains are allowed.

Scenario: Your organization has a personal productivity environment (Green) where makers can safely experiment with SharePoint-grounded agents, and a project environment (Yellow) that adds access to official Microsoft documentation. You need to understand the boundaries of each before choosing where to build your production agent.

Objective

Create a “Copilot Studio Advisor” agent in both the Green and Yellow zones, test knowledge source access in each, and observe DLP enforcement in action.

Step-by-step instructions

Part 1: Green Zone (SharePoint Knowledge Only)

1. Go to https://copilotstudio.microsoft.com (https://copilotstudio.microsoft.com).
2. Select the **Environment selector** in the top-right corner of the screen.
3. Search for `Bootcamp Green` and select it.
4. In the **“What would you like to build?”** pane, find the text area that says *“Start building by describing what your agent needs to do”*.
5. Copy and paste the following text into the description field:

```
Help me build an agent that knows everything about building agents in Power Platform Copilot Studio. You're an expert, you're a coach, you give proactive advice on how to build Copilot Studio agents. And your knowledge is built on top of a SharePoint document.
```

6. After typing the description, add the **SharePoint link** that was shared with you by the facilitator.
7. At the end of your instructions, add the following text:

```
Please name this agent Copilot Studio Advisor [YourUsername]
```

> ℹ️
> **Note:** We add the username so we can find your agent easily in this shared environment.

8. Before clicking the blue arrow to create, select the **Settings** wheel icon in the bottom-left corner.
9. In the Settings pane, make sure you select the **Solution** that was created at the start of this bootcamp.
10. Optionally, give your agent a custom **Schema Name**.

> 💡
> **Tip:** Schema names are used for advanced management of your agents. We advise using schema names in collaboration with the description. For example: `mcs_build_advisor_[YourUsername]_green`. Include the zone name (green, yellow, red) so you can tell them apart later.

11. Click the **blue arrow** on the right-hand side to submit and create your agent.
12. Wait for Copilot Studio to build your agent. It will generate your name, description, and auto-generated instructions.
13. Scroll down and notice that Copilot Studio has added suggested knowledge sources such as training hands-on labs, PowerPoint decks, and other capabilities.

Add SharePoint Knowledge

14. In this Green zone, DLP policies restrict knowledge to **SharePoint only**.
15. Select the **Knowledge** tab.
16. Click **Add knowledge**.

17. Select **SharePoint**.
18. Paste in the SharePoint link provided by the facilitator.
19. Click **Add**.
20. Check the name of the knowledge source. It should reference the Microsoft Copilot Studio Implementation Guide PPTX.
21. Review the description.

> ℹ️
> **Note:** The default name and description are fine for now. However, we encourage you to be more descriptive with naming and descriptions. The knowledge you add and how you describe it will be discussed in best practices. Good descriptions help the orchestrator understand what the knowledge is used for.

22. Click **Add to agent**.
23. Verify that the added knowledge source shows a **green check mark**, meaning it is ready.

Test the Green Zone Agent

24. In the **Test** pane on the right-hand side, type the following prompt:

```
Please give me some best practices on Copilot Studio
```

25. Press **Enter** or click **Send**.
26. On the left-hand side, notice that the agent is reviewing knowledge from the SharePoint source you added.
27. Review the response. It will give you best practices found in the Implementation Guide.

28. Notice the **citations** in the response. You can click on them and they will hyperlink you to the specific location inside the PowerPoint document.
29. Scroll down to the **References** section. Notice that it only references the Copilot Studio Implementation Guide and nothing else. This is because the Green zone restricts knowledge to SharePoint only.

Attempt to Add a Public Website (Will Be Blocked)

30. Go back to the **Knowledge** tab.
31. Click **Add knowledge**.
32. Select **Public websites**.
33. Enter the following URL:

```
learn.microsoft.com
```

34. Click **Add**.
35. Review the name and description.

> ℹ️
> **Note:** Again, the defaults are fine for now, but do improve these for production agents.

36. Click **Add to agent**.
37. After a couple of seconds, you will see two knowledge sources listed: one SharePoint, one Public Web.
38. Notice that `learn.microsoft.com` shows a status of **Not Allowed**.

⚠️

IMPORTANT: The status message will say something like *“Not allowed due to your organizational data loss prevention policies. Contact your admin.”* This is the DLP policy in action, blocking public website knowledge in the Green zone.

Part 2: Yellow Zone (Microsoft Learn Allowed)

ℹ️

Note: In a real organization, you would need to go through your company’s approval process to get access to a Yellow zone environment. For this bootcamp we have pre-provisioned access.

39. Click the **Environment selector** in the top-right corner.
40. Search for and select `Bootcamp Yellow`.
41. In the **“What would you like to build?”** pane, copy and paste the following text:

```
Help me build an agent that knows everything about building agents in Power Platform Copilot Studio. You're an expert, you're a coach, you give proactive advice on how to build Copilot Studio agents. And your knowledge is built on top of learn.microsoft.com as a public website.
```

42. Before clicking the blue arrow, select the **Settings** wheel icon again.
43. Double-check that the correct **Solution** is selected.
44. Give your agent a schema name similar to the Green zone but with `yellow` in it.

> 💡
> **Tip:** For example: `mcs_build_advisor_[YourUsername]_yellow`. Keeping a consistent naming pattern across zones helps you stay organized.

45. Click the **blue arrow** to create the agent in the Bootcamp Yellow environment.
46. Wait for the agent to be created. Your screen will say *“Getting things ready”*.
47. Once ready, verify that the agent has your name, description, and auto-generated instructions.
48. Scroll down and notice the knowledge suggestions again. You can add a couple that make sense for you.

Add Public Website Knowledge (Microsoft Learn)

49. Click **Add knowledge**.
50. Select **Public websites**.
51. Enter the following URL:

```
learn.microsoft.com
```

52. Click **Add**.
53. Review the name and description.

> ℹ️
> **Note:** This is fine for now. However, do make sure you create names and descriptions so the orchestrator can fully understand what this knowledge is used for.

54. Click **Add to agent**.

55. Notice that the knowledge source shows up with a **green Ready** status.

> ℹ️
> **Note:** The Yellow zone allows public websites from Microsoft domains. This is why `learn.microsoft.com` works here but was blocked in the Green zone.

Test the Yellow Zone Agent

56. In the **Test** pane, enter the same prompt used in the Green zone:

```
Please give me some best practices on Copilot Studio
```

57. Click **Send**.

58. Watch the right-hand side of the test pane. It shows the agent searching `learn.microsoft.com` for information.

59. Review the response. It will give you best practices pulled from Microsoft Learn documentation.

60. Scroll to the bottom and check the **References** section. You should see multiple references, all with URLs starting with `learn.microsoft.com`.

> ℹ️
> **Note:** Your results may vary, but all references should come from `learn.microsoft.com`.

Attempt to Add a Non-Microsoft Website (Will Be Blocked)

61. Select the **Knowledge** tab.

62. Click **Add knowledge**.
63. Select **Public websites**.
64. Enter the following URL:

```
microsoft.github.io/mcs-cat-blog
```

65. Click **Add**.
66. Review the name and description as before.
67. Click **Add to agent**.
68. Notice that the blog shows up as **Blocked**.

> ⚠️
> **IMPORTANT:** The Yellow zone only allows public knowledge from websites on the `microsoft.com` domain. The blog at `microsoft.github.io` is not on the `microsoft.com` domain, so it is blocked by the DLP policy.

🏅 Congratulations! You've completed Use Case #1!

Test your understanding

Key takeaways:

- **Green zone = SharePoint only** — DLP policies block all public website knowledge sources. This is the safest environment for personal productivity agents grounded in internal documents.

- **Yellow zone = Approved domains** — DLP policies allow public websites from specific approved domains (e.g., `microsoft.com`). Non-approved domains are still blocked.
- **DLP enforcement is silent at design time** — You can add any knowledge source in the UI, but blocked sources show “Not Allowed” status only after you attempt to add them.

Lessons learned & troubleshooting tips:

- If a knowledge source shows “Not Allowed”, check your environment’s DLP policies — do not assume the feature is broken.
- Always name and describe your knowledge sources clearly. The orchestrator uses these to decide which source to query.
- Use consistent schema naming across zones (e.g., `_green`, `_yellow`, `_red`) to keep your agents organized in shared environments.

Challenge: Apply this to your own use case

- Which governance zone does your organization’s default Copilot Studio environment belong to?
- What knowledge sources does your team’s agent need — and are they available in your assigned environment?
- If you needed to request access to a higher zone, what business case would you make?

🔄 Use Case #2: Red Zone — Full Access and MCP Integration

Build an agent in the Red zone with unrestricted public website access, then explore how an MCP server adds governed quality on top of open access.

Use case	Value added	Estimated effort
Red Zone — Full Access and MCP Integration	Build an agent with full web access and explore MCP as a governed knowledge layer	20 minutes

Summary of tasks

In this section, you'll learn how to create an agent with multiple public website knowledge sources in the Red zone and explore an MCP server as a curated knowledge tool.

Scenario: Your development team has been granted access to a Red zone sandbox for prototyping. You want to build the most capable version of your Copilot Studio Advisor agent — one that can pull from community blogs, GitHub documentation, and official Microsoft Learn content. You also want to evaluate whether an MCP server can provide higher-quality answers than open web search alone.

Objective

Create a "Copilot Studio Advisor" agent in the Red zone with full public website access, verify unrestricted knowledge source behavior, and explore the MCP server as a governed knowledge tool.

Step-by-step instructions

Create the Red Zone Agent

1. Click the **Environment selector** in the top-right corner.
2. Search for and select `Bootcamp Red`.
3. In the **"What would you like to build?"** pane, copy and paste the following text:

```
Help me build an agent that knows everything about building agents in Power Platform Copilot Studio. You're an expert, you're a coach, you give proactive advice on how to build Copilot Studio agents. And your knowledge is built on top of the following sources:
```

> ℹ️
> **Note:** After the text above, add the list of public website URLs provided by the facilitator. These are useful sources for building Copilot Studio agents — and great bookmarks for your own reference.

4. Select the **Settings** wheel icon.
5. Double-check your **Solution**.
6. Give your agent a schema name with `red` in it, following the same pattern as before.

> 💡
> **Tip:** For example: `mcs_build_advisor_[YourUsername]_red`

7. Click the **blue arrow** to create the agent.
8. Wait for the agent to be created.
9. Once ready, verify your agent has the correct name, description, and instructions.
10. Scroll down. You should see that the URLs you provided in the prompt have been added as suggestions.

Add Public Website Knowledge

11. In the suggestions pane, click **Add** next to the suggested knowledge sources.
12. For each suggestion, it will show the link to the website. Click **Add**.
13. Review the name and description for each source.

> 💡
> **Tip:** As always, make sure that names and descriptions are useful. The orchestrator uses these to decide which knowledge source to query.

14. Click **Add to agent** for each source.
15. Repeat this process for each public website you want to add as knowledge.

Test the Red Zone Agent

16. In the **Test** pane, enter the same test prompt:

```
Please give me some best practices on Copilot Studio
```

17. Click **Send**.
18. Watch the right-hand side. It shows the agent searching across **multiple public websites**.
19. Review the response. It should provide best practices pulled from a variety of sources.
20. Check the **References** section at the bottom. You should see citations from **multiple different websites**.

> ℹ️
> **Note:** The Red zone allows all public websites. Your agent now has access to community content, blogs, and other sources beyond just Microsoft Learn.

Bonus: Add and Explore the MCP Server

> ℹ️
> **Note:** This section is for those who finish early. There are no detailed step-by-step instructions for this part, but here is what you need to know.

21. Inside the Bootcamp Red environment, an MCP server has been pre-configured.
22. The MCP server name is:

    ```
    MCS Best Practice MCP
    ```

23. When creating a connection, it will ask for an access key. Use the following:

    ```
    mcs-demo-key
    ```

24. Add the MCP server as a **tool** and explore the available capabilities.
25. Try asking your agent questions and see how it uses the MCP tools to provide structured, curated answers.

> 💡
> **Tip:** MCP is not just “more access.” It provides curated, searchable, governed knowledge that beats random internet searches. Structured queries, copy-paste ready code snippets, and step-by-step troubleshooting guides are what make MCP powerful.

🏅 Congratulations! You’ve completed Use Case #2!

Test your understanding

Key takeaways:

- **Red zone = Full access** — All public websites are allowed as knowledge sources. This gives maximum capability but reduces quality control over what the agent returns.
- **MCP adds governance to openness** — An MCP server provides curated, structured knowledge that delivers higher-quality answers than unrestricted web search alone.
- **More access means more responsibility** — In a Red zone, you must validate agent responses more carefully since they may come from unvetted sources.

Lessons learned & troubleshooting tips:

- In the Red zone, verify that your agent’s references come from trustworthy sources before promoting it to production.
- MCP servers offer structured queries and curated content that open web knowledge cannot match — consider MCP for production agents in permissive environments.

- Always run evaluations before deploying any agent to production, regardless of governance zone.

Challenge: Apply this to your own use case

- What public websites would provide the most value as knowledge sources for your agent?
- Would an MCP server benefit your use case? What structured knowledge would you want it to provide?
- How would you design a promotion path for your agent from Red (prototype) to Green (production)?

🏆 Summary of learnings

True learning comes from doing, questioning, and reflecting — so let's put your skills to the test.

To maximize the impact of governance-aware agent design:

- **Choose the right zone for the right purpose** — Green for safe personal productivity, Yellow for approved external sources, Red for prototyping and innovation.
- **DLP policies are invisible until they block you** — Always verify knowledge source availability in your target environment early in your design process.
- **Naming conventions matter at scale** — Consistent schema names and descriptive knowledge source labels make agents manageable across environments and teams.
- **MCP bridges the gap between access and quality** — In permissive environments, MCP servers provide the governance layer that open web access lacks.
- **Never skip evaluations** — Even changing one word in an agent's instructions can change its behavior. Treat evaluations as your user acceptance test before any production deployment.

Conclusions and recommendations

Governance zones golden rules:

- Always check your environment’s DLP policies before designing an agent’s knowledge architecture.
- Use the Green zone for internal-only agents grounded in SharePoint and Dataverse.
- Use the Yellow zone when you need official Microsoft documentation alongside internal sources.
- Use the Red zone for prototyping and innovation — but never promote a Red zone agent to production without evaluations.
- Adopt MCP servers in permissive environments to add structured, curated knowledge that scales better than bookmarking public websites.
- Document your agent’s governance zone requirements so that deployment across environments is predictable and repeatable.

By following these principles, you’ll build agents that work reliably within your organization’s governance framework — delivering innovation where it’s needed without compromising security or quality.