Kyūdō

SOVEREIGNTY-GRADE AI · GRC

Kyūdō Quick Start Guide

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · WELCOME

Welcome to Kyūdō.

Kyūdō is the AI-native Governance, Risk, and Compliance platform that runs inside your Azure tenant, reads your Microsoft Security stack natively, and converts it into the audit-ready evidence your auditors, regulators, and customers will accept. This guide gets you from ‘we just signed’ to ‘our evidence is already true’ in seven days.

Most GRC platforms are SaaS. They extract your posture to their cloud, run their own AI over it, and present results in their own dashboards. Kyūdō inverts the architecture: the platform deploys inside your security boundary, reads your environment in place, and stores all governance data in your tenant. That difference is not a feature. It is the entire product.

This Quick Start Guide is for people who will own Kyūdō in the first seven days: the security or compliance lead who sponsored the platform, the platform admin who will run the deployment, the GRC practitioners who will use it daily, and the executive sponsor who needs to see results within one week. Everyone else — auditors, board members, customers reviewing your trust posture — will eventually consume Kyūdō outputs, but the people in those roles do not need to read this document.

The four-vector frame

Kyūdō is built on four architectural commitments. Each one is a claim you can verify; none is configurable; together they are what makes the platform structurally different from anything else in the GRC market.

Vector	What it means in practice
Sovereignty-grade deployment	Kyūdō runs inside your Azure tenant — including the AI that reasons over your governance. Your data never leaves your security boundary. Your identity plane is yours. Your encryption keys are yours. No vendor data plane.
Microsoft-native evidence	Defender, Sentinel, Purview, Entra, and Azure Policy signals become governed evidence automatically, in your environment, without ETL or vendor data extraction. Read-only, least-privilege, system-assigned managed identity throughout.
Knowledge Graph reasoning	Controls, evidence, risks, policies, vendors, and frameworks are typed entities in a unified graph. AI reasons over the graph; every output is cited; every claim has a source. Spreadsheets and disconnected tools do not survive the four-concurrent-framework reality.

Vector	What it means in practice
Operational AI governance	114 AI governance controls. EU AI Act, ISO/IEC 42001, and NIST AI RMF built in. Govern the AI you deploy — using the same platform that governs your security controls. AI governance is not a separate product.

What this guide will not cover

This is a product onboarding document, not a framework reference. If you need the working detail of SOC 2, ISO 27001, NIST CSF v2.0, CMMC L2, or HIPAA, the Kyūdō framework guide series at kyudo.ai/guides covers each individually. Those guides are referenced throughout this document but not reproduced.

This guide also does not cover the technical deployment runbook (Bicep templates, AKS topology, networking, Conditional Access binding). That material lives in the Kyūdō Client-Hosted Azure Reference Architecture & Servicing Runbook, distributed to platform admins on engagement.

01 · WHAT KYŪDŌ DOES

Eight things, every minute.

This is the operational view. Kyūdō runs continuously — these eight functions execute every minute against every signal source connected to the platform. Auditors and regulators will eventually ask about these capabilities individually; in operation, they run together.

Capability	What it produces
Posture clarity	Real-time insight across identities, data, applications, devices, and infrastructure. The single dashboard your CISO opens before a board meeting, the single dashboard the auditor opens on Day 1.
Risk intelligence	Predictive analytics over the full control graph, not isolated risk registers. Risks are linked to the controls that mitigate them and the evidence that proves the control is operating.
Control automation	Continuous compliance checks against 70+ frameworks from a single control set. Test once, satisfy SOC 2 + ISO 27001 + NIST CSF + CMMC + HIPAA + EU AI Act simultaneously.
Policy precision	AI-driven authoring, mapping, and lifecycle governance of every policy. Drafts arrive cited. Updates propagate to the controls they govern. Sunset and review reminders fire automatically.
Vendor assurance	Automated questionnaire handling, scoring, and continuous third-party posture monitoring. Vendor risk is no longer point-in-time at onboarding.
Evidence engine	Automated validation workflow — evidence is current between audits, not just before them. Hash, lineage, and confidence score on every artifact.
Trust Center	Real-time external-facing posture for customers, partners, and regulators. Security questionnaires compress from weeks to hours. Pre-fill with citations and confidence scores.
AI governance	Inventory and policy control for AI systems and agents. ISO/IEC 42001 and EU AI Act compliance from the same platform that governs your other controls.

Source — Kyūdō platform capability map; Kyūdō one-pager (April 2026).

How the eight fit together

These capabilities are not eight separate products. They are eight surfaces over the same Knowledge Graph. A change in one propagates to the others: a new Sentinel detection rule registers as evidence under Control Automation, updates the risk treatment status under Risk Intelligence, changes a vendor's posture score under Vendor Assurance if the rule covers a vendor system, and updates the Trust Center's external-facing posture in real time. The integration is structural, not feature-by-feature.

The practical implication for the first seven days: you do not need to deploy the eight capabilities sequentially. They activate together as connections to your environment come online. Connect Microsoft Defender, and posture clarity, control automation, evidence engine, and (where Defender signals affect vendor systems) vendor assurance all populate together.

02 · THE SIX MODULES

Six integrated modules. One Knowledge Graph.

The eight capabilities surface through six product modules. The modules are how users navigate — each has a dedicated UI, role-based access, and a primary persona. The Knowledge Graph is what makes them integrated; a control modified in one module propagates to the others without manual reconciliation.

Controls Hub

The authoritative registry for every control your organization is responsible for. Controls are auto-discovered from your integrations, mapped to 80+ frameworks via Set Theory Relationship Mapping (STRM), and scored for completeness on a 0–100 scale. The Controls Hub is the single source of truth for ‘what controls do we have, what frameworks do they satisfy, are they operating effectively right now’. Primary persona: GRC Lead, Compliance Officer.

Evidence Hub

Automated collection from Microsoft Security and cloud platforms. Every artifact is a Knowledge Graph entity with a cryptographic hash, a lineage chain back to the source signal, and an AI-computed confidence score. The Evidence Hub is where the auditor's ‘show me the evidence for AC.L2-3.1.1’ question is answered in seconds rather than days. Primary persona: GRC Practitioner, Internal Auditor.

Policy Center

AI-authored policy grounded in the controls the policy governs. Continuous gap analysis flags policies that are inconsistent with their governing controls. Every draft is cited. Every change updates downstream controls and evidence requirements. Policy is treated as a living entity, not a Word document refreshed annually. Primary persona: Policy Manager, Compliance Officer.

Risk Management

Risks are typed entities linked to the controls that mitigate them and the evidence that proves the controls are operating. Posture reflects live operational reality — if a Conditional Access policy is modified in Entra ID, the risk treatment status updates within minutes. Board-ready dashboards present residual risk as a trajectory rather than a snapshot. Primary persona: Risk Manager, CISO.

Vendor Risk Management

Automated questionnaire handling with Knowledge Graph citations — Kyūdō answers most security questionnaires from existing evidence with confidence scores per answer. AI-scored

vendor posture against 0–10 risk scales. Continuous monitoring of public-facing vendor posture, not annual review. Primary persona: Vendor Risk Analyst, Procurement.

Trust Center

Customer-facing transparency portal. Replaces the security questionnaire mill that consumes weeks of GRC time per quarter. Customers and prospects review your posture in a controlled portal with appropriate access scoping. Pre-fill any remaining questionnaires with citations and confidence scores. Security reviews compress from weeks to hours. Primary persona: GRC Lead, Sales Engineering.

Two additional engines run beneath the modules

CMCAE — the Continuous Multi-Framework Control Assessment Engine. Recalculates control completeness, Capability Maturity Levels 1–5, and residual risk on every signal change. The mechanism that makes ‘evidence is already true’ architecturally rather than aspirationally.

STRM — Set Theory Relationship Mapping (per NIST IR 8477). The mathematical substrate that makes one control set satisfy 70+ frameworks simultaneously. STRM is the reason Kyūdō can answer SOC 2 + ISO 27001 + CMMC + HIPAA from the same control evidence without redundant testing.

03 · TWO WAYS TO DEPLOY

SaaS or sovereign. Same platform, different boundary.

Kyūdō supports two deployment topologies. Both run the same code, the same Knowledge Graph, the same modules. The difference is where the security boundary sits.

Topology	Where Kyūdō runs	When to choose it
Multi-tenant SaaS	Shared AKS cluster managed by Kyūdō, with logical isolation (tenant-scoped RBAC + network policy). Standard SOC 2-grade SaaS deployment with the Kyūdō tenant as the security boundary.	Mid-market organizations without specific data-residency mandates. Faster onboarding (provisioned in hours, not days). Lower up-front cost. Same product capabilities.
Client-hosted Azure	Dedicated Helm-deployed services inside your Azure tenant. Hub-and-spoke topology with strict private endpoints. AKS, Azure SQL, Cosmos DB, ADLS Gen2, Azure OpenAI — all in your subscription, your tenant, your encryption keys.	Regulated organizations: defense (CMMC), healthcare (HIPAA, regional residency), financial services with strict data localization, organizations with federal contracts, organizations on Azure Government / GCC High.

The architectural mechanisms behind client-hosted

If you choose the client-hosted Azure topology, four mechanisms are not configurable — they are how the deployment is built.

- No cross-tenant data plane. Every Kyūdō service runs inside your Azure subscription. There is no path for compliance data to reach vendor infrastructure, because no such path exists in the architecture.
- Private endpoints on every service. Application services, storage, Key Vault, SQL, Identity, and AI inference — every service exposes private endpoints only. Traffic never leaves the Microsoft backbone.
- System-assigned managed identities. Service-to-service authentication uses managed identities bound to your tenant. No shared secrets. No vendor-held credentials.
- Tenant-scoped AI inference. AI operations execute on Azure OpenAI Service in your tenant, with your model deployments, your content filtering, your audit logs.

The deployment quick reference

For client-hosted Azure deployments, the bootstrap sequence is captured in the reference runbook. Implementation timeline: 1–2 days including Azure landing zone preparation, AKS provisioning, networking, Entra ID integration, and Sentinel connectivity. The high-level shape:

Step	Activity	Owner
1	Authenticate to Azure CLI; set the target subscription.	Platform admin
2	Create the resource group in your primary region (typical: Canada Central, East US, West Europe per residency).	Platform admin
3	Deploy the Bicep baseline with environment, region, AKS sizing, and network ranges parameters. Outputs include managed-identity resource IDs and private DNS zone bindings.	Platform admin
4	Bind private endpoints (SQL, Storage, OpenAI) if not auto-created. Configure Conditional Access policies for Kyūdō administrative access.	Platform admin + identity admin
5	Register Entra ID groups and map them to Kyūdō RBAC roles. Onboard your first administrative users.	Identity admin
6	Enable Sentinel analytics and dashboards (if Sentinel is in scope).	SOC lead
7	Validate against SLOs: API P95 ≤500ms, evidence ingest ≤2s, Light-RAG P95 ≤500ms, HITL threshold 0.7.	Platform admin

Source — Kyūdō Client-Hosted Azure Reference Architecture & Servicing Runbook v1.0, Appendix D.

04 · PRE-FLIGHT CHECKLIST

What to have ready before kickoff.

Kyūdō onboarding moves at the speed of access. Most onboarding delays trace to a single category: the customer team did not have the necessary identities, permissions, or organizational decisions in place when the engagement started. The checklist below covers the items that, if assembled before kickoff, make the seven-day timeline achievable. Items missed here are the single largest source of slip.

Organizational

- Executive sponsor identified. Typically the CISO, CIO, or Chief Compliance Officer. The person who can break ties on framework prioritization and resource allocation.
- Platform admin identified. The person responsible for the Kyūdō deployment and ongoing operation. Will hold tenant-admin scope in Kyūdō RBAC. Has 50–70% of their working time available across the seven days.
- Frameworks in scope decided. Which 1–2 frameworks does the first week target? SOC 2 is typical for SaaS organizations. CMMC is typical for defense. HIPAA is typical for healthcare. Pick the smallest set that addresses your near-term external commitment — second framework can activate in Week 2.
- Existing GRC tools inventoried. If you are migrating from Vanta, Drata, OneTrust, ServiceNow GRC, or LogicGate, identify which artifacts to import (policies, controls, evidence) and which to leave behind. Migration itself happens in Week 2; the inventory drives Day 5–6 prep.

Technical — Microsoft 365 and Azure

- Tenant identified. Production tenant for Kyūdō operations; in client-hosted deployments, the same tenant Kyūdō will deploy into.
- Subscription identified. The Azure subscription Kyūdō will deploy into (client-hosted) or read from (SaaS). Subscription-level Reader access required minimum; specific role assignments per integration documented in Appendix B.
- Region selected. Primary region for Kyūdō services; secondary region for DR. Choose based on data-residency requirements (Canada Central + Canada East for Canadian residency; East US + West US for U.S.; West Europe + North Europe for EU).
- Microsoft Entra ID tenant administrator available. Required for OAuth consent flows during integration setup. The platform admin should either hold this role or have a path to it within hours, not days. The single most common Day 0–2 slip is OAuth consent timing.
- Existing Microsoft licenses confirmed. Microsoft 365 E3 or higher recommended; E5 unlocks the densest evidence (Defender for Endpoint, Defender for Office 365, Purview, Sentinel). Azure subscription with Defender for Cloud Standard tier.

Technical — access and credentials

- OAuth consent. The platform admin will be prompted to consent to read-only Graph API scopes during integration setup. Pre-coordinate with your identity team if Conditional Access or admin consent workflows will require additional approval.
- Service principal (client-hosted only). The Bicep deployment requires a service principal with Contributor at the resource group level. Kyūdō does not require subscription-level Contributor. Pre-provision in advance if your service principal creation process takes more than four hours.
- Customer-managed keys (optional). If you require customer-managed encryption keys for Kyūdō's storage, identify the Key Vault and the keys before deployment.
- Conditional Access scope. Identify which Conditional Access policies will apply to Kyūdō administrative access. Phishing-resistant MFA recommended.

Documentation

- Existing policies. Information security policy, access control policy, incident response plan, business continuity plan, vendor management policy. If you have these in any form (Word, SharePoint, Confluence), Kyūdō Policy Center can ingest them in Week 2; the inventory is what's needed for Day 7.
- Most recent audit reports. SOC 2, ISO 27001, CMMC, HIPAA risk analyses, third-party assessments. Useful for both context and evidence-of-prior-state.

> **If you do not have all of this, do not delay kickoff**
>
> The pre-flight checklist is the optimal state. The reality is that most organizations are missing items — frequently the existing policies, specific framework decisions, or pre-provisioned service principals. Kyūdō's onboarding is designed to surface these gaps quickly and address them in Days 1–3 rather than block engagement on their resolution.
>
> If you have the executive sponsor, the platform admin, the tenant identified, and at least one framework decision, you have enough to start. The remaining items can be assembled in parallel with the first deployment activities. The seven-day timeline assumes the high-leverage items (tenant access, OAuth consent path, service principal) are in place.

Day 0 to Day 7.

Kyūdō is engineered for a one-week onboarding. The deployment itself is one to two days; the Microsoft integrations connect in 30–60 minutes each; control auto-discovery and evidence flow begin within minutes of each integration coming online. By Day 7, the platform is operational, your priority Microsoft integrations are connected, the Knowledge Graph holds thousands of evidence artifacts, and your first framework is mapped against live posture.

The seven-day cadence below is the typical shape across customers. SaaS deployments tend to compress Days 1–2 into a single afternoon. Client-hosted Azure deployments use the full Day 1–2 window for the Bicep baseline, private endpoints, and identity binding. From Day 3 onward, the two topologies look identical.

Day 0 — Kickoff

A 90-minute kickoff call with your Kyūdō customer success engineer, your executive sponsor, your platform admin, and any other Day-1 stakeholders. The call walks the architecture, confirms the framework scope, validates the pre-flight checklist, and agrees on the seven-day milestones.

- Output: signed deployment plan; named owners per workstream; Day 1–7 milestones with specific dates and times; Slack or Teams channel for ongoing collaboration; service principal and OAuth consent coordination confirmed.

Days 1–2 — Deploy

In a SaaS deployment, this is provisioning your tenant in the Kyūdō platform — typically completed within hours. In a client-hosted Azure deployment, this is the Bicep deployment described in Section 3 of this guide and detailed in the Reference Runbook — typically completed across one to two business days.

1. Day 1 morning: Tenant provisioned (SaaS) or Bicep deployment kicked off (client-hosted). Resource group created. Bicep template applied with parameters for region, environment, AKS sizing.
2. Day 1 afternoon: Private endpoints bound (client-hosted). Conditional Access policies configured for Kyūdō administrative access. Entra ID groups created and bound to Kyūdō RBAC roles.
3. Day 2 morning: First administrative user signs in. Multi-factor authentication confirmed working. Platform SLOs validated: API P95 ≤500ms; evidence ingest ≤2s; Light-RAG P95 ≤500ms.
4. Day 2 afternoon: First Microsoft integration connected. Typically Microsoft Entra ID, since it has the lightest footprint and validates the OAuth consent flow with the lowest blast radius. Initial signal flow confirmed; first auto-discovered controls visible in the Controls Hub.

Output by end of Day 2: platform deployed, first user authenticated with MFA, Entra ID integration connected, first auto-discovered controls visible, first evidence artifacts registered. The platform is operational; the rest of the week extends signal coverage.

Days 3–5 — Connect the Microsoft estate

Connect the remaining Microsoft integrations in priority order. Each connection adds evidence sources and increases control coverage. Each integration follows the same five-stage pattern: initiate from Settings > Integrations, authorize via OAuth or service principal, validate the test connection, configure the data ingestion schedule, and confirm the resource inventory. Most integrations complete in 30–60 minutes once the authorization is in place.

Day	Microsoft service	What it adds
3	Microsoft Defender for Cloud	CSPM findings, regulatory compliance dashboard, secure score trend, recommendations. Highest evidence density per integration; the single highest-leverage Microsoft connection.
3	Microsoft Defender XDR	Threat detections, Defender for Endpoint device compliance, Defender for Office 365 attack simulation training records, alert handling history.
4	Microsoft Sentinel	SIEM telemetry, analytic rule definitions, incident records, SOAR playbook execution. Activates Continuous Monitoring controls.
4	Microsoft Purview	Data classification, sensitivity labels, DLP policy executions, eDiscovery records. Activates Data Security and Privacy controls.
5	Azure Policy + Resource Graph	Configuration compliance state, baseline enforcement evidence, drift detection at the resource level.
5	Microsoft Graph API (M365)	M365 Unified Audit Log, mailbox configuration, SharePoint policy state, Teams compliance settings.

Output by end of Day 5: the seven priority Microsoft integrations connected; the Controls Hub populating with auto-discovered controls mapped to your in-scope frameworks; the Evidence Hub registering thousands of artifacts; the Risk Management module surfacing initial risk assessment based on observed posture.

Day 6 — First framework activation

Day 6 is when Kyūdō's value proposition becomes operational. Your platform admin and GRC lead activate the first framework against the live posture. Most of the work has already happened invisibly — the Microsoft integrations of Days 3–5 produce the evidence the

framework requires; STRM mapping has already aligned the auto-discovered controls to the framework's specific requirements; CMCAE has scored each control for completeness.

- Confirm framework selection (decided in pre-flight). SOC 2, ISO 27001, NIST CSF, CMMC L2, or HIPAA — the framework guide series at kyudo.ai/guides covers each.
- Walk the Controls Hub view filtered to the selected framework. Identify control gaps (controls scored below 50% completeness) and review with the GRC lead.
- Walk the Evidence Hub view for the same framework. Spot-check evidence per control: hash, lineage, confidence score, source signal. This is the same view an auditor will see.
- Configure the Trust Center with the selected framework as the headline posture artifact. Pre-fill any standing customer questionnaires with citations.

Output by end of Day 6: first framework operational with continuous evidence; control completeness baseline established; gap list produced; Trust Center configured for external visibility.

Day 7 — Executive readout

Day 7 closes the week with an executive readout. The session is 60 minutes; the audience is the executive sponsor plus any other senior stakeholders relevant to the GRC program. The readout is not a status update — it is the demonstration of the new operating cadence.

- Posture clarity dashboard — control completeness across the activated framework; trajectory since Day 1; identified gaps.
- Evidence summary — total artifacts collected; coverage by control category; sample audit-defensible evidence walked end-to-end.
- Risk surface — initial risk register derived from observed posture; treatment recommendations; trajectory.
- Trust Center demonstration — what your customers, auditors, and regulators will see when they request transparency on your posture.
- Week 2 plan — absorbing the existing GRC program (policies, risk register, vendor inventory) and activating any second framework. This sets the cadence for the remainder of Month 1.

Output by end of Day 7: executive readout delivered; Week 2 plan agreed; the audit-story-already-true outcome demonstrable rather than aspirational.

After Day 7

The seven-day arc gets you to operational. Week 2 absorbs the existing GRC program: policies are imported into the Policy Center and aligned to controls; the existing risk register is normalized into the Risk Management module; the vendor inventory is bootstrapped into VRM. By the end of Week 2, Kyūdō is the system of record for your governance, not just an evidence-collection layer over your Microsoft estate.

Weeks 3–4 add additional frameworks (each subsequent framework activates faster than the first because the STRM mapping is already populated) and run the first internal audit cycle. By Day 30, customers typically have 2–4 frameworks operational and the audit-story-already-true outcome demonstrated to internal stakeholders.

The integration walk.

Every Microsoft integration in Kyūdō follows the same five-stage workflow. The detail varies (OAuth vs service principal, scope per integration, data ingestion schedule), but the shape is consistent.

The five stages

Stage	What happens	Owner
1. Initiate	Tenant admin opens Settings > Integrations, selects the desired integration, clicks Set Up. The setup wizard loads with a description, required permissions list, and (where available) a video walkthrough.	Tenant admin
2. Authorize	OAuth (M365, Entra, Defender, Graph): ‘Sign in with Microsoft’ prompt; admin grants requested scopes. Service principal (Azure Resource Graph, Azure Policy): admin pastes service principal credentials. All credentials stored encrypted in Azure Key Vault.	Tenant admin + identity admin
3. Validate	Kyūdō performs a test call against the integration to verify minimal permissions. ‘Test Connection’ button confirms the integration is functional.	Automatic
4. Configure	Set the data ingestion schedule (typical: every 15 minutes for high-velocity signals, hourly for configuration state). Define the resource scope (which subscriptions, which tenants, which environments).	Tenant admin
5. Confirm	Resource inventory populates (e.g., AWS EC2 instances, Azure subscription list, Entra ID users, Conditional Access policies). Controls auto-discover. First evidence artifacts register.	Automatic

Permission scopes per integration

Every Microsoft integration is read-only and least-privilege by design. Kyūdō never requires admin tokens; nothing the platform does requires write access to your tenant. The scopes per integration are documented per service in Appendix B and in the Settings > Integrations detail page for each service.

Beyond the Microsoft stack

Microsoft integrations are the most common deployment pattern, but Kyūdō also reads natively from non-Microsoft sources. Each follows the same five-stage workflow with the appropriate authentication mechanism.

Source	What Kyūdō ingests
AWS (CloudTrail, Config, Security Hub, GuardDuty)	Account-level posture, audit-log telemetry, configuration findings. IAM-based authentication via AWS access key and secret.
Google Cloud (SCC, Cloud Audit Logs, Asset Inventory)	Findings, asset state, audit telemetry. Service account JSON-based authentication.
Kubernetes (AKS, EKS, GKE, OpenShift)	Cluster posture, admission decisions, workload identity, workload configuration. Authenticated via cluster-bound service account or managed identity.
GitHub (Advanced Security, Audit Log, Dependabot)	Code scanning findings, secret detection, repository configuration, audit log. GitHub App authentication.
Oracle Cloud Infrastructure (Cloud Guard, Audit, IAM)	Posture findings, identity state, audit telemetry. OCI API key authentication.

07 · YOUR FIRST AUDIT STORY

What “evidence already true” actually looks like.

By Day 7, Kyūdō should change how your team operates around audits. The conventional pattern — evidence collection sprint in the 6–8 weeks before an audit, fire-drill mapping, last-minute control remediation, anxiety throughout — should be replaced by a continuously-current posture that survives the auditor's first questions.

Three concrete scenarios illustrate what changes.

Scenario 1 — The auditor's Day 1 evidence request

An external auditor begins a SOC 2 Type II observation period and asks for evidence of access reviews for in-scope systems for the past quarter.

Conventional	With Kyūdō
GRC lead emails the IT team. IT pulls Entra ID Governance access review reports for the relevant systems, manually filters for in-scope users, exports to PDF, formats for the auditor, and sends to the GRC lead. Three to five business days; multiple back-and-forth clarifications; one or two systems usually missed in the first pass.	GRC lead opens the Evidence Hub, filters by control (Access Reviews — mapped to SOC 2 CC6.2), filters by date range. Every access review record for the period appears with hash, timestamp, lineage to the originating Entra ID Governance review, and confidence score. Exported as a single PDF or shared with the auditor through the Trust Center. Same day; no IT involvement.

Scenario 2 — The customer security questionnaire

A prospect sends a 200-question security questionnaire as part of vendor due diligence. Response deadline: 5 business days.

Conventional	With Kyūdō
Sales engineer or GRC analyst opens the questionnaire. Manually answers each question by referencing the most recent SOC 2 report, the security policies, the BAA, and (for unanswerable questions) the GRC lead's institutional knowledge. Typically 2–3 days of dedicated effort. Quality varies by analyst.	Sales engineer or GRC analyst uploads the questionnaire to the Trust Center. Kyūdō pre-fills 70–85% of answers with citations and confidence scores. The analyst reviews flagged answers (low confidence or no source), confirms or edits, exports the completed questionnaire. Typically 2–4 hours.

Scenario 3 — The board posture review

CISO presents quarterly to the board. Board wants to see security posture trajectory across the year, framework compliance posture, top risks, and material control gaps.

Conventional	With Kyūdō
CISO requests reports from the security operations team (Defender Secure Score), the GRC team (compliance status), the risk team (risk register), and the audit team (recent findings). Each team produces a slide. CISO assembles into a deck, often discovering inconsistencies between the slides that require reconciliation. Two weeks of back-and-forth.	CISO opens the Kyūdō executive dashboard. Posture clarity, control completeness, residual risk trajectory, and recent evidence trend are present in real time. Exports the relevant views directly to the board deck. The reconciliation problem does not exist because all views read from the same Knowledge Graph.

08 · WHERE TO GO NEXT

Resources, contacts, and the framework guide series.

This Quick Start Guide gets you operational in seven days. The deeper material lives elsewhere — the framework guides for compliance specifics, the Reference Runbook for deployment depth, your customer success engineer for the day-to-day. The map below points to each.

The Kyūdō framework guide series

Five flagship guides cover the frameworks Kyūdō customers most commonly operate against. Each is freestanding, sourced to authoritative regulation and standards, and reflects current 2026 reality. Available at kyudo.ai/guides.

Guide	When to read it
SOC 2 Type II Preparation Guide	Before your first SOC 2 Type II observation period; for refining the existing program; for the Trust Services Criteria deep dive.
ISO 27001 Implementation Guide	Before scoping or recertifying an ISMS; reflects the post-October 31, 2025 reality where 27001:2013 is no longer valid; covers the new-in-2022 controls and the SoA mechanics.
NIST CSF v2.0 Mapping Reference	For board communication, regulator engagement, or aligning the program against a recognized framework. Includes complete subcategory enumeration and cross-framework crosswalks.
CMMC Level 2 Readiness Checklist	If your organization is in the U.S. Defense Industrial Base; 30–90 days before a C3PAO assessment; especially relevant given Phase 2 begins November 10, 2026.
HIPAA Compliance Automation Guide	Healthcare covered entities and business associates; addresses both the current Security Rule and the pending NPRM expected for May 2026 finalization.

Internal Kyūdō resources

- The Reference Architecture & Servicing Runbook — detailed deployment guidance for client-hosted Azure topology. Provided to platform admins on engagement. Bicep templates, network topology, security baseline, monthly update channel.

- The Marketing Constitution — the brand and messaging foundation. Internal-facing; shapes how Kyūdō speaks and what claims are defensible.
- Per-module deep documentation — in-product help for Controls Hub, Evidence Hub, Policy Center, Risk Management, VRM, and Trust Center.
- API documentation — for organizations integrating Kyūdō with their own systems. REST and GraphQL endpoints; authentication via OAuth 2.0.

Kyūdō-led engagements

- Architecture briefing — 30 minutes; the deployment in your tenant; controls, evidence flow, sovereignty model. → hello@kyudo.ai
- Mission workshop — 90 minutes; mapping your current control set to the continuous-evidence model; SOC 2, ISO 27001, EU AI Act views from a single control set. → kyudo.ai/workshop
- Trust packet — our SOC 2 report, architecture diagrams, data-residency statement, the Microsoft estate dependency map. Available on request.

Where this leaves you

Kyūdō is a system of record for governance — not a dashboard with a chatbot. The first seven days establish the platform inside your environment and connect it to the operational sources of truth. After that, the platform runs continuously: evidence is captured at execution time, controls are scored on every signal change, policies stay aligned to controls, risks are tracked against live posture. The audit story writes itself because there is no separate audit-story-writing process — the Knowledge Graph is the audit story, queryable on demand.

If at any point the work feels harder than it should, talk to your customer success engineer. The platform is designed to remove operational drag from compliance work; if drag returns, something is configurable. Most issues we hear about resolve in a 30-minute call.

—

> **Ready when you are**
>
> If you are reading this guide before signing, the next step is the architecture briefing. 30 minutes; in your tenant; with your platform admin and security lead. → hello@kyudo.ai
>
> If you are reading this guide after signing, the next step is your Day 0 kickoff. Your customer success engineer will reach out within 2 business days of signing.
>
> If you are reading this guide after Day 0, this document is the map. Every section beyond this one is a runbook for the corresponding stage of your first seven days.

APPENDIX A · ROLES AND ACCESS

Kyūdō RBAC at a glance.

Kyūdō RBAC maps to Entra ID groups in your tenant. The role assignments below are the canonical set; custom roles are supported but rarely needed. All roles are scoped to your tenant; cross-tenant role inheritance does not exist by design.

Role	Description	Access level
System Admin	Platform administrator managing global configurations and tenants. Held only by Kyūdō operations personnel in SaaS deployments; held by platform admin in client-hosted deployments.	Full
Tenant Admin	Manages tenant-specific modules, users, integrations, and roles. The senior administrative role inside your organization.	High
Compliance Officer	Tracks controls, manages evidence, generates reports. Cannot modify integrations or RBAC.	Medium
Policy Manager	Authors and updates policies via the Policy Center. AI-assisted authoring; approval workflow integration.	Medium
Risk Manager	Identifies and tracks organizational risks. Risk register management; risk treatment workflow.	Medium
Vendor Risk Analyst	Manages third-party assessments, vendor inventory, questionnaire automation, continuous monitoring of vendor posture.	Medium
Auditor	Reviews audit logs, tests, and evidence. Read-everything plus annotation capability; no modification.	Read/Write
General User	Submits data, uploads evidence, uses chat interfaces. Limited to assigned workflows and queues.	Limited

Source — Kyūdō SRS v7, User Classes and Characteristics.

Mapping to Entra ID groups

During Days 1–2 of onboarding, your identity admin creates Entra ID groups corresponding to each role and assigns users. Kyūdō then binds the groups to the platform RBAC roles. The

recommended pattern is one group per role with descriptive names (e.g., ‘Kyūdō-TenantAdmins’, ‘Kyūdō-ComplianceOfficers’).

Conditional Access policies should target the Kyūdō groups specifically, requiring phishing-resistant MFA and compliant device for any role above General User. The platform administrator role and tenant administrator role should additionally require Privileged Identity Management activation rather than standing access.

What scope each integration requires.

Kyūdō operates on a strict least-privilege principle. Every integration uses the minimum scope required to retrieve the data Kyūdō needs. The table below lists the Microsoft Graph and service-specific scopes per integration; scopes are confirmed during the OAuth consent flow at integration setup time.

Microsoft Graph (M365 + Entra ID)

Scope	Why Kyūdō needs it
AuditLog.Read.All	Read the M365 Unified Audit Log; activate Audit Controls evidence.
Directory.Read.All	Read users, groups, role assignments, service principals; activate Identity and Access Control evidence.
Policy.Read.All	Read Conditional Access policies, identity protection policies, authorization policies.
IdentityRiskyUser.Read.All	Read Entra ID Identity Protection risky user signals; activate Identity Risk evidence.
IdentityRiskEvent.Read.All	Read Identity Protection risk events.
AccessReview.Read.All	Read Entra ID Governance access reviews; activate Access Review evidence.
AuditLog.Read.All / SignIns	Read Entra ID sign-in logs; activate Authentication evidence.

Microsoft Defender for Endpoint

Scope	Why Kyūdō needs it
Machine.Read.All	Read device inventory and compliance state; activate Device Compliance evidence.
Alert.Read.All	Read security alerts; activate Threat Detection evidence.
Vulnerability.Read.All	Read vulnerability findings; activate Vulnerability Management evidence.
AdvancedQuery.Read.All	Read Advanced Hunting query results; activate Threat

Scope	Why Kyūdō needs it
	Hunting evidence (optional).

Microsoft Defender for Cloud

Scope	Why Kyūdō needs it
Reader (subscription level)	Read Defender for Cloud recommendations, Secure Score, regulatory compliance dashboard. The single highest-density Microsoft integration for control evidence.
Security Reader	Read security alerts and assessments at the subscription level.

Microsoft Purview

Scope	Why Kyūdō needs it
Compliance Manager Reader	Read Compliance Manager assessments, improvement actions, and scoring; activate cross-framework Compliance Manager evidence.
DataLossPreventionPolicy.Read.All	Read DLP policies and policy execution evidence.
InformationProtectionPolicy.Read.All	Read sensitivity labels and policy configuration.
RecordsManagement.Read.All	Read retention policies and label state.

Microsoft Sentinel + Azure

Scope	Why Kyūdō needs it
Microsoft Sentinel Reader	Read Sentinel analytic rules, incidents, workbooks, hunting query history.
Azure Policy Reader	Read Azure Policy compliance state across the subscription.
Azure Resource Graph Reader	Read resource topology, tagging, and configuration state.
Reader (subscription)	Baseline for Azure Resource Graph queries; minimum role for service principal authentication.

Source — Kyūdō SRS v7 Appendix A, Consolidated Microsoft Services Permissions Matrix. Scopes confirmed at OAuth consent during integration setup.

APPENDIX C · GLOSSARY

Kyūdō terms used in this guide.

Term	Definition
AKS	Azure Kubernetes Service. The container orchestration platform Kyūdō microservices run on, in both SaaS and client-hosted deployments.
Bicep	Microsoft's domain-specific language for declarative Azure resource deployment. The Kyūdō client-hosted deployment is captured in a Bicep baseline plus parameter overrides.
Capability Maturity Levels (CML)	1–5 scale used by the CMCAE to characterize the maturity of each control implementation. Maps to the NIST Cybersecurity & Privacy Capability Maturity Model.
Client-hosted deployment	The deployment topology in which Kyūdō runs entirely inside the customer's Azure tenant. Helm-deployed services, customer-owned data plane, no cross-tenant data movement.
CMCAE	Continuous Multi-Framework Control Assessment Engine. The Kyūdō engine that recalculates control completeness, CML, and residual risk on every signal change.
Confidence score	AI-computed score on every Kyūdō output. Indicates how strongly the source signals support the conclusion. Below the HITL (Human-in-the-Loop) threshold of 0.7, outputs are flagged for human review.
Controls Hub	The Kyūdō module that serves as the authoritative registry for every control your organization is responsible for.
Evidence Hub	The Kyūdō module that holds every evidence artifact, with hash, lineage, and confidence score. The destination of automated evidence collection from Microsoft and other integrations.
HITL	Human-in-the-Loop. The threshold (0.7 default) below which AI-produced outputs require human review before they propagate.
Knowledge Graph	The Kyūdō substrate that stores controls, evidence, policies, risks, vendors, and frameworks as typed entities with explicit relationships. The foundation that makes ‘a change in one domain propagates intelligently across the others’ architecturally true.
Light RAG	Light Retrieval-Augmented Generation. The Kyūdō inference pattern that grounds AI outputs in Knowledge Graph context with citations on every claim.

Term	Definition
Managed identity	Azure mechanism for service-to-service authentication without shared secrets. System-assigned managed identities are the default Kyūdō pattern for client-hosted deployments.
Multi-tenant SaaS	The deployment topology in which Kyūdō runs in a shared cluster managed by Kyūdō, with logical isolation per tenant.
NIST IR 8477	Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines. The NIST Internal Report that formalizes Set Theory Relationship Mapping.
Policy Center	The Kyūdō module for AI-authored, control-aligned policy lifecycle management.
Private endpoint	Azure mechanism for service-to-service connectivity via private IP addresses on the Microsoft backbone, never traversing the public internet. The default Kyūdō client-hosted networking pattern.
Risk Management	The Kyūdō module for risk identification, treatment, and ongoing monitoring linked to the controls and evidence in the Knowledge Graph.
RBAC	Role-Based Access Control. The Kyūdō authorization model, mapped to Entra ID groups in your tenant.
SCF	Secure Controls Framework. The meta-framework substrate that anchors the Kyūdō Knowledge Graph; 1,470+ controls across 80+ frameworks.
SLO	Service Level Objective. The Kyūdō platform SLOs: API P95 ≤500ms; evidence ingest ≤2s; Light-RAG P95 ≤500ms; HITL threshold 0.7.
STRM	Set Theory Relationship Mapping (per NIST IR 8477). The mathematical substrate that makes one Kyūdō control set satisfy 70+ frameworks simultaneously.
Tenant	In Azure terminology, an Entra ID-bounded directory representing your organization. In Kyūdō terminology, your isolated data and configuration boundary within the platform.
Trust Center	The Kyūdō module that provides external-facing posture visibility for customers, partners, and regulators.
VRM	Vendor Risk Management. The Kyūdō module for third-party risk assessment, questionnaire automation, and continuous vendor posture monitoring.