



MSP OAuth Governance Blueprint
A vendor-agnostic playbook to turn OAuth
oversight into a recurring managed service for
Microsoft 365

A Vendor-Agnostic Playbook To Turn OAuth Oversight Into A Recurring Managed Service For Microsoft 365

Table of Contents

— MSP OAuth Governance Blueprint

Overview: Why OAuth Governance Now?	03
Outcomes & Audience	04
The 3-Tier Governance Framework	05
Workflow, Data Model, and Evidence Pack	06
Manual vs Faster with AppGuard360	07
Rollout Plan, Pricing & Next Steps	09

What Is the MSP OAuth Governance Blueprint?

The MSP OAuth Governance Blueprint is a vendor-agnostic playbook that helps MSP owners, vCIOs, and TAMs convert OAuth oversight into a recurring managed service for Microsoft 365 clients. It addresses blind consent grants, unverified publishers, scope creep, webhook sprawl, and expiring secrets, and defines a 3-tier framework (Visibility & Reporting; Governance & Attestation; Continuous Monitoring) with clear deliverables, SLAs, and measurable KPIs.





Outcomes and Who It's For

Faster Time to Control

MSPs implement a standardized discovery → review → approval workflow to rapidly identify and remediate risky OAuth apps and reduce exposure across tenants.

Audit-Ready Proof

An Evidence Pack consolidates inventory, owner attestations, rotation logs, and mappings to SOC 2 CC6.6 and ISO 27001 A.9 to simplify audits and compliance reporting.

Risk Transparency

A weighted risk scoring model surfaces high-risk apps, excessive scopes, expiring secrets, and webhook sprawl so teams can prioritize remediation with confidence.

Operational Discipline

Defined review cadences, SLAs, and alerting (e.g., 45/30/14/7-day secret notices) make governance continuous and measurable rather than a one-time effort.

Stakeholder Alignment

App owners provide attestations and justifications; vCIOs and TAMs use QBR-ready KPIs and dashboards to demonstrate security improvements to customers.

KPIs & SLAs

Measure risk reduction, time-to-approval, percentage of verified publishers, alert mean time to remediate (MTTR), and provide monthly assurance reports to demonstrate improvement.

Break the program into three progressive levels so clients get visibility first, enforceable governance next, and ongoing monitoring that prevents regression. Each tier includes specific outputs, service-level expectations, and KPIs aligned to compliance and risk reduction.

The 3-Tier Governance Framework

01

Intro: Structure your service into tiers with clear deliverables, SLAs, and KPIs.

Organize your MSP offering into an operational model that delivers repeatable oversight and measurable assurance for Microsoft 365 tenants.

02

Tier 1: Visibility & Reporting

Perform comprehensive inventory of apps, publishers, scopes, owners, webhooks, and secret expiration dates; produce standardized reports and a baseline risk register.

03

Tier 2: Governance & Attestation

Execute a discovery → review → approval workflow, capture owner justifications, apply the decision matrix to approve/reduce/decommission, and store attestation evidence.

04


Tier 3: Continuous Monitoring

Enforce periodic review cadences and proactive alerts (45/30/14/7-day secret notifications), continuous webhook and scope surveillance, and automated anomaly detection.

05

Evidence Pack — Audit-Ready Artifacts

Maintain an evidence pack containing inventory exports, high-risk item lists, owner attestations, rotation timelines, change logs, and mappings to SOC 2 CC6.6 and ISO 27001 A.9.



Manual vs Faster with AppGuard360

Capability	Manual	Scripts/PDFs	Basic Tenant Tools	AppGuard360
Multi-tenant monitoring	×	×	×	✓
Risk scoring rubric	×	△	×	✓
Branded client dashboards	×	×	×	✓
Export automation (Evidence Pack)	×	△	×	✓
Secret expiry alerts (45/30/14/7)	×	△	△	✓
Webhook and scope inventory	×	△	△	✓
Owner attestation workflow	×	×	×	✓

Case Study: 30/60/90 Rollout in Action

Scenario

An MSP needs to standardize OAuth governance across 18 Microsoft 365 tenants and demonstrate control during quarterly business reviews. They must inventory integrations, surface unverified publishers, and identify secrets nearing expiry.



Baseline discovery is completed across all tenants, flagging high-risk apps and connections, and capturing publisher verification and scope details for each integration.



The team implements the discovery → review → approval workflow, collects owner attestations, and applies the decision matrix to approve, reduce scopes, or decommission apps.



Alerting is enabled with 45/30/14/7-day secret warnings; excessive scopes are reduced and unused apps are decommissioned to shrink the attack surface.



An Evidence Pack is compiled for QBRs showing outcomes: a 38% weighted risk score reduction and 100% of expiring secrets rotated on schedule.

Advantages of Governance as a Service



Speed

Standardized discovery and approval workflows shorten time-to-approval and remediation.



Assurance

Audit-ready artifacts and an Evidence Pack simplify SOC 2 and ISO 27001 evidence requests.



Continuous Improvement

Monitoring, review cadences, and risk scoring drive measurable risk reduction over time.



Client Trust

Branded dashboards and QBR-ready reports make progress visible and reinforce recurring value.

Limitations to Plan For



Change Management

Application owners may delay attestations without clear SLAs and escalation paths.



Tool Coverage

Some integrations lack APIs or metadata; plan documented exceptions and manual checks.



Customization Boundaries & Data Quality

Scope reductions can affect app functionality and accurate owner tagging is essential for reliable KPIs.



Packaging and Pricing Options

Per-Tenant

Flat monthly fee billed per tenant; pricing scales with number of integrations, inventory size, and alerting volume.

Add-On Bundle

Attach governance as a module to existing security or managed detection plans to expand service breadth without a full re-sell.

Fixed Monthly

Single set fee covering a defined range of tenants; includes a monthly Evidence Pack and scheduled attestations.

Tiered Service

Three-tier offering: T1 Visibility & Reporting, T2 Governance & Attestation, T3 Continuous Monitoring — each with clear deliverables and SLAs.

QBR Value

Position the service as ongoing assurance rather than a one-time audit by showing KPIs and risk reduction in every quarterly business review.

Conclusion

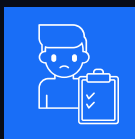
The MSP OAuth Governance Blueprint converts fragmented OAuth checks into a repeatable, revenue-generating managed service. Using a standard data model per integration (publisher verification, scopes, owner, justification, risk, expiry, webhooks), a weighted risk scoring rubric, and defined review cadences with secret alerts, MSPs can discover, review, and remediate risky apps quickly while producing audit-ready evidence mapped to compliance frameworks.



Key Takeaways



Framework: A practical three-tier path—T1 visibility, T2 governance & attestation, T3 continuous monitoring—so you move from discovery to enforced controls.



Compliance: Evidence Pack and data mappings align app inventory and attestations to SOC 2 CC6.6 and ISO 27001 A.9 for audit readiness.



Acceleration: AppGuard360-style automation enables multi-tenant discovery, risk scoring, branded dashboards, and exportable reports—reducing manual work and speeding deployments.

With a 3-tier delivery model (Tier 1: Visibility & Reporting, Tier 2: Governance & Attestation, Tier 3: Continuous Monitoring), clear SLAs/KPIs, and an Evidence Pack for audits, MSPs can launch fast, scale across tenants, and demonstrate measurable security improvements in every QBR—turning governance into ongoing assurance rather than a one-time project.

