# FSI Agent Governance Framework: Comprehensive Validation and Enhancement Report

## Executive Summary

This comprehensive research report provides a rigorous validation and enhancement analysis of the **FSI Agent Governance Framework (Beta v1.0, December 2025)**. Commissioned to ensure alignment with the latest **Microsoft Learn** documentation and the specific, stringent regulatory requirements of the United States **Financial Services Industry (FSI)**, this document evaluates the framework's effectiveness in governing Microsoft 365 Copilot, Copilot Studio agents, and the underlying Power Platform infrastructure.

The analysis operates under the assumption of the current operational landscape as of **January 6, 2026**. This temporal context is critical, as it places the assessment in a technological environment where pivotal governance features—specifically **SharePoint Restricted Site Creation**, **Advanced Connector Policies (ACP)**, and **Microsoft Purview Data Security Posture Management (DSPM) for AI**—have transitioned from preview to General Availability (GA). These features are no longer optional "nice-to-haves" but fundamental components of a defensible compliance posture for institutions regulated by the **SEC**, **FINRA**, **OCC**, and **Federal Reserve**.

The findings indicate that while the Beta framework provides a robust conceptual architecture, it requires significant technical remediation to address the practical realities of the Microsoft platform. Foremost among these is the governance of the **Default Power Platform Environment**. The framework's current implication—that agent creation can be simply "disabled"—is technically inaccurate and presents a severe compliance risk. This report establishes that the "Environment Maker" role is indelible in the Default environment, necessitating a shift from a strategy of "Prevention" to one of "Sterile Containment" via Data Loss Prevention (DLP) blocking and Environment Routing. Furthermore, the report identifies critical terminology misalignments, such as the use of "Copilot Command Center" instead of the official **"Copilot Hub"**, and advocates for the elevation of **Restricted SharePoint Search (RSS)** as the primary "Zero Trust" control for high-risk data repositories.

The following sections detail the strategic architecture, validate specific controls across all four pillars, and provide granular, cited corrections to ensure the framework serves as an audit-ready artifact.

## 1. Strategic Architecture and Regulatory Alignment

The foundational architecture of any FSI governance framework must balance the imperative for innovation with the non-negotiable requirements of stability and supervision. The FSI Agent Governance Framework utilizes a three-zone model—**Personal**, **Team**, and **Enterprise**—which aligns conceptually with the "Safety Tiers" approach found in **Model Risk Management (MRM)** guidance (OCC 2011-12 / SR 11-7). However, the technical implementation of these zones, particularly regarding the environment strategy, requires deeper scrutiny to ensure it withstands regulatory examination.

### 1.1 The "Default Environment" Conundrum: From Prevention to Containment

A primary focus of this validation is the governance of the "Default" Power Platform environment. In most Microsoft 365 tenants, this environment serves as the catch-all for personal productivity. In an FSI context, however, the Default environment represents a significant "Shadow AI" vulnerability. The core issue lies in the permissions model: every user in the tenant is automatically assigned the "Environment Maker" role in the Default environment, and this role cannot be removed.1

The current iteration of the FSI Agent Governance Framework implies that administrators can simply "disable agent creation" in this environment. Extensive review of Microsoft documentation refutes this capability. Microsoft explicitly states: *"You can't disable agent creation. Our guidance is to use data policies to disable anyone from chatting with that agent"*.3 This technical constraint fundamentally alters the governance strategy. If a policy states "We prevent creation" but the technical reality allows creation (even if unpublished), the control design is deficient and effectively indefensible during a compliance audit.

Consequently, the framework must be updated to prescribe a **"Sterile Containment Strategy."** Since preventing the *act* of creation is impossible via native toggles, the governance controls must prevent the *utility* of any created agent. This involves a multi-layered defense:

1. **Rendering Agents Impotent via DLP:** Administrators must configure a Data Loss Prevention (DLP) policy scoped exclusively to the Default environment that blocks all publication channels. By blocking the **"Chat with Agent"**, **"Microsoft Teams"**, **"Direct Line"**, and **"Facebook"** channels, any agent created in the Default environment remains trapped in a "test" state, accessible only to its creator and unable to interact with other users.5
2. **Severing Distribution Mechanisms:** The strategy must further degrade the utility of the Default environment by disabling sharing capabilities. Using the Set-TenantSettings PowerShell cmdlet to set $settings.powerPlatform.powerApps.disableShareWithEveryone = $true ensures that makers cannot circumvent publication blocks by simply sharing the raw agent file with the entire organization.6
3. **Evacuation via Environment Routing:** The most effective long-term control is to ensure users never land in the Default environment in the first place. **Environment Routing** features allow administrators to automatically redirect makers to their own personal **Developer Environments** when they attempt to access Copilot Studio.7 This feature routes the traffic of creation away from the shared Default environment into isolated, governable sandboxes.

### 1.2 Regulatory Implications of Environment Strategy

Financial regulators enforce a "Books and Records" regime that extends beyond financial transactions to include electronic communications and the supervisory systems used to manage them (SEC Rule 17a-4, FINRA Rule 3110). The configuration of the Power Platform environment strategy is itself a supervisory record.

If an FSI organization claims that "Personal Productivity" agents (Zone 1) are low risk because they cannot access sensitive data, they must be able to prove this technically. The Default environment, often cluttered with legacy connections and broad permissions, makes this proof difficult. By mandating **Environment Routing**, the framework ensures that Zone 1 agents are created in **Developer Environments** where the organization can apply a standard, restrictive DLP policy (e.g., blocking SQL connectors, allowing only Office 365 connectors). This segregation of duties—keeping "Personal" play in sandboxes and "Enterprise" work in Managed Environments—provides the clear delineation required to satisfy the "separation of functions" principles inherent in **SOX 404** internal control requirements.

Furthermore, the audit trail for agents created in these personal environments must be preserved. While the agent may be "personal," if it interacts with corporate data, its logs are subject to retention. The framework must emphasize that **Control 1.7 (Audit Logging)** applies universally, and that the organization's **Microsoft Purview** retention policies must cover the **Dataverse** capacity associated with these personal developer environments, ensuring that conversation transcripts are not lost if a user leaves the firm.8

### 1.3 The Role of Managed Environments

The framework correctly identifies **Control 2.1 (Managed Environments)** as a key component, but it must be explicit about *why* this is critical for FSI. Managed Environments provide the "Usage Insights" and "Sharing Limits" that transform a chaotic collection of apps into a governed fleet. For FSI customers, the ability to limit sharing to a specific security group (or block it entirely) is vital for preventing the viral spread of an unverified agent that might contain hallucination risks or outdated financial models.9

The analysis confirms that Environment Routing creates *Managed* Developer Environments by default.7 This is a significant advantage, as it ensures that even personal sandboxes come equipped with the governance "sidecars" necessary for admin oversight. The framework should update Control 2.15 (Environment Routing) to highlight this synergy: routing is not just about placement; it is about automatically applying a "Managed" governance tier to every new maker in the organization.

## 2. Pillar 1: Security Controls – Detailed Validation

Pillar 1 focuses on the technical safeguards protecting data and systems. The 19 controls listed are comprehensive, yet several require updates to reflect the technical realities of 2026, particularly regarding Advanced Connector Policies and the rebranding of AI security tools.

### 2.1 Control 1.4: Advanced Connector Policies (ACP)

Control 1.4 is listed as "Advanced Connector Policies." The analysis validates that ACP has moved from a preview feature to a critical governance instrument, particularly for FSI organizations that require granular control over data flow. While standard DLP policies operate at the *connector* level (e.g., "Block SQL Server"), ACP allows for **action-level filtering** and **endpoint filtering**.10

In an FSI context, this distinction is profound. A "Customer Service Agent" might legitimately need to *read* a client's balance from a SQL database but should never have the permission to *update* or *delete* that balance. Standard DLP acts as a blunt instrument—allow or block. ACP allows the administrator to permit the GetRow action while explicitly blocking UpdateRow and DeleteRow.11 This enforces the "Principle of Least Privilege" at the API level, a requirement often cited in **GLBA** safeguards assessments.

Furthermore, ACP has evolved to support the **Model Context Protocol (MCP)**. MCP servers act as gateways for agents to connect with external tools and data sources. The ability to block specific **MCP Servers** via ACP ensures that agents cannot surreptitiously "phone home" to unauthorized third-party AI services or data processors.10 The framework must update Control 1.4 to explicitly mention **MCP Server Blocking** and **Action-Level Filtering** as mandatory configurations for Zone 3 (Enterprise) agents.

### 2.2 Control 1.6: Microsoft Purview Data Security Posture Management (DSPM) for AI

The framework currently references "Microsoft Purview: DSPM for AI" or occasionally "AI Hub." It is critical to standardize this terminology. The feature formally known as "Microsoft Purview AI Hub" was rebranded to **"Data Security Posture Management (DSPM) for AI"** in mid-2025.13

Beyond the name change, the functional scope of this control must be expanded in the documentation. DSPM for AI is not merely a reporting tool; it is a proactive defense mechanism. It utilizes "Adaptive Protection" to dynamically adjust DLP policies based on the risk level of the user interacting with the AI.15 For example, if a trader is flagged as a "high insider risk" due to resignation behavior, DSPM for AI can automatically restrict their ability to paste sensitive data into Copilot, even if that action was previously allowed.

FSI organizations must leverage the **"Detect sensitive info added to AI sites"** policy.15 This policy specifically monitors for the pasting of Sensitive Information Types (SITs)—such as credit card numbers, SWIFT codes, or ABA routing numbers—into generative AI prompts. This visibility is essential for **GLBA 501(b)** compliance, which requires financial institutions to protect against unauthorized access to customer information. The framework should update Control 1.6 to mandate the activation of these specific SIT detection policies.

### 2.3 Control 1.8: Runtime Protection and External Threat Detection

The framework lists "Runtime Protection" as a control. Validation against current Microsoft capabilities confirms that **Microsoft Defender** now offers **real-time protection** for Copilot Studio agents.16 This capability is distinct from static analysis; it monitors the agent's behavior *during execution*.

For FSI, the threat landscape includes adversarial attacks such as **Prompt Injection** (tricking the AI into ignoring instructions) and **Jailbreaking** (bypassing safety filters). Defender's runtime protection monitors tool invocation calls and blocks suspicious sequences *before* they are executed.17 This is analogous to an Endpoint Detection and Response (EDR) system but for AI logic. The framework must elevate this control to "Mandatory" for all external-facing (Zone 3) agents, as these are exposed to the public internet and represent the highest risk surface for reputational damage and data exfiltration.

### 2.4 Control 1.1: Restrict Agent Publishing

Control 1.1 focuses on restricting who can publish agents. While DLP policies can block channels, a more definitive control exists at the tenant level. The framework should incorporate the use of the PowerShell cmdlet Set-PowerAppDlpErrorSettings and associated publishing block commands to enforce a hard ban on publishing in specific environments.18

Relying solely on "soft" controls (like user training or UI warnings) is insufficient for FSI standards. The "Block agent publishing" feature allows administrators to technically prevent the "Publish" button from functioning in the Default environment, providing a definitive control that can be evidenced to auditors. This aligns with the "Safety by Design" principles advocated in the **NIST AI Risk Management Framework**.

## 3. Pillar 2: Management Controls – Operationalizing Governance

Pillar 2 governs the lifecycle of the agent. The analysis identifies that the most significant gap in the current framework is the lack of a cohesive strategy for the Default environment, as discussed in Section 1.1. Additionally, the operational controls for **Environment Routing** and **Model Risk Management** require refinement.

### 3.1 Control 2.15: Environment Routing and Auto-Provisioning

Environment Routing is the linchpin of the "Sterile Default" strategy. It functions by intercepting the user's intent to "make" and redirecting it to a safe location. The framework must clarify the nuances of this control:

* **Scope:** Routing applies to *new* makers. Users who have already created artifacts in the Default environment may not be automatically rerouted unless the administrator explicitly configures the routing rule to target "All Makers" effectively.7
* **Target Group:** The routing rule must target a specific **Environment Group** (e.g., "Personal Productivity").7 This allows the administrator to pre-configure that group with restrictive DLP policies (Control 1.5) and Sharing Limits (Control 2.1) so that every new environment born into that group is secure by default.
* **Documentation:** The framework should direct administrators to the **Power Platform Admin Center (PPAC)** > **Tenant Settings** > **Environment Routing** blade for configuration.7

### 3.2 Control 2.6: Model Risk Management (MRM)

FSI regulators (specifically the Fed and OCC under **SR 11-7**) expect organizations to maintain an inventory of all models, including AI agents. The framework currently treats MRM as a set of qualitative policies. It must be updated to link Control 2.6 directly to **Control 3.1 (Inventory)**.

The **Agent Inventory** in the Power Platform Admin Center provides the technical baseline for this MRM inventory.19 It lists every custom agent, its creator, its environment, and its authentication status. FSI organizations should be advised to export this inventory regularly and reconcile it with their GRC (Governance, Risk, and Compliance) systems to ensure that every "Model" (Agent) active in the environment has a corresponding risk assessment on file. An agent that exists in the technical inventory but lacks a risk assessment in the GRC system represents a "Model Risk" gap that must be remediated.

## 4. Pillar 3: Reporting Controls – Accurate Terminology and Visibility

Pillar 3 ensures visibility and accountability. The review identifies a critical terminology error that could confuse administrators, as well as a need to clarify the fragmented nature of agent inventories.

### 4.1 Control 3.8: Correction to "Copilot Hub"

The framework refers to Control 3.8 as "Copilot Command Center." While the term "Command Center" has appeared in some Office client release notes (e.g., for Mac) 20, the official feature name within the **Power Platform Admin Center (PPAC)**—where governance actually happens—is **"Copilot Hub"**.21

Using the correct terminology is vital for operational execution. An administrator searching for "Command Center" in the PPAC navigation menu will find nothing. The **Copilot Hub** is the centralized dashboard that provides insights into Copilot adoption, readiness, and governance settings. It allows admins to view the number of active agents, session success rates, and total sessions.21 The framework must update the control name to **"Copilot Hub and Usage Insights"** to align with the UI and Microsoft documentation.

### 4.2 Control 3.1: The Tale of Two Inventories

The framework's reference to "Agent Inventory" simplifies a complex reality. In 2026, administrators must monitor two distinct inventories to have a complete view of the "Universe of Agents":

1. **Agent Registry (Microsoft 365 Admin Center):** This registry tracks **Declarative Agents** and **M365 Copilot Plugins** that are integrated directly into the M365 ecosystem.24
2. **Agent Inventory (Power Platform Admin Center):** This inventory tracks **Copilot Studio Custom Agents** and their environment distribution.19

While Microsoft is moving toward a unified "Agent 365" view 26, the prudent approach for an FSI framework is to explicitly mandate the reconciliation of *both* sources. Relying on just one leaves a blind spot. For instance, a declarative agent built in VS Code and deployed to M365 might not appear in the Power Platform inventory but still poses a data leakage risk. The framework must require auditors to validate complete coverage by checking both registries.

### 4.3 Control 3.9: Microsoft Sentinel Integration

For FSI security operations centers (SOCs), visibility is paramount. The framework correctly identifies Sentinel integration but should specify the mechanics. The **"Microsoft Power Platform"** and **"Microsoft 365"** connectors for Sentinel are the pipelines for this data.28 Specifically, enabling the **"Audit Logs"** connector ensures that agent creation, modification, and deletion events are ingested into the SIEM (Security Information and Event Management) system. This allows for correlation rules, such as "Alert if a user in the 'High Risk' group creates a new agent in the 'Default' environment."

## 5. Pillar 4: SharePoint Advanced Management – The Knowledge Layer

Copilot's intelligence is derived from the data it can access, which primarily resides in SharePoint. Therefore, SharePoint governance is effectively AI governance. Pillar 4 requires significant expansion to distinguish between different access control methodologies and to incorporate the newly GA feature of **Restricted Site Creation**.

### 5.1 Control 4.1: The Distinction Between RCD and RSS

The framework discusses "Information Access Governance" but glosses over the critical distinction between **Restricted Content Discovery (RCD)** and **Restricted SharePoint Search (RSS)**. These are opposing control models:

* **Restricted Content Discovery (RCD):** This is a **"Block List"** (Negative Control). Administrators identify specific sensitive sites (e.g., "Project Falcon M&A") and flag them to be excluded from Copilot summaries and enterprise search.29 Users with direct links can still access the files, but the AI remains blind to them. This is useful for specific, known pockets of high-secrecy data.
* **Restricted SharePoint Search (RSS):** This is an **"Allow List"** (Positive Control). Administrators define a curated list of safe sites (e.g., "Official Policies," "Intranet"). Copilot is restricted to *only* looking at these sites (plus the user's own files).30

**FSI Recommendation:** For financial institutions operating under a "Zero Trust" model, **RSS** is often the superior starting point. It contains the risk of oversharing by default, allowing the organization to slowly expand the AI's scope as data classification matures. Control 4.1 must explicitly describe both options and recommend RSS for initial Zone 3 deployments.

### 5.2 Control 4.6 (New): Restricted Site Creation

The framework is missing a dedicated control for **Restricted Site Creation**, a feature of SharePoint Advanced Management (SAM) that reached General Availability in 2025.31

* **The Risk:** Agents often create or require knowledge sources. If every user can create a new SharePoint Team Site to host their agent's data, the organization faces "Site Sprawl," where data is scattered across thousands of unmanaged containers.
* **The Control:** Use the Set-SPORestrictedSiteCreation cmdlet to limit the ability to create new sites to a specific security group (e.g., "IT Support" or "Departmental Admins").31
* **Action:** Add **Control 4.6: Restricted Site Creation Policies** to the framework. This serves as a "dam" against the flood of unmanaged data repositories.

### 5.3 Control 4.7 (New): Restricted Access Control (RAC)

While Control 4.4 mentions "Guest Access," it misses the more powerful internal control: **Restricted Access Control (RAC)**.

* **The Capability:** RAC limits access to a SharePoint site to a specific security group *regardless* of individual sharing actions. Even if a site owner creates a "Share with Everyone" link, a user cannot access the site unless they are a member of the RAC security group.33
* **FSI Use Case:** This is the technical implementation of **"Ethical Walls"** or "Chinese Walls" required by regulation (e.g., separating Investment Banking from Equity Research). If an agent generates a report based on data in a Research site protected by RAC, a Banking employee will be unable to view that source data, preserving the regulatory barrier.
* **Action:** Add **Control 4.7: Restricted Access Control (RAC)** as the mechanism for enforcing ethical walls in the age of AI.

## 6. Consolidated Corrections and Additions Table

The following table summarizes the specific, actionable updates required for the GitHub repository documentation to align with this report's findings.

### Section: Getting Started / Overview

| **Current Content** | **Required Correction / Addition** | **Rationale & Citation** |
| --- | --- | --- |
| **Governance Zones** | **Update Zone 1 (Personal) Definition:** Explicitly state that Zone 1 agents must be routed to a **Developer Environment** via **Environment Routing**. Explicitly prohibit reliance on the **Default Environment** for any production or governed workload. | Aligns with the "Sterile Default" strategy and the inability to disable creation natively. 7 |
| **Pillars** | **Update Pillar 3 Description:** Change "Copilot Command Center" to **"Copilot Hub"**. | Aligns with the official naming convention in the Power Platform Admin Center. 21 |

### Section: Pillar 1 - Security Controls

| **Control ID** | **Required Correction / Addition** | **Rationale & Citation** |
| --- | --- | --- |
| **1.1 Agent Publishing** | **Add Implementation Step:** "Configure 'Block internal' and 'Block external' publishing via PowerShell cmdlet Set-PowerAppDlpErrorSettings to enforce a hard ban on agent publishing in restricted environments." | Provides a definitive "hard block" capability beyond the "soft" warnings of standard DLP. 18 |
| **1.4 Advanced Connector Policies** | **Expand Scope:** "Implement blocking of specific connector *actions* (e.g., Block 'Delete Row' while allowing 'Get Row') and blocking of unauthorized **MCP Servers**." | Standard DLP cannot filter actions or MCPs; this is critical for FSI "Least Privilege" access. 10 |
| **1.6 DSPM for AI** | **Rename Control:** Change "Microsoft Purview AI Hub" to **"Microsoft Purview Data Security Posture Management (DSPM) for AI"**. Add guidance to enable the "Detect sensitive info added to AI sites" policy. | Reflects the official product rebranding and leverages SIT detection for GLBA compliance. 13 |
| **1.8 Runtime Protection** | **Add Implementation Step:** "Enable **Microsoft Defender for Cloud** runtime protection to block prompt injections, jailbreaks, and malicious tool invocations in real-time." | Adds a dynamic defense layer essential for mitigating adversarial AI attacks. 16 |
| **1.19 eDiscovery** | **Clarify Retention Locations:** "Ensure retention policies cover **Exchange Online** (for user prompts) AND **Dataverse** (for agent conversation transcripts). Failure to retain Dataverse logs is a common compliance gap." | Ensures full compliance with SEC Rule 17a-4 recordkeeping requirements. 8 |

### Section: Pillar 2 - Management Controls

| **Control ID** | **Required Correction / Addition** | **Rationale & Citation** |
| --- | --- | --- |
| **2.1 Managed Environments** | **Add Requirement:** "Enforce 'Limit Sharing' settings in Managed Environments to exclude security groups and limit user sharing (e.g., max 2 users) for Personal/Developer environments." | Prevents the viral spread of unverified agents within personal spaces. 9 |
| **2.15 Environment Routing** | **Refine Guidance:** "Configure Environment Routing to target the 'All Makers' group, redirecting them to a designated 'Personal Productivity' Environment Group that is pre-configured with restrictive DLP policies." | Ensures that new makers are automatically captured and governed, avoiding the Default environment. 7 |
| **MISSING (New Control)** | **Add Control 2.16: Default Environment Lockdown.** "Implement a 'Sterile Containment' strategy: 1) DLP block on all publishing channels. 2) PowerShell disableShareWithEveryone. 3) PowerShell enableChatbotOnWebsiteCreation = $false for Power Pages." | Addresses the specific "Default Environment" vulnerability where creation cannot be disabled. 3 |

### Section: Pillar 3 - Reporting Controls

| **Control ID** | **Required Correction / Addition** | **Rationale & Citation** |
| --- | --- | --- |
| **3.1 Agent Inventory** | **Expand Scope:** "Reconcile the **Microsoft 365 Agent Registry** (Declarative Agents) with the **Power Platform Admin Center Agent Inventory** (Custom Agents) to ensure a complete view of the agent landscape." | Clarifies the two distinct inventory views admins must monitor for regulatory reporting. 24 |
| **3.8 Copilot Command Center** | **Rename Control:** **"Copilot Hub"**. Update description to "Centralized dashboard in PPAC for AI usage analytics, governance settings, and readiness." | Corrects the terminology to match the actual admin interface. 21 |

### Section: Pillar 4 - SharePoint Advanced Management

| **Control ID** | **Required Correction / Addition** | **Rationale & Citation** |
| --- | --- | --- |
| **4.1 IAG** | **Add Detail:** "Differentiate between **Restricted Content Discovery (RCD)** which is a 'Block List' and **Restricted SharePoint Search (RSS)** which is an 'Allow List'. Use RSS for high-security 'Zero Trust' zones." | Critical distinction for FSI data governance models. 29 |
| **MISSING (New Control)** | **Add Control 4.6: Restricted Site Creation.** "Configure Set-SPORestrictedSiteCreation to limit new site generation to specific IT and Governance security groups." | Prevents site sprawl and the creation of unmanaged data repositories by agents. 31 |
| **MISSING (New Control)** | **Add Control 4.7: Restricted Access Control (RAC).** "Apply RAC policies to high-risk sites to enforce ethical walls (e.g., Research vs. Banking) regardless of individual sharing links." | Provides technical enforcement for regulatory information barriers (MNPI). 34 |

## 7. Deep Dive Implementation Guide: The "Sterile Default" Strategy

Because the "Default Environment" presents a unique challenge where the "Environment Maker" role cannot be revoked, the framework must include a dedicated implementation guide for what this report terms the **"Sterile Default"** strategy. This approach accepts that while agents may be *born* in the Default environment, they must never be allowed to *leave* it.

**Implementation Steps:**

1. **Block Publishing Channels (DLP):**
   * **Action:** Create a DLP Policy named "Default Environment - Block All Publish".
   * **Scope:** Apply strictly to the "Default" environment.
   * **Configuration:** Move the **"Chat with Agent"**, **"Microsoft Teams"**, **"Direct Line"**, and **"Facebook"** connectors to the **Blocked** data group.
   * **Effect:** A user can build an agent, but the "Publish" action will fail or result in an agent that cannot be connected to any user interface. It remains a "brain in a jar," unable to communicate.5
2. **Restrict Sharing Capability:**
   * **Action:** Use PowerShell to disable the "Share with Everyone" feature.
   * **Command:** $settings.powerPlatform.powerApps.disableShareWithEveryone = $true via Set-TenantSettings.
   * **Effect:** Makers cannot broadcast their agents to the entire organization, severely limiting the "blast radius" of any unapproved agent.6
3. **Divert Traffic (Environment Routing):**
   * **Action:** Enable Environment Routing for "All Makers".
   * **Target:** A designated "Personal Productivity" Environment Group.
   * **Effect:** When a user clicks "Create Agent" in Copilot Studio, the platform automatically switches them out of the Default environment and into their personal developer environment. This drastically reduces the volume of accidental creation in Default by changing the path of least resistance.7
4. **Power Pages Prevention:**
   * **Action:** Disable automatic bot creation for Power Pages sites.
   * **Command:** enableChatbotOnWebsiteCreation = $false via Set-TenantSettings.
   * **Effect:** Prevents the "side-effect" creation of agents when users experiment with Power Pages in the Default environment.35
5. **Reactive Policing (Automated Cleanup):**
   * **Action:** Deploy the **Center of Excellence (CoE) Starter Kit** or a custom flow using the "Power Apps for Admins" connector.
   * **Logic:** Trigger on New Bot creation in the Default Environment -> Send Email to Owner ("Please use your Developer Environment") -> Remove Permissions / Delete Bot.
   * **Effect:** Provides education and enforcement for persistent offenders who bypass other controls.

## 8. Conclusion

The FSI Agent Governance Framework provides a necessary and solid foundation for compliance in an AI-driven era. However, the rapid evolution of the Microsoft platform—specifically the maturation of **Advanced Connector Policies**, the rebranding of **DSPM for AI**, and the introduction of **Restricted Site Creation**—requires the specific updates detailed in this report.

By adopting the **"Sterile Default"** strategy, correcting terminology to match the **"Copilot Hub"** reality, and distinguishing between the "Block List" nature of **RCD** and the "Allow List" nature of **RSS**, FSI organizations can move from a posture of "policy-based hope" to "technical enforcement." These updates ensure that the framework not only satisfies the theoretical requirements of regulations like **SEC 17a-4** and **FINRA 3110** but also survives the practical reality of a live, evolving Microsoft 365 tenant in 2026.

#### Works cited

1. Environment Maker Role on Default Environment : r/PowerApps - Reddit, accessed January 6, 2026, <https://www.reddit.com/r/PowerApps/comments/1m8ovqw/environment_maker_role_on_default_environment/>
2. Restricting Copilot Agent Creation in Copilot Studio : r/microsoft365 - Reddit, accessed January 6, 2026, <https://www.reddit.com/r/microsoft365/comments/1ll232n/restricting_copilot_agent_creation_in_copilot/>
3. Security FAQs for Copilot Studio - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-copilot-studio/security-faq>
4. accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-copilot-studio/security-faq#:~:text=You%20can't%20disable%20agent,from%20chatting%20with%20that%20agent.>
5. Configure data policies for agents - Microsoft Copilot Studio, accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-copilot-studio/admin-data-loss-prevention>
6. Secure the default environment - Power Platform | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/guidance/adoption/secure-default-environment>
7. Environment routing - Power Platform - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/admin/default-environment-routing>
8. Microsoft Copilot Studio implementation Guide | PDF - Scribd, accessed January 6, 2026, <https://www.scribd.com/document/944246790/Microsoft-Copilot-Studio-implementation-Guide>
9. Block and limit sharing for Copilot Studio | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/release-plan/2024wave2/power-platform-governance-administration/turn-sharing-off-copilot-studio>
10. Advanced connector policies (preview) - Power Platform - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/admin/advanced-connector-policies>
11. Announcing managed security enhancements for Microsoft Copilot Studio, accessed January 6, 2026, <https://www.microsoft.com/en-us/microsoft-copilot/blog/copilot-studio/announcing-managed-security-enhancements-for-microsoft-copilot-studio/>
12. Data policies - Power Platform | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention>
13. Learn about Data Security Posture Management for AI - (classic), accessed January 6, 2026, <https://learn.microsoft.com/en-us/purview/dspm-for-ai>
14. accessed January 6, 2026, <https://www.microsoft.com/releasecommunications/api/v2/m365/469509?&responseFormat=csv>
15. Considerations for deploying Microsoft Purview Data Security Posture Management (DSPM) for AI, accessed January 6, 2026, <https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations>
16. Protect Copilot Studio AI Agents in Real Time with Microsoft Defender, accessed January 6, 2026, <https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/protect-copilot-studio-ai-agents-in-real-time-with-microsoft-defender/4446560>
17. Strengthen agent security with real-time protection in Microsoft Copilot Studio, accessed January 6, 2026, <https://www.microsoft.com/en-us/microsoft-copilot/blog/copilot-studio/strengthen-agent-security-with-near-real-time-protection-in-microsoft-copilot-studio/>
18. Weekly digest: Office 365 changes – 23 to 27 June News #Office365 #421 - Nuno Árias Silva Website, accessed January 6, 2026, <https://www.nuno-silva.net/blog/post/13528/weekly-digest-office-365-changes-23-to-27-june-news-office365-421>
19. Monitor agents using Agent Inventory in Copilot Studio Kit - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-copilot-studio/guidance/kit-agent-inventory>
20. Release notes for Office for Mac - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/officeupdates/release-notes-office-for-mac>
21. Track, manage, and scale Copilot adoption in the Power Platform - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/admin/copilot/copilot-hub>
22. Announcing General Availability of Copilot hub in Power Platform Admin Center - Microsoft, accessed January 6, 2026, <https://www.microsoft.com/en-us/power-platform/blog/2024/12/02/announcing-general-availability-of-copilot-hub-in-power-platform-admin-center/>
23. Copilot hub for Power Pages (preview) - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-pages/admin/copilot-hub>
24. Agent Registry in the Microsoft 365 admin center, accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/agent-registry?view=o365-worldwide>
25. View agent inventory (preview) - Power Platform | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-platform/admin/tenant-wide-agent-inventory>
26. Security as the core primitive - Securing AI agents and apps | Microsoft Community Hub, accessed January 6, 2026, <https://techcommunity.microsoft.com/blog/microsoft-security-blog/security-as-the-core-primitive---securing-ai-agents-and-apps/4470197>
27. Microsoft Agent 365: The control plane for AI agents | Microsoft 365 Blog, accessed January 6, 2026, <https://www.microsoft.com/en-us/microsoft-365/blog/2025/11/18/microsoft-agent-365-the-control-plane-for-ai-agents/>
28. Audit Microsoft 365 Copilot Studio Agents & Graph Connectors Across Your Tenant - nBold, accessed January 6, 2026, <https://nboldapp.com/audit-microsoft-365-copilot-studio-agents-graph-connectors-across-your-tenant/>
29. Restrict discovery of SharePoint sites and content - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/sharepoint/restricted-content-discovery>
30. Restricted SharePoint Search - SharePoint in Microsoft 365 | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/sharepoint/restricted-sharepoint-search>
31. Restrict OneDrive and SharePoint site creation by users - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/sharepoint/restricted-site-creation>
32. What's new in Content Governance in SharePoint, OneDrive, and Teams for AI era, accessed January 6, 2026, <https://techcommunity.microsoft.com/blog/spblog/what%E2%80%99s-new-in-content-governance-in-sharepoint-onedrive-and-teams-for-ai-era/4411645>
33. SharePoint Advanced Management overview - SharePoint in Microsoft 365 | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/sharepoint/advanced-management>
34. Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups, accessed January 6, 2026, <https://learn.microsoft.com/en-us/sharepoint/restricted-access-control>
35. Manage agent provisioning | Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/power-pages/getting-started/manage-agent-provisioning>
36. Configure a policy for the channels used to publish agents - Microsoft Copilot Studio, accessed January 6, 2026, <https://learn.microsoft.com/en-us/microsoft-copilot-studio/dlp-example-6>
37. How to disable app sharing with everyone in default environment? - Microsoft Learn, accessed January 6, 2026, <https://learn.microsoft.com/en-us/answers/questions/1329815/how-to-disable-app-sharing-with-everyone-in-defaul>