Kyūdō

SOVEREIGNTY-GRADE AI · GRC

First 30 Days — Implementation Roadmap

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 · HOW TO USE THIS ROADMAP

Thirty days from kickoff to operating cadence.

This is the operational roadmap for the first 30 days of Kyūdō after kickoff. It assumes you have signed, your customer success engineer has been assigned, and your Day 0 kickoff has happened or is imminent. If you are still evaluating Kyūdō or have not yet completed the pre-flight checklist, start with the Kyūdō Quick Start Guide — this document picks up where that one ends and goes deeper.

The 30-day roadmap is built around four weeks. Week 1 (Days 0–7) deploys the platform, connects the Microsoft estate, activates the first framework, and produces a Day 7 executive readout — this is the same arc as the Quick Start Guide, with day-by-day operational detail added. Week 2 (Days 8–14) absorbs your existing GRC program: policies into the Policy Center, the existing risk register into Risk Management, the vendor inventory into VRM, the Trust Center configured for external visibility. Week 3 (Days 15–21) activates additional frameworks against the same control set. Week 4 (Days 22–30) runs the first internal audit cycle and produces the Day 30 executive readout that establishes the new operating cadence.

By Day 30 you should have automated evidence flowing for two to four frameworks, your existing policies and risk register normalized into the Knowledge Graph, your vendor inventory under continuous monitoring, your Trust Center serving inbound questionnaires, a successful internal audit cycle on at least one framework, and an executive briefing that establishes the new operating cadence. The audit-story-already-true outcome is no longer a claim — it is what your team is measurably operating on.

Who this roadmap is for

Role	How to use this document
Platform admin	Read end-to-end before Day 1. The day-by-day activities in Sections 03–06 are your working schedule. Appendix A consolidates every activity into a single matrix you can paste into your project tracker.
GRC lead / compliance officer	Read Sections 00–02 then focus on Sections 04–06. The Week 2 transition (Day 8+) is where most of your work begins. You can skim the deployment week — your platform admin owns it.
Executive sponsor	Read Sections 00, 01, and 06. The Day 7 readout (Section 03 close) and Day 30 readout (Section 06) are the two senior-stakeholder sessions you will receive. Use them as the templates for what to expect.
Customer success	This document is your shared script with the customer. Walk it

Role	How to use this document
engineer (Kyūdō-side)	during Day 0 kickoff; reference it in weekly syncs; track progress against the daily activity matrix in Appendix A.

The four-week shape

Read the table below before reading anything else. It is the map of the next 30 days at the deepest possible compression. Every section after this one is detail; the shape stays consistent.

Week	Days	What happens	Exit criterion
1 — Deploy & connect	0–7	Bicep deployment or tenant provisioning. Identity binding. First sign-in. Seven priority Microsoft integrations connected. First framework activated. Day 7 readout.	Platform operational; 7 Microsoft integrations connected; first framework mapped against live posture; Day 7 readout delivered.
2 — Absorb	8–14	Existing policies imported into Policy Center. Risk register normalized into Risk Management. Vendor inventory bootstrapped into VRM. Trust Center configured.	Policies aligned to controls; risks linked to controls and evidence; vendors under continuous monitoring; Trust Center serving questionnaires.
3 — Extend	15–21	Second and (where applicable) third framework activated. Cross-framework consolidation. Non-Microsoft sources connected (AWS, GCP, GitHub) where in scope.	2–4 frameworks operational; same evidence satisfying multiple frameworks via STRM; non-Microsoft sources connected.
4 — Prove	22–30	First internal audit cycle on the lead framework. Auditor walks the Evidence Hub end-to-end. Findings logged. Day 30 readout. Operating cadence established.	Internal audit cycle complete; findings logged; Day 30 readout delivered; operating cadence agreed.

If you only read one thing

The most consequential decision in your first 30 days is which 1–2 frameworks you activate in Week 1. Customers who let that decision drift past Day 5 finish Month 1 without the audit-story-already-true outcome. Lock the framework decision in pre-Day-0; it belongs to your executive sponsor.

01 · THE 30-DAY SHAPE

Four weeks. Four exit criteria. Two executive readouts.

The four weeks above are not a project plan you can ignore once it is approved. They are the sequence in which Kyūdō becomes operational, and skipping or compressing a week produces predictable downstream problems. Each week has an exit criterion that must be met before the next week begins; the platform admin is the gatekeeper.

Why the order matters

Week 1 has to be first because no integration can connect without the platform deployed and identity bound, and no framework can activate without the integrations producing evidence. Week 2 has to follow Week 1 because absorbing your existing GRC program (policies, risks, vendors) is most efficient once the controls have already auto-discovered — importing policies before the controls populate means manually reconciling them later. Week 3 has to follow Week 2 because additional frameworks activate fastest when the control set is already populated and the existing program has been absorbed; new frameworks then inherit coverage from existing evidence via STRM. Week 4 has to be last because the first internal audit cycle is meaningful only after the program is fully populated.

The temptation to do everything in parallel is real, especially for organizations with internal pressure to show fast results. Resist it. The 30-day timeline as designed produces an operational platform with two to four frameworks active by Day 30 and a successful internal audit cycle. The same activities done in parallel typically produce a half-deployed platform with multiple frameworks partially mapped, no integrations fully validated, no internal audit cycle, and a Day 30 executive readout that is not defensible. The phased approach is faster.

What changes for SaaS vs client-hosted Azure

Both deployment topologies follow the same four weeks with the same exit criteria. The difference is concentrated in Week 1: client-hosted deployments use the full Days 1–2 window for Bicep provisioning and private endpoint binding; SaaS deployments compress this into hours. From Day 3 onward, the two topologies look identical.

Week	Multi-tenant SaaS	Client-hosted Azure
Week 1 — Deploy & connect	Tenant provisioning in hours. Day 1 first sign-in possible. From Day 2 onward identical to client-hosted.	Bicep deployment across Days 1–2. Day 2 first sign-in. From Day 3 onward identical to SaaS.
Week 2 — Absorb	Identical for both topologies.	Identical for both topologies.

Week	Multi-tenant SaaS	Client-hosted Azure
Week 3 — Extend	Identical for both topologies.	Identical for both topologies.
Week 4 — Prove	Identical for both topologies.	Identical for both topologies.

Owners and cadence

The 30-day cadence assumes:

- Daily standup, 15 minutes — platform admin + customer success engineer; daily through Week 1, three times a week in Weeks 2–3, twice a week in Week 4.
- Weekly sync, 60 minutes — platform admin + GRC lead + customer success engineer + executive sponsor (when relevant); end of each week.
- Week exit reviews, 30 minutes each — at the end of each week, before the next week begins; platform admin walks the exit criterion.
- Day 7 executive readout, 60 minutes — executive sponsor + platform admin + GRC lead + customer success engineer; the deployment outcome and Week 2 plan.
- Day 30 executive readout, 60 minutes — same audience; the operating-cadence baseline and the next-quarter plan.

02 · PRE-DAY-0

Final readiness gate.

Day 0 is the kickoff call. Before Day 0, everyone on your side should be ready to execute against the schedule below. Items missed here produce 1–3 days of slip in Week 1; the cumulative cost of pre-Day-0 misses is the single largest source of delay across all Kyūdō implementations. The Quick Start Guide pre-flight checklist covers the same ground at higher level; this section adds the specific items that, if assembled, make a 30-day timeline achievable.

Names and roles

- Executive sponsor named. The decision-maker on framework prioritization, scope tradeoffs, and resource allocation. Available within 24 hours for escalations during the 30 days. Attends the Day 7 and Day 30 readouts.
- Platform admin named. The operational owner for Kyūdō in your environment. Holds tenant-admin scope in Kyūdō RBAC. Has 50–70% of their working time available across Week 1; 30–40% in Week 2; 20–30% in Weeks 3–4.
- GRC lead or compliance officer named. The owner of the framework decision (Day 6, Days 15–21) and the existing-program-absorption work (Week 2). 30–40% of their working time across Weeks 2–4; less in Week 1.
- Identity admin available. Not necessarily dedicated, but available for OAuth consent flows in Days 2–5 and Conditional Access policy review in Day 1–2. Typically 4–6 hours total across the 30 days.
- SOC lead identified (if Sentinel is in scope). Available for the Sentinel integration in Day 4 and the analytic rule review. Typically 2–4 hours total.
- Internal auditor or audit partner identified. The person who will run the internal audit cycle in Week 4. Identified by Day 14 at the latest; engaged Day 22.

Decisions made

- Deployment topology decided. Multi-tenant SaaS or client-hosted Azure. The decision drives the Days 1–2 timeline (hours vs days) and the Bicep prerequisites.
- Subscription and region identified. The Azure subscription Kyūdō will deploy into (client-hosted) or read from (SaaS); the primary and DR regions; data-residency commitments.
- First framework selected. The framework that activates on Day 6. Pick the smallest set that addresses your most immediate external commitment — SOC 2 for SaaS organizations, CMMC for defense, HIPAA for healthcare, ISO 27001 for international, NIST CSF for board-level alignment.
- Second framework identified. Not finalized — final selection is in Week 3 — but narrowed enough that Week 3 selection is a confirmation, not a research project.

- Existing GRC tools inventoried. If migrating, the source platform (Vanta, Drata, OneTrust, ServiceNow GRC, LogicGate) and the artifacts to import (policies, controls, evidence). If greenfield, that is also a valid decision.

Access and credentials

- Tenant identified and accessible. Production tenant for Kyūdō. Platform admin has Global Administrator or equivalent.
- Subscription access. Platform admin has Owner or Contributor on the target subscription (client-hosted) or Reader minimum (SaaS).
- OAuth consent path understood. Whether your tenant requires admin consent for new applications; whether the platform admin can grant consent or needs to coordinate with an identity admin. The single most common Day 1–2 slip is OAuth consent timing.
- Service principal pre-provisioned (client-hosted only). With Contributor at the resource group level, not subscription level. If your service principal creation process takes more than four hours, do this now.
- Key Vault and customer-managed keys identified (optional). If you require customer-managed encryption keys for Kyūdō's storage, identify the Key Vault and keys before deployment.

Documentation gathered

- Existing policies in any form. Information security, access control, incident response, business continuity, vendor management. Any extant Word documents, SharePoint pages, Confluence pages, or markdown files. Imported in Week 2.
- Existing risk register. In any form. Even a spreadsheet from 18 months ago is useful starting material. Imported in Week 2.
- Vendor inventory. List of business associates, subprocessors, security-significant vendors. The current Defender for Cloud Apps inventory is the alternate path if no curated list exists. Bootstrapped in Week 2.
- Most recent audit reports. SOC 2, ISO 27001, CMMC, HIPAA risk analyses, third-party assessments. Useful as both context and prior-state evidence in Week 4.
- BAAs (HIPAA-regulated organizations). The list of business associate agreements signed and the inventory of who is upstream and downstream.

> **Pre-Day-0 self-assessment**
>
> If you can answer yes to all sixteen items above, you are ready for Day 0. If you can answer yes to twelve or more, you are ready and can address the remaining items in Days 1–3 in parallel with deployment. If you can answer yes to fewer than twelve, talk to your customer success engineer about pushing kickoff back several days. Starting Week 1 with significant pre-Day-0 gaps consistently produces a Week 1 that takes 9–10 days instead of 7.

03 · WEEK 1 · DAYS 0–7

Deploy. Connect. Activate the first framework.

Week 1 follows the seven-day arc covered in the Quick Start Guide, with day-by-day operational detail added. By the end of Day 7, the platform is deployed, the seven priority Microsoft integrations are connected, the first framework is activated against live posture, and the executive sponsor has received the first readout. Nothing in subsequent weeks works without Week 1 complete — if Week 1 slips past Day 7, hold the start of Week 2 rather than running them in parallel.

Day 0 — Kickoff

A 90-minute kickoff call sets the schedule. Attendees: executive sponsor, platform admin, GRC lead, customer success engineer.

Activities

- Walk this roadmap document together; confirm pre-Day-0 readiness; agree Week 1 milestones with specific times.
- Set up the shared collaboration channel — Slack or Teams channel with the customer success engineer and named owners.
- Confirm deployment topology, subscription, region; lock in service principal and OAuth consent coordination.

Day 0 deliverables

- Signed deployment plan with Week 1 milestones.
- Shared collaboration channel active.
- Service principal pre-provisioned (client-hosted) or tenant provisioning kicked off (SaaS).

Day 1 — Provision

Day 1 stands up the platform. Tenant provisioning (SaaS) or Bicep deployment (client-hosted).

Activities

- (SaaS) Customer success engineer provisions the tenant in the Kyūdō platform. Customer receives the platform URL via secure channel. Typically completes in hours.
- (Client-hosted) Run `az login`; `az account set --subscription <SUBSCRIPTION_ID>`; verify platform admin can list resources in the target subscription.
- (Client-hosted) Create the resource group: `az group create -n kyudo-prod-rg -l <region>`.
- (Client-hosted) Run the Bicep baseline deployment: `az deployment group create -g kyudo-prod-rg -f kyudo-baseline-deploy-v1.0.bicep -p location=<region> drLocation=<dr-region> environment=prod aksNodeCount=3 aksNodeSize=Standard_D4s_v5`. Typically completes in 30–60 minutes.

- Configure Conditional Access policies for Kyūdō administrative access. Recommended: phishing-resistant MFA required (FIDO2, Windows Hello, certificate-based); compliant device required; geographic restrictions per your policy.
- Create Entra ID groups: Kyūdō-TenantAdmins, Kyūdō-ComplianceOfficers, Kyūdō-PolicyManagers, Kyūdō-RiskManagers, Kyūdō-VendorRiskAnalysts, Kyūdō-Auditors, Kyūdō-Users.

Day 1 deliverables

- Resource group created (client-hosted) or tenant provisioned (SaaS).
- Bicep baseline deployed and outputs captured (client-hosted).
- Conditional Access policies configured.
- Entra ID groups created.

Day 2 — Identity binding and first integration

Day 2 binds Entra ID groups to Kyūdō RBAC, gets the platform admin signed in, validates SLOs, and connects the first integration.

Activities

- (Client-hosted) Verify Bicep outputs. Confirm AKS healthy: `kubectl get pods -A`. Bind private endpoints (SQL, Storage, OpenAI) if not auto-created. Validate via Network Watcher.
- Bind Entra ID groups to Kyūdō RBAC roles. Add platform admin to Kyūdō-TenantAdmins; add GRC lead to Kyūdō-ComplianceOfficers.
- First sign-in. Platform admin opens Kyūdō URL, authenticates with Entra ID, completes MFA. Verify dashboard loads with TenantAdmin scope.
- Validate platform SLOs: API P95 ≤500ms; evidence ingest ≤2s; Light-RAG P95 ≤500ms; HITL threshold 0.7.
- Connect the first Microsoft integration: Microsoft Entra ID. Open Settings > Integrations > Microsoft Entra ID > Set Up. Grant requested OAuth scopes (Directory.Read.All, Policy.Read.All, AuditLog.Read.All, IdentityRiskyUser.Read.All, IdentityRiskEvent.Read.All, AccessReview.Read.All).
- Confirm initial signal flow. Within 15–30 minutes, the Controls Hub begins populating with auto-discovered identity controls; the Evidence Hub registers its first artifacts (Conditional Access policies, sign-in logs, role assignments, access reviews).

Day 2 deliverables

- Platform admin signed in with MFA.
- Platform SLOs validated.
- Entra ID integration connected; first auto-discovered controls visible.
- First evidence artifacts registered.

Day 3 — Defender for Cloud + Defender XDR

Day 3 connects the two highest-leverage Microsoft integrations. Defender for Cloud is the single highest-density integration for control evidence; Defender XDR extends posture across endpoints, email, and identity.

Activities

- Connect Microsoft Defender for Cloud. Settings > Integrations > Defender for Cloud > Set Up. Grant Reader at the subscription level; grant Security Reader for alerts and assessments. Configure ingestion schedule (every 15 minutes for findings, hourly for Secure Score).
- Confirm Defender for Cloud signal flow. The Controls Hub populates with hundreds of new controls (CSPM findings map to controls; Secure Score recommendations become control gaps). The regulatory compliance dashboard data ingests for any framework you have enabled in Defender for Cloud (NIST 800-171, CIS, ISO 27001, etc.).
- Connect Microsoft Defender XDR. Grant Machine.Read.All, Alert.Read.All, Vulnerability.Read.All, AdvancedQuery.Read.All. Configure ingestion schedule.
- Confirm Defender XDR signal flow. Device compliance state, security alerts, vulnerability findings, attack simulation training records all begin populating the Evidence Hub.

Day 3 deliverables

- Defender for Cloud integration connected.
- Defender XDR integration connected.
- Evidence Hub artifact count typically passes 1,000+ by end of day.

Day 4 — Sentinel + Purview

Day 4 connects Sentinel and Purview. Sentinel activates Continuous Monitoring controls; Purview activates Data Security and Privacy controls.

Activities

- Connect Microsoft Sentinel. Settings > Integrations > Sentinel > Set Up. Grant Microsoft Sentinel Reader at the workspace level. Configure ingestion schedule for analytic rules (daily), incidents (hourly), workbooks (daily).
- Walk Sentinel evidence with the SOC lead. Confirm analytic rule definitions are flowing as control evidence; confirm incident records are surfacing in the Evidence Hub with hash, lineage, and confidence score.
- Connect Microsoft Purview. Grant Compliance Manager Reader, DataLossPreventionPolicy.Read.All, InformationProtectionPolicy.Read.All, RecordsManagement.Read.All.
- Confirm Purview signal flow. Sensitivity labels, DLP policies, retention policies, eDiscovery records populate. Compliance Manager assessments cross-reference with Kyūdō's own Controls Hub view.

Day 4 deliverables

- Sentinel integration connected.
- Purview integration connected.
- Continuous Monitoring controls populated; Data Security and Privacy controls populated.

Day 5 — Azure Policy + Graph API

Day 5 connects the two final Microsoft integrations. Azure Policy and Resource Graph activate Configuration controls; Microsoft Graph API extends M365 coverage.

Activities

- Connect Azure Policy + Resource Graph. Grant Azure Policy Reader and Azure Resource Graph Reader at the subscription level. Reader is required as baseline.
- Confirm Azure Policy signal flow. Policy compliance state, baseline enforcement evidence, drift detection at the resource level all populate. Configuration controls auto-discover.
- Connect Microsoft Graph API (M365). Grant AuditLog.Read.All. Confirm M365 Unified Audit Log ingestion; mailbox configuration; SharePoint policy state; Teams compliance settings.
- End-of-day check: all seven priority Microsoft integrations connected. Controls Hub typically shows 200–500 auto-discovered controls; Evidence Hub holds thousands of artifacts.

Day 5 deliverables

- Azure Policy + Resource Graph connected.
- Microsoft Graph API connected.
- All seven priority Microsoft integrations operational.

Day 6 — First framework activation

Day 6 is when Kyūdō's value proposition becomes operational. 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 2–5 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.

Activities

- 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.
- Activate the framework in the Controls Hub. The CMCAE recalculates control completeness against the activated framework's specific requirements; STRM mapping populates.
- Walk the Controls Hub view filtered to the activated framework. Identify control gaps (controls scored below 50% completeness). Review with GRC lead. Produce the gap list.
- 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.

Day 6 deliverables

- 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 a 60-minute executive readout. Audience: executive sponsor + platform admin + GRC lead + customer success engineer. The readout is a demonstration of the new operating cadence, not a status update.

Agenda

1. Posture clarity dashboard — control completeness across the activated framework; trajectory since Day 1; identified gaps. (10 minutes)
2. Evidence summary — total artifacts collected; coverage by control category; sample audit-defensible evidence walked end-to-end with hash, lineage, and confidence score. (15 minutes)
3. Risk surface — initial risk register derived from observed posture; treatment recommendations; trajectory. (10 minutes)
4. Trust Center demonstration — what your customers, auditors, and regulators will see when they request transparency on your posture. (10 minutes)
5. Week 2 plan — absorbing the existing GRC program; activating any second framework. (15 minutes)

Day 7 deliverables

- Executive readout delivered.
- Week 1 exit criterion met: platform operational; 7 Microsoft integrations connected; first framework mapped against live posture.
- Week 2 plan agreed; Week 2 begins Day 8.

04 · WEEK 2 · DAYS 8–14

Absorb the existing GRC program.

Week 2 transforms Kyūdō from ‘evidence-collection layer over the Microsoft estate’ to ‘system of record for governance.’ The Microsoft integrations are doing the heavy lifting on automated evidence; this week brings in the human-authored material your existing program has produced: policies, the risk register, the vendor inventory, the Trust Center configuration. By the end of Week 2, Kyūdō holds the artifacts your auditors, regulators, and customers will reference.

Day 8 — Kick off Week 2; Policy Center bootstrap

Day 8 starts the program-absorption work. Platform admin + GRC lead are the primary owners. Most of Week 2's hours land on the GRC lead, not the platform admin.

Activities

- Inventory existing policies. Information security policy, access control policy, incident response plan, business continuity plan, vendor management policy, data classification policy, change management policy, acceptable use policy. List each with location and last-modified date.
- Open Policy Center. Use the bulk-import workflow to upload the inventoried policies. Each policy is parsed; the AI proposes which controls the policy governs; confidence scores per mapping.
- Review proposed control mappings. Confirm or adjust. Below 0.7 confidence, the AI flags for human review (HITL threshold).
- Identify policy gaps. Which controls have no governing policy? The Policy Center surfaces these as Policy Gaps; they will drive Week 2 net-new authoring.

Day 8 deliverables

- Policy inventory complete.
- Existing policies imported into Policy Center.
- Initial control-to-policy mapping reviewed.
- Policy gap list produced.

Day 9 — Policy authoring and gap closure

Day 9 closes the most material policy gaps. The Policy Center's AI authoring drafts new policies cited to the controls they govern; the GRC lead reviews and approves.

Activities

- For each policy gap on the list, decide: author net-new (most common), update existing (if a related policy can be extended), or accept the gap (rare; requires documented rationale).

- AI-author net-new policies. The Policy Center generates a draft grounded in the controls it will govern, with citations. GRC lead reviews and edits as needed.
- For updated policies, update the existing version in Policy Center. The system tracks revision history.
- Configure policy review cadence. Annual is typical; some policies (incident response, business continuity) benefit from more frequent review.

Day 9 deliverables

- Material policy gaps closed.
- Net-new policies authored, reviewed, approved.
- Policy review cadence configured.

Day 10 — Risk register normalization

Day 10 brings the existing risk register into the Risk Management module. Most organizations have a risk register in some form — even a spreadsheet — and even a stale register provides useful starting material.

Activities

- Export existing risk register from current source (Vanta, Drata, Excel, ServiceNow GRC, LogicGate, custom). The Risk Management module imports CSV directly; for native GRC platforms, the customer success engineer typically provides a migration template.
- Walk imported risks. Each risk is normalized into a typed entity in the Knowledge Graph: category, likelihood, impact, current treatment, residual risk.
- Link risks to controls. The AI proposes mappings (‘this risk is mitigated by these controls’); GRC lead confirms or adjusts.
- Link controls to evidence. The auto-discovered evidence from Week 1 already attests to many of the linked controls; residual risk recalculates against live evidence.
- Identify risks without mitigating controls and risks without supporting evidence. These become the Week 2 risk-treatment work.

Day 10 deliverables

- Existing risk register imported.
- Risks linked to controls.
- Controls linked to evidence.
- Residual risk baseline established.

Day 11 — Vendor inventory bootstrap

Day 11 brings the vendor inventory into the VRM module. Vendors are auto-discovered from Defender for Cloud Apps (connected Day 3) but a curated inventory accelerates the work.

Activities

- Reconcile auto-discovered vendors against your curated list. The auto-discovery typically captures cloud applications and SaaS vendors; the curated list adds non-SaaS vendors (consulting, professional services, infrastructure providers, payroll, etc.).
- For each vendor, set tier and risk classification. Critical vendors (high data access or operational dependency) get full continuous monitoring; tier-2 vendors get periodic re-assessment; tier-3 vendors get annual review.
- Import existing vendor questionnaires (if any). The VRM module retains the artifacts and links them to the vendors.
- Configure questionnaire automation. Inbound questionnaires are pre-filled by the AI from existing evidence with citations and confidence scores.

Day 11 deliverables

- Vendor inventory reconciled.
- Vendor tiers and risk classifications set.
- Existing questionnaires imported.
- Inbound questionnaire automation configured.

Day 12 — Trust Center configuration

Day 12 configures the Trust Center for external visibility. The Trust Center replaces the security questionnaire mill that consumes weeks of GRC time per quarter.

Activities

- Decide Trust Center publication scope. Public posture (what every visitor sees), authenticated posture (what registered prospects see), customer posture (what active customers see). Typical pattern: framework certifications and high-level posture public; detailed evidence and per-control mappings authenticated.
- Configure the headline content: framework activated in Week 1 as the headline posture artifact; trust badges; data residency statement; subprocessor list; security contact.
- Walk the customer view. The Trust Center is what your customers and prospects will see; the GRC lead and the sales engineering team review together.
- Configure access controls. Who at customer organizations can access the authenticated view; how access is granted and revoked.

Day 12 deliverables

- Trust Center publication scope decided.
- Headline content configured.
- Customer view reviewed and approved.
- Access controls configured.

Day 13 — Week 2 consolidation

Day 13 consolidates the week's work and addresses any items that surfaced during the absorption activities.

Activities

- Walk the Knowledge Graph view filtered to the activated framework. Confirm policies are aligned to controls, controls have evidence, risks are linked to controls, vendors are tracked.
- Address residual program gaps. Any policy mapped to no controls; any control with no policy; any risk with no mitigating control; any vendor with no risk classification.
- Capture Week 2 lessons. What surprised you? What was harder than expected? What was easier? Customer success engineer captures the input for product feedback.

Day 13 deliverables

- Knowledge Graph integrity verified.
- Residual program gaps addressed.
- Lessons captured.

Day 14 — Week 2 exit review

Day 14 closes the week with the Week 2 exit review. Platform admin + GRC lead + customer success engineer; 30 minutes.

Activities

- Walk the Week 2 exit criterion: policies aligned to controls; risks linked to controls and evidence; vendors under continuous monitoring; Trust Center serving inbound questionnaires.
- Confirm the framework selection for Week 3 (the second framework). The pre-flight checklist narrowed the candidates; this is the final lock-in.
- Identify the internal auditor or audit partner for Week 4 if not already named.
- Schedule the Day 30 executive readout. 60 minutes; same audience as Day 7.

Day 14 deliverables

- Week 2 exit criterion met.
- Second framework decision locked in.
- Internal auditor identified.
- Day 30 readout scheduled.

05 · WEEK 3 · DAYS 15–21

Extend coverage. Activate additional frameworks.

Week 3 activates the second framework. Subsequent frameworks activate faster than the first because the control set is already populated, the evidence is already flowing, and STRM mapping crosswalks the existing controls to the new framework's specific requirements. Most customers find that the second framework activates in 1–2 days rather than the 4–5 days the first framework required.

Week 3 also connects non-Microsoft sources where in scope: AWS, Google Cloud, Kubernetes, GitHub, Oracle Cloud Infrastructure. Each follows the same five-stage workflow as the Microsoft integrations with the appropriate authentication mechanism.

Day 15 — Second framework activation

Day 15 activates the second framework against the same control set populated in Week 1. The activation is a Controls Hub configuration change — the underlying evidence does not need to be re-collected.

Activities

- Activate the second framework in the Controls Hub. CMCAE recalculates control completeness against the new framework's specific requirements; STRM mapping populates the framework-specific control IDs.
- Walk the Controls Hub view filtered to the second framework. Compare the gap list to the first framework's gap list — most gaps overlap because the underlying control coverage is the same.
- Identify gaps unique to the second framework. These typically reflect framework-specific requirements (e.g., CMMC's six non-POA&M-eligible 1-point controls; HIPAA's specific Risk Analysis structure; ISO 27001's SoA mechanics).
- Walk the Evidence Hub view for the second framework. Spot-check evidence per control.

Day 15 deliverables

- Second framework operational.
- Cross-framework gap analysis complete.
- Framework-specific gaps logged.

Days 16–17 — Cross-framework consolidation

Days 16–17 consolidate the cross-framework view. The Knowledge Graph holds one control set; multiple frameworks read from it; gaps that satisfy one framework's requirement automatically satisfy the others where STRM crosswalks hold.

Activities

- Walk the cross-framework view in the Controls Hub. The same evidence attests against multiple frameworks; the same control-completeness scoring applies; the same residual risk calculation.
- Address any framework-specific gaps that affect multiple frameworks. Typically these are high-leverage — fixing one gap moves multiple framework completeness scores upward.
- Configure framework-specific reporting. Each framework gets its own audit-ready evidence package view; the Trust Center's framework selector exposes the right view to the right audience.
- If a third framework is in scope, repeat Day 15 activities for the third framework. Most customers stop at two frameworks in the first 30 days; some customers (typically multi-regulated organizations) push to three.

Days 16–17 deliverables

- Cross-framework view consolidated.
- High-leverage cross-framework gaps addressed.
- Framework-specific reporting configured.
- Third framework activated (if in scope).

Days 18–20 — Non-Microsoft sources

Days 18–20 connect non-Microsoft sources where in scope. Most customers have at least one non-Microsoft source: GitHub for code repositories; AWS or GCP for non-Microsoft cloud workloads; Kubernetes for container workloads; Oracle Cloud for legacy infrastructure.

Activities

- Identify non-Microsoft sources to connect. Priority order: GitHub (most common), AWS or GCP (where workloads exist), Kubernetes (if workloads run there), Oracle Cloud (where legacy systems exist).
- Connect each source via Settings > Integrations. Each follows the five-stage workflow with appropriate authentication: GitHub App for GitHub; IAM access key + secret for AWS; service account JSON for GCP; cluster-bound service account or managed identity for Kubernetes; OCI API key for Oracle.
- Confirm signal flow. Each source produces evidence in the Evidence Hub, populates additional auto-discovered controls in the Controls Hub, and surfaces additional findings in Risk Management.
- Update the cross-framework view. Non-Microsoft signals satisfy framework requirements that Microsoft sources cannot reach.

Days 18–20 deliverables

- Non-Microsoft sources connected.
- Cross-source evidence populated.
- Cross-framework view updated.

Day 21 — Week 3 exit review

Day 21 closes Week 3.

Activities

- Walk the Week 3 exit criterion: 2–4 frameworks operational; same evidence satisfying multiple frameworks via STRM; non-Microsoft sources connected where applicable.
- Confirm the lead framework for the Week 4 internal audit cycle. Typically the most-mature framework (the one activated Day 6); occasionally a secondary framework if it has a more imminent external commitment.
- Brief the internal auditor on the Week 4 plan. Walk the platform; introduce the Evidence Hub view they will use; agree the audit scope.

Day 21 deliverables

- Week 3 exit criterion met.
- Lead framework for internal audit confirmed.
- Internal auditor briefed.

06 · WEEK 4 · DAYS 22–30

Prove the operating model. First internal audit cycle.

Week 4 is the proving ground. Run an internal audit cycle against the lead framework. Have your internal auditor (or an external audit partner) use Kyūdō as if they were the external assessor: pull evidence per control, verify control operation, document the audit trail. The cycle is not a dress rehearsal — it is a real audit, with real findings, against real evidence.

If the cycle succeeds — evidence is current, controls are mapped, the audit trail is defensible — the platform is operational for that framework. If the cycle surfaces gaps — missing evidence, mapping inconsistencies, integration gaps — work the gaps with your customer success engineer in real time. The cycle is meant to surface issues now, not in the external audit three months from now.

Days 22–23 — Internal audit cycle: walk-through

Days 22–23 are the audit walk-through. The internal auditor opens Kyūdō and traverses the Evidence Hub end-to-end.

Activities

- Internal auditor opens Kyūdō with the Auditor RBAC role (read-everything plus annotation; no modification).
- Walk control by control through the lead framework. For each control: confirm the implementation description, spot-check the evidence, verify the lineage and confidence score, annotate any concerns.
- Document any findings. A finding is a control where the evidence does not support the implementation description, or where the evidence is missing, or where the confidence score is below the audit threshold.
- For each finding, work with the GRC lead and platform admin in real time to determine: is this an evidence-collection gap (fixable in the platform), an implementation gap (fixable through control remediation), or a documentation gap (fixable through SSP / policy update)?

Days 22–23 deliverables

- Audit walk-through complete.
- Findings logged with categorization.
- Real-time remediation initiated for evidence-collection gaps.

Days 24–25 — Findings remediation

Days 24–25 work the findings. Most findings remediate within these two days because the platform was already producing the evidence; the issue was usually how the evidence was surfaced.

Activities

- Evidence-collection gaps: typically fixed by adjusting the integration scope, the data ingestion schedule, or the control-to-evidence mapping. Customer success engineer assists in real time.
- Implementation gaps: typically require coordination with the technical team that owns the control. Logged in Risk Management with a remediation owner and timeline; deferred where appropriate.
- Documentation gaps: typically require a Policy Center update or an SSP entry. Authored or edited inline.
- Re-walk remediated controls with the internal auditor. Confirm the finding is closed.

Days 24–25 deliverables

- Evidence-collection gaps closed.
- Implementation gaps logged with remediation plan.
- Documentation gaps closed.
- Remediated controls re-walked and verified.

Days 26–27 — Audit report and trajectory

Days 26–27 produce the audit report and update the program trajectory.

Activities

- Internal auditor produces the formal audit report. Findings; remediation; residual gaps; recommendations. The report is itself an artifact in the Evidence Hub for future reference.
- GRC lead updates the risk register based on findings. New risks added; existing risks adjusted; risk trajectory updated.
- Platform admin updates the Trust Center to reflect the post-audit posture. The framework's compliance status is current as of the internal audit date.
- Schedule the next external audit if relevant. The internal audit's outcome informs whether the organization is ready for an external audit; if ready, the booking happens now.

Days 26–27 deliverables

- Internal audit report produced.
- Risk register updated.
- Trust Center updated.
- External audit scheduled (if applicable).

Days 28–29 — Operating cadence preparation

Days 28–29 prepare the post-Day-30 operating cadence. The first 30 days have been intensive; the steady-state cadence is materially lighter.

Activities

- Document the operating cadence. Daily: Sentinel alerts review (5 minutes by SOC). Weekly: Controls Hub posture review (20 minutes by GRC lead). Monthly: cross-framework posture and risk register review (60 minutes; GRC lead + platform admin). Quarterly: external Trust Center review with sales engineering (30 minutes).
- Configure the alerting that drives the cadence. Defender for Cloud regulatory compliance regression alerts; control-completeness drop below threshold alerts; risk-trajectory inflection alerts; vendor posture alerts.
- Plan the next 90 days. Which frameworks to add (the third or fourth); which non-Microsoft sources to connect; which existing programs (if any) to retire as Kyūdō becomes the system of record.
- Prepare the Day 30 executive readout deck. Use the Kyūdō executive dashboard as the foundation — the readout is built from queries over the Knowledge Graph, not assembled from disparate sources.

Days 28–29 deliverables

- Operating cadence documented.
- Alerting configured.
- Next-90-days plan drafted.
- Day 30 readout deck prepared.

Day 30 — Executive readout

Day 30 closes the month with the senior-stakeholder readout. Audience: executive sponsor + platform admin + GRC lead + customer success engineer + (optionally) board liaison or audit committee chair. 60 minutes.

Agenda

1. Posture clarity — control completeness across all activated frameworks; trajectory since Day 1; current gap list. (10 minutes)
2. Internal audit outcome — the audit report; findings; remediation; residual gaps. The single most important slide for the executive sponsor. (15 minutes)
3. Risk surface — the risk register against live evidence; residual risk trajectory; treatment recommendations. (10 minutes)
4. Trust Center demonstration — the post-audit external posture; questionnaire automation in operation; customer-facing transparency. (10 minutes)
5. Operating cadence — the post-Day-30 rhythm; next-90-days plan; the framework or program ambitions for Q2. (15 minutes)

Day 30 deliverables

- Day 30 executive readout delivered.
- Operating cadence agreed.
- Next-90-days plan approved.
- Engagement transitions to steady-state operation.

After Day 30

The first 30 days establish the platform, absorb the existing program, prove the operating model through an internal audit cycle, and set the steady-state cadence. Beyond Day 30, 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 Trust Center serves inbound questionnaires; the framework guide series at kyudo.ai/guides is your ongoing reference for whatever specific compliance regime you are operating against.

The marginal cost of maintaining compliance, supporting external audits, and adding cross-framework coverage approaches zero. If at any point that drag returns, talk to your customer success engineer — the platform is designed to keep operational drag low, and most issues that produce drag are configurable. Most resolve in a 30-minute call.

APPENDIX A · DAILY ACTIVITY MATRIX

All 30 days, consolidated.

The full 30-day schedule in a single matrix. Use it to populate your project tracker, brief stakeholders, and validate that no day is over- or under-loaded.

Day	Phase	Activity	Owner
0	Kickoff	90-minute kickoff call; signed deployment plan; collaboration channel active.	All
1	Deploy	Resource group; Bicep baseline (client-hosted) or tenant provisioning (SaaS); Conditional Access; Entra ID groups.	Platform admin
2	Deploy	Identity binding; first sign-in with MFA; SLO validation; Entra ID integration connected.	Platform admin
3	Connect	Defender for Cloud + Defender XDR connected; Evidence Hub passes 1,000+ artifacts.	Platform admin
4	Connect	Sentinel + Purview connected; Continuous Monitoring and Data Security controls populated.	Platform admin + SOC lead
5	Connect	Azure Policy + Resource Graph + Microsoft Graph API connected; all 7 Microsoft integrations operational.	Platform admin
6	Activate	First framework activated; Controls Hub view; gap list; Trust Center configured.	Platform admin + GRC lead
7	Readout	Day 7 executive readout; Week 1 exit criterion confirmed.	All
8	Absorb	Policy inventory; Policy Center bulk import; control-to-policy mapping; policy gap list.	GRC lead
9	Absorb	Policy authoring; policy gap closure; policy review cadence configured.	GRC lead
10	Absorb	Risk register normalization; risks linked to controls; controls linked to evidence.	GRC lead
11	Absorb	Vendor inventory bootstrap; tier and risk classification; questionnaire automation configured.	GRC lead + VRA
12	Absorb	Trust Center configuration; publication scope;	GRC lead +

Day	Phase	Activity	Owner
		access controls.	Sales Engineering
13	Absorb	Knowledge Graph integrity check; residual program gap closure.	Platform admin + GRC lead
14	Readout	Week 2 exit review; second framework decision; internal auditor identified.	Platform admin + GRC lead
15	Extend	Second framework activated; cross-framework gap analysis; framework-specific gap log.	Platform admin + GRC lead
16–17	Extend	Cross-framework consolidation; high-leverage gap closure; framework-specific reporting.	Platform admin + GRC lead
18–20	Extend	Non-Microsoft sources connected (GitHub, AWS, GCP, Kubernetes, OCI as in scope).	Platform admin
21	Readout	Week 3 exit review; lead framework for internal audit confirmed; internal auditor briefed.	Platform admin + GRC lead
22–23	Prove	Internal audit walk-through; findings logged; categorization; real-time remediation initiated.	Internal auditor + GRC lead
24–25	Prove	Findings remediation; evidence-collection gaps closed; documentation gaps closed.	Platform admin + GRC lead
26–27	Prove	Audit report; risk register update; Trust Center update; external audit scheduled (if applicable).	Internal auditor + GRC lead
28–29	Prove	Operating cadence documented; alerting configured; next-90-days plan drafted; Day 30 deck prepared.	Platform admin + GRC lead
30	Readout	Day 30 executive readout; operating cadence agreed; engagement transitions to steady-state.	All

APPENDIX B · OWNER PLAYBOOK

What each role does, week by week.

Roles can be confused with personas. The matrix below reads roles as the person executing the activity — multiple roles may map to the same person in smaller organizations, and large organizations may distribute roles across teams.

Platform admin

Week	Primary activities
1	Bicep deployment; identity binding; Microsoft integration connections; SLO validation. Heaviest week — 50–70% of working time.
2	Knowledge Graph integrity verification; technical support for Policy Center / Risk Management / VRM imports. 30–40% of working time.
3	Second framework activation; non-Microsoft source connections; cross-framework reporting configuration. 20–30% of working time.
4	Internal audit support (technical findings remediation); operating cadence configuration; alerting setup. 20–30% of working time.

GRC lead / compliance officer

Week	Primary activities
1	Day 0 kickoff attendance; framework selection confirmation Day 6; gap list review. Lighter week — 10–20% of working time.
2	Policy import and authoring; risk register normalization; vendor classification; Trust Center configuration. Heaviest week — 40–60% of working time.
3	Second framework gap analysis; cross-framework consolidation; non-Microsoft source coordination. 30–40% of working time.
4	Internal audit cycle coordination; findings remediation; risk register update; Day 30 readout preparation. 40–50% of working time.

Executive sponsor

Week	Primary activities
1	Day 0 kickoff (90 min); Day 7 executive readout (60 min); ad-hoc decisions.

Week	Primary activities
	Total time: 2–3 hours.
2	Available for escalations; decision input on framework selection if needed. Total time: 1–2 hours.
3	Available for escalations; decision input on framework or scope adjustments. Total time: 1–2 hours.
4	Day 30 executive readout (60 min); next-90-days plan approval. Total time: 1–2 hours.

Identity admin (extended role)

Week	Primary activities
1	OAuth consent flows for Microsoft integrations; Conditional Access policy review; Entra ID group provisioning. 4–6 hours total.
2	OAuth consent for non-Microsoft sources if connected early. 1–2 hours.
3	OAuth consent for any remaining sources. 1–2 hours.
4	Available for any access-related findings remediation. As needed.

SOC lead (where Sentinel is in scope)

Week	Primary activities
1	Day 4 Sentinel integration walk-through; analytic rule confirmation. 2–4 hours.
2	Available for Sentinel-related questions during program absorption. 1 hour.
3	Sentinel coverage adjustments for second framework if needed. 1–2 hours.
4	Internal audit support for Sentinel-derived evidence. 1–2 hours.

Internal auditor

Week	Primary activities
1–3	Identification by Day 14; briefing by Day 21. Light involvement.
4	Internal audit walk-through (Days 22–23); findings re-walk (Days 24–25); audit report (Days 26–27). 16–20 hours total.

APPENDIX C · SUCCESS CRITERIA & ESCALATION

Exit criteria, success markers, and when to escalate.

Exit criteria per week

Week	Exit criterion
1 — Days 0–7	Platform operational; 7 Microsoft integrations connected; first framework mapped against live posture; Day 7 readout delivered. Verifiable: platform admin signs in with MFA; Entra ID + Defender for Cloud + Defender XDR + Sentinel + Purview + Azure Policy + Graph API all show 'Connected'; the Controls Hub shows the activated framework with completeness scoring; the Day 7 readout slides exist.
2 — Days 8–14	Policies aligned to controls; risks linked to controls and evidence; vendors under continuous monitoring; Trust Center serving inbound questionnaires. Verifiable: Policy Center shows imported policies with control mappings; Risk Management shows the imported risk register with control links; VRM shows the vendor inventory with tier and risk classification; the Trust Center is accessible to authenticated customers.
3 — Days 15–21	2–4 frameworks operational; same evidence satisfying multiple frameworks via STRM; non-Microsoft sources connected where applicable. Verifiable: Controls Hub shows multiple framework views; the cross-framework view demonstrates STRM crosswalks; non-Microsoft sources show 'Connected' status.
4 — Days 22–30	Internal audit cycle complete; findings (if any) logged and remediated; Day 30 readout delivered; weekly/monthly operating cadence agreed. Verifiable: the audit report exists; Risk Management shows updated risks; Trust Center reflects post-audit posture; the cadence document is signed.

Success markers (in addition to exit criteria)

- Day 7 — the Evidence Hub holds 1,000+ artifacts with hash, lineage, and confidence score per artifact.
- Day 14 — the Knowledge Graph is queryable end-to-end: a single question ('what evidence supports control AC.L2-3.1.1?') returns a single answer with sources.
- Day 21 — a customer security questionnaire (real or simulated) is pre-filled by the Trust Center with at least 70% confidence-scored answers.
- Day 30 — the executive sponsor can describe the operating cadence in their own words without reference to the readout deck.

When to escalate

Trigger	Escalation path
Phase 1 (Day 1–3) deployment fails to complete by Day 3	Customer success engineer escalates to Kyūdō platform engineering. Hold Phase 2 until resolved.
OAuth consent for a Microsoft integration cannot be granted	Identity admin + customer success engineer; if blocked, executive sponsor for organizational override.
Framework decision drifts past Day 5	Customer success engineer flags to executive sponsor in writing; without the decision, Day 6 framework activation cannot happen.
Existing GRC migration produces unexpected complexity (Week 2)	Customer success engineer engages Kyūdō migration team; consider extending Week 2 by 2–3 days rather than compressing the activities.
Internal audit produces material findings that cannot be remediated in Days 24–25	Document as Open Findings in Risk Management with remediation plan; proceed to Day 30 readout with the open list. The cycle is meant to surface this material; do not delay readout to close everything.
Day 30 executive readout cannot be scheduled	Customer success engineer flags to platform admin and GRC lead by Day 25 at the latest; reschedule with executive sponsor immediately.