Kyūdō

SOVEREIGNTY-GRADE AI · GRC

User Onboarding Checklist

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

You have one hour. Let’s get you working.

Welcome to Kyūdō. Your Tenant Admin has provisioned you with a role on the platform, and you have either received a welcome email with a sign-in link, or your administrator has shared the platform URL with you directly. This checklist gets you from first sign-in to operational — doing real work in the role you have been assigned — in roughly one hour.

This is a working checklist, not background reading. Each phase has a small number of concrete steps; check them off as you complete them. By the end, you will be signed in, your profile will be set up, you will know where to find what you need, and you will have completed at least one real task in your role. The platform is designed for the rest to be self-evident from there.

How to use this checklist

Five phases, in order. Phases 1–3 are universal — everyone signs in, sets up a profile, gets oriented. Phase 4 is role-specific — jump to the section that matches your role. Phase 5 is what to expect after Day 1, so you know the rhythm of regular use. Each phase takes 10–20 minutes.

Phase	What you do	Time
1 — Sign in	Authenticate with Microsoft Entra ID, complete MFA, confirm your role.	5–10 minutes
2 — Set up profile	Add your display name, photo, notification preferences, time zone.	5–10 minutes
3 — Get oriented	Walk the dashboard, find your queue, locate help and support.	10–15 minutes
4 — First role tasks	Complete one or two real tasks in your role to confirm the platform works for you.	20–30 minutes
5 — Daily cadence	Understand what to expect in regular weekly use after Day 1.	5 minutes (read-only)

Before you start

You will need: your work device with a current browser, your Microsoft 365 credentials, and your MFA method (authenticator app, FIDO2 key, Windows Hello). If you do not know which role you have been assigned, ask your Tenant Admin before you start — Phase 4 changes based on it.

First sign-in and profile setup are easier on a desktop or laptop. Subsequent daily use works on any device.

01 · PHASE 1 · SIGN IN

Authenticate. Confirm your role.

Kyūdō uses Microsoft Entra ID for sign-in. Your existing work credentials — the same ones you use for Microsoft 365, Teams, Outlook — are the only credentials you need. There is no separate Kyūdō password to remember. If your organization uses Conditional Access policies (most do), you may be prompted to confirm your device is compliant or use a phishing-resistant MFA method.

Steps

- Open the Kyūdō platform URL in your browser. Your Tenant Admin shared this URL in your welcome email; if you cannot find it, ask them. The URL is typically of the form `kyudo.your-organization.com` or `your-organization.kyudo.app`.
- Click Sign in with Microsoft. You will be redirected to your organization's Microsoft Entra ID sign-in page. This is the same sign-in flow you use for any other Microsoft 365 application.
- Enter your work email address and your Microsoft password.
- Complete multi-factor authentication when prompted. Use the MFA method your organization has configured — typically Microsoft Authenticator approval, FIDO2 security key, Windows Hello biometric, or certificate-based authentication.
- If your organization's Conditional Access policy requires it, confirm device compliance. Your device must be enrolled in Intune (or your organization's mobile device management) and meet the security baseline.
- Accept any first-time consent prompts. If this is your first time signing into Kyūdō, you may see a prompt asking you to consent to the application reading your basic profile information. This is read-only and required to map your Entra ID identity to your Kyūdō role.
- Land on the Kyūdō dashboard. You should see the home screen with the navigation menu on the left and your role indicator in the top-right corner of the screen.

> **You will know it worked when...**
>
> Your name and role appear in the top-right corner of the screen. The role indicator reflects what your Tenant Admin assigned you — Tenant Admin, Compliance Officer, Policy Manager, Risk Manager, Vendor Risk Analyst, Auditor, or General User. If the role does not match what your Tenant Admin told you, do not change anything yourself — contact them directly to verify the Entra ID group assignment.

If something goes wrong

Symptom	What to try
"Sign in failed" or "Access	Verify with your Tenant Admin that you have been added

Symptom	What to try
denied”	to a Kyūdō Entra ID group. Common groups: Kyudo_ComplianceOfficer, Kyudo_PolicyManager, Kyudo_RiskManager. Group changes can take up to 30 minutes to propagate.
MFA prompt does not appear	Open Microsoft Authenticator (or your MFA app) directly. Some Conditional Access policies push the MFA notification rather than displaying it inline; checking the app may surface the request.
“Device not compliant” message	Open the Microsoft Intune Company Portal (or your organization’s device-compliance app) and confirm your device check-in is current. Some compliance evaluations refresh on a schedule — a manual sync usually resolves it.
No role indicator appears	Sign out completely, close your browser, and sign in again. Token claims occasionally lag the first time a new user is provisioned. If this persists for more than 30 minutes, contact your Tenant Admin.
Cannot find the platform URL	Check your work email inbox (and spam folder) for the Kyūdō welcome message. If you cannot find it, ask your Tenant Admin to resend it.

02 · PHASE 2 · SET UP YOUR PROFILE

Five fields. One photo. Done.

Your Kyūdō profile drives how the platform addresses you, when it notifies you, and which time zone it uses to schedule recurring activities. Most fields inherit from your Microsoft Entra ID profile; you only need to confirm or override a small number.

Steps

- Click your role indicator in the top-right corner. Select Profile from the dropdown menu.
- Confirm your display name. This is inherited from Entra ID and is read-only if your organization has Entra-controlled profiles enabled. If editable, set it to how you want colleagues and external auditors to see you.
- Add a profile photo (optional but recommended). The photo helps colleagues recognize you in workflow approvals and audit annotations. Square images at 256x256 pixels or larger work best.
- Set your time zone. This determines when scheduled tasks fire, when reminders are sent, and how dates display in audit logs. Default is your tenant's configured time zone; override if you are in a different region.
- Set your notification preferences. Choose how you want to be notified: email (default), in-app only, Microsoft Teams (if integrated), or all. Notifications include workflow assignments, approval requests, evidence-collection reminders, and posture-change alerts.
- Set your communication language (if multi-language is enabled). Default is your browser's preferred language; override if needed.
- Save your changes. The Save button is at the bottom of the profile panel.

> **You will know it worked when...**
> Your photo appears in the top-right corner of the screen, replacing the default initials avatar. Your display name is visible on hover. The notification preferences you set govern how the platform contacts you for the rest of your tenure.

Notification recommendations by role

These are starting points; adjust as you learn how active your role is.

Role	Recommended notification mix
Tenant Admin	Email + in-app. You will receive integration health alerts, user provisioning events, and platform-level posture changes.
Compliance Officer	Email + in-app. You will receive workflow assignments, evidence-

Role	Recommended notification mix
	collection reminders, and framework-status updates.
Policy Manager	In-app + Teams (if integrated). You will receive policy review requests, approval notifications, and gap-analysis flags.
Risk Manager	Email + in-app. You will receive risk-trajectory inflection alerts, treatment-overdue notifications, and board-cycle reminders.
Vendor Risk Analyst	Email + Teams (if integrated). You will receive vendor questionnaire arrivals, posture-change alerts, and renewal reminders.
Auditor	Email only. You will receive engagement-start notifications and report-due reminders. No real-time alerts.
General User	In-app only. You will receive task assignments and the occasional informational notification.

03 · PHASE 3 · GET ORIENTED

Find your way around. Find your queue.

Kyūdō is built around six modules connected through a shared Knowledge Graph. The modules you can see and use depend on your role; everyone sees the dashboard. Spend ten to fifteen minutes walking the platform before you start your first real task. Familiarity now saves time later.

The dashboard

Your home screen. The dashboard surfaces the items most relevant to your role: tasks assigned to you, items awaiting your review, recent activity, and any alerts that require attention. The top of the dashboard shows your role-specific Posture Summary; the middle shows your Action Queue; the bottom shows Recent Activity.

The navigation menu

On the left side of every screen. Six modules appear in the order they are most commonly used; modules you do not have access to appear grayed out or hidden, depending on your tenant's configuration.

Module	What you find here
Controls Hub	Every control in your environment, mapped to the frameworks that govern it. Filter by framework, by status, by completeness score.
Evidence Hub	Every evidence artifact — logs, screenshots, configuration exports, attestation records — with hash, lineage, and confidence score on each.
Policy Center	Your policy library. Drafts, approved policies, scheduled reviews, gap analyses against the controls each policy governs.
Risk Management	Your risk register. Risks linked to controls, treatment status, residual exposure trajectory, board-ready dashboard views.
Vendor Risk Management	Your vendor inventory. Tier classifications, continuous posture monitoring, questionnaire automation, vendor-specific risk trajectories.
Trust Center	Your customer-facing transparency portal. Manage what external stakeholders see; respond to inbound questionnaires.

Your action queue

The most important screen for daily use. Your Action Queue holds every item assigned to you that requires action: workflow assignments, approval requests, evidence-collection tasks, review reminders, escalations. Items are prioritized by deadline; overdue items surface in red.

Walk to the queue now. Even if it is empty on Day 1, knowing where it is and how it is organized saves you from missing your first assignment.

Help and support

Three places to go for help, in increasing order of escalation.

- In-product help. Click the question mark icon in the top-right corner; a contextual help panel opens with help for whatever screen you are on. Articles, walkthroughs, and short videos.
- Your Tenant Admin. The person inside your organization who provisioned you. They know your tenant's configuration, your framework selection, and your team's working patterns. Most questions are answered fastest here.
- Kyūdō customer success. For issues that go beyond your tenant configuration. Your Tenant Admin can route you, or you can reach out at hello@kyudo.ai.

> **You will know it worked when...**
> You can find each of the six modules from memory, you have located your Action Queue, and you know how to open in-product help. You do not need to know how to use every module — you only need to know where to find them.

04 · PHASE 4 · YOUR FIRST TASKS

One or two real tasks. Confirm the platform works for you.

Phase 4 is role-specific. Find your role below; complete the suggested first tasks. The goal is to do real work, not training simulation — every task in this phase produces output that is useful to your team.

If you cannot find your role, check your role indicator in the top-right corner. If your role does not match anything below, you are likely a General User — see the General User card at the end of this section.

PHASE 4 · TENANT ADMIN

Tenant Admin — first tasks

As Tenant Admin, you manage your organization's tenant: users, integrations, framework selection, RBAC, configuration. Most Tenant Admin work is one-time setup followed by periodic maintenance. If you are reading this checklist before your tenant is fully deployed, your customer success engineer is likely your primary working partner; this list assumes the tenant is operational.

Task 1 — Walk the user roster

- Open Settings > Users. The roster shows every user provisioned in your tenant.
- Confirm role assignments are correct. Each user should have one or more roles consistent with their job function. Tenant Admins should be limited to two or three people maximum.
- Walk the Entra ID group mappings. Settings > Identity > Group Mappings. Verify each Kyūdō role is mapped to the correct Entra security group (Kyudo_TenantAdmin, Kyudo_ComplianceOfficer, etc.).

Task 2 — Verify integration health

- Open Settings > Integrations. Each connected integration shows a status indicator: green (operational), yellow (degraded), red (failed).
- Click any integration showing yellow or red. The detail panel surfaces the specific issue — expired credentials, scope changes, throttling, or missing permissions.
- Confirm last-ingestion timestamps are recent. Each integration should show a recent successful ingestion. Stale timestamps mean the integration is not pulling data, even if the status indicator is green.

Task 3 — Review framework selection

- Open Settings > Frameworks. Confirm the frameworks active in your tenant are the ones your organization needs to satisfy.
- Walk the Controls Hub view filtered to one of the active frameworks. Verify control completeness scores look reasonable for where your program is in maturity.

PHASE 4 · COMPLIANCE OFFICER

Compliance Officer — first tasks

As Compliance Officer, you operate the controls and evidence side of the platform. You review evidence, generate reports, walk control completeness, and surface gaps to the Tenant Admin and the broader team. Your daily working surface is the Controls Hub and the Evidence Hub; everything else supports those two.

Task 1 — Walk the Controls Hub

- Open Controls Hub. Filter by your most active framework (typically SOC 2, ISO 27001, or whatever your organization's flagship is).
- Sort by completeness score, lowest first. The lowest-scoring controls are your immediate gap list — these are the controls where evidence is missing, stale, or insufficient.
- Click into the lowest-scoring control. Read the implementation description; spot-check the evidence; review the AI-generated control assessment. Note any concerns for the Tenant Admin.

Task 2 — Walk the Evidence Hub

- Open Evidence Hub. Filter by date range — the past 7 days — to see what is flowing in from your integrations.
- Spot-check three artifacts. Click into each. Verify the source signal is what you would expect; verify the lineage chain is intact; verify the confidence score is acceptable.
- Note any artifacts with confidence scores below 0.7. These are the items the AI flagged for human review (HITL threshold). Some require your judgment before they propagate.

Task 3 — Generate your first report

- From Controls Hub, select your active framework. Click Generate Report.
- Choose the report type: framework attestation, gap analysis, or control completeness summary. The framework attestation is most commonly the right choice for an initial walkthrough.
- Export to PDF and review. The report is what your auditor or Tenant Admin will see; if anything looks wrong, it tells you something is wrong upstream — evidence missing, mappings off, or a control implementation that needs revision.

PHASE 4 · POLICY MANAGER

Policy Manager — first tasks

As Policy Manager, you author and maintain the policies that govern your organization’s controls. Your daily working surface is the Policy Center. AI-assisted authoring is the platform’s most distinctive Policy Center feature — every draft arrives cited to the controls it governs.

Task 1 — Walk the policy library

- Open Policy Center. The library shows every policy currently in your tenant: drafts, approved, in review, expired.
- Filter by status. Start with policies in review — these are the ones that need your attention soonest.
- Click into one. Walk the policy: the body, the controls it governs, the version history, the gap analysis (if any).

Task 2 — Review one policy gap

- From Policy Center, open the Gap Analysis tab. The tab lists controls that have no governing policy.
- Pick one gap. Use the AI authoring assistant to draft a policy: click Author with AI, describe the policy intent in plain language, and review the draft the AI produces.
- The draft will arrive cited to the controls it governs. Review the citations; edit the body; save as draft.
- Submit the draft for review (if your tenant has an approval workflow configured).

Task 3 — Configure policy review cadences

- Open Policy Center > Settings > Review Cadences. Each policy can have a review cadence configured (annual is typical; some policies benefit from more frequent review).
- Confirm the cadences for your organization’s key policies. Information security, incident response, and business continuity are the three most commonly worth more-frequent review.

PHASE 4 · RISK MANAGER

Risk Manager — first tasks

As Risk Manager, you operate the risk register, drive risk treatment, and surface posture trajectory to the leadership team and the board. Your daily working surface is Risk Management; the Knowledge Graph linkage to controls and evidence is what makes your risks live rather than static.

Task 1 — Walk the risk register

- Open Risk Management. The register shows every risk currently tracked in your tenant: identified, in treatment, accepted, transferred, and closed.
- Sort by residual risk score, highest first. The highest residual risks are your priority for treatment review.
- Click into the top risk. Walk the risk: the description, the controls that mitigate it, the evidence supporting those controls, the treatment plan, the trajectory.

Task 2 — Open one risk and update its treatment status

- From the register, pick a risk where the treatment status is overdue or where the residual score has changed in the last 30 days.
- Walk the linked evidence. The evidence is what justifies the residual score — if the evidence has changed, the score should reflect it.
- Update the treatment status. Add a note describing what you changed and why. Save.

Task 3 — Walk the board dashboard

- Open Risk Management > Board View. The board view is the trajectory-focused dashboard your leadership team will see.
- Spot-check the residual risk trajectory chart. Compare the current month to the previous month and the same month last year. The trajectory tells you whether the program is improving or regressing.
- Note any inflection points. An unexpected uptick in residual risk is the kind of thing your board will ask about; understanding why now means you have an answer when asked.

PHASE 4 · VENDOR RISK ANALYST

Vendor Risk Analyst — first tasks

As Vendor Risk Analyst, you operate the vendor inventory, run third-party assessments, and respond to inbound vendor security questionnaires. Your daily working surface is Vendor Risk Management. Continuous monitoring of vendor public-facing posture is the platform's most distinctive VRM feature — vendor risk is no longer point-in-time.

Task 1 — Walk the vendor inventory

- Open Vendor Risk Management. The inventory shows every vendor tracked in your tenant: tier classification, current posture score (0–10), last-assessment date, renewal date.
- Sort by posture score, lowest first. The lowest-scored vendors are your immediate review priority.
- Click into a tier-1 vendor (highest criticality). Walk the vendor: the public posture signals (BitSight, SecurityScorecard if integrated), the questionnaire history, the contractual artifacts (BAA if HIPAA-relevant), the recent risk trajectory.

Task 2 — Pre-fill an inbound questionnaire

- From the dashboard or your Action Queue, find an inbound questionnaire (or use the demo questionnaire if your tenant is new).
- Click Pre-fill with AI. Kyūdō draws from your existing evidence to answer 70–85% of the questions, with citations and confidence scores per answer.
- Review answers below the 0.7 confidence threshold. These are the items where the AI is unsure; your judgment is needed.
- Confirm or edit each flagged answer. Export the completed questionnaire when done.

Task 3 — Configure continuous monitoring for one vendor

- Pick a tier-1 vendor without continuous monitoring already configured.
- Open the vendor detail page > Settings > Continuous Monitoring. Enable monitoring; configure the alert thresholds (typical: alert on posture score drop of 1.5+ points, or on a new finding of severity High or Critical).
- Configure your notification preference for the vendor (typical for Vendor Risk Analyst: email + Teams).

PHASE 4 · AUDITOR

Auditor — first tasks

As Auditor, your role is read-everything plus annotation. You traverse the Controls Hub and Evidence Hub like an external auditor would, document findings, and produce reports. You cannot modify configuration; that is by design — the read-only scope is what makes the auditor role auditor-defensible. Internal auditors and external audit partners both use this role.

Task 1 — Walk the audit-ready Evidence Hub

- Open Evidence Hub. Filter by the framework you are auditing.
- Walk the evidence by control. For each control: review the implementation description, spot-check the evidence, verify the lineage and confidence score, document any concerns inline.
- Use the annotation feature liberally. Annotations attach to specific evidence artifacts; they are visible to the GRC team and to your audit report.

Task 2 — Generate your audit traverse report

- From Evidence Hub, click Generate Audit Report. Select the framework you are auditing; select the controls in scope; select the date range.
- Review the generated report. The report shows every control in scope, the evidence supporting each, the confidence scores, and your annotations.
- Export to PDF. The PDF is the working artifact for your audit engagement; it stands as a defensible record of what you reviewed and what you concluded.

Task 3 — Document any findings

- From the Evidence Hub or the audit report, identify any controls where the evidence does not support the implementation description.
- Open the Findings module (if your tenant has it enabled) or annotate the relevant evidence artifacts. Each finding should have: a description, the affected control, the supporting evidence, and a recommended remediation.
- Coordinate with the Compliance Officer for finding resolution — your role is to surface; their role is to remediate.

PHASE 4 · GENERAL USER

General User — first tasks

As General User, your role is task-based: respond to assignments from the GRC team, upload evidence when requested, attest to controls when required, complete training modules. Your daily working surface is your Action Queue; you do not need to walk the modules unless directed.

Task 1 — Walk your Action Queue

- From the dashboard, click into your Action Queue. The queue shows every item assigned to you that requires action.
- If the queue is empty, that is normal for Day 1. You will be assigned tasks by the GRC team as the program operates.
- If items exist, click into the highest-priority item. Most assignments are short — a few minutes to upload evidence, attest to a control, or acknowledge a policy.

Task 2 — Complete one assignment (if any)

- Read the task description carefully. The description tells you what the GRC team needs from you and why.
- Provide the requested input. Common request types: upload a screenshot or document, attest that a process is in place, acknowledge a policy update.
- Submit. Your submission is captured as evidence with hash, timestamp, and lineage — the same chain-of-custody treatment as automated evidence.

05 · PHASE 5 · DAILY AND WEEKLY CADENCE

After Day 1: the rhythm of regular use.

After your first hour, Kyūdō becomes part of your regular working rhythm. The cadence depends on your role; the framework below is what most users settle into within their first month. Adjust based on how active your tenant is.

Daily — 5 to 15 minutes

- Check your Action Queue first thing in the morning. Items that arrived overnight (usually evidence-collection requests, integration alerts, or workflow assignments) are surfaced first.
- Acknowledge any notifications. Email, Teams, or in-app, depending on your preferences. Most notifications are informational — the ones that need action are flagged.
- Spot-check the dashboard. Any red items in your role-specific Posture Summary or Action Queue. Red items mean something needs attention; green means the program is running.

Weekly — 30 to 60 minutes

- Walk your role-specific module. Compliance Officers walk the Controls Hub; Policy Managers walk the Policy Center; Risk Managers walk the risk register; Vendor Risk Analysts walk the vendor inventory. The walk surfaces drift, recently-completed tasks, and any items you missed in the daily check-in.
- Review the weekly Posture Summary. Most tenants generate a weekly summary view at the end of the week. The summary captures what changed, what was completed, and what is pending.
- Sync with your team. Most GRC teams have a weekly stand-up or synchronization call; Kyūdō outputs (Posture Summary, framework status, risk trajectory) are useful inputs.

Monthly — 60 to 90 minutes

- Run a cross-framework consolidation review. If your tenant has multiple frameworks active, walk the cross-framework view to confirm controls, evidence, and policies remain consistent across them. STRM mapping handles most of this automatically; the monthly review catches edge cases.
- Review the risk trajectory chart. The month-over-month and year-over-year trajectories are the inputs to your monthly leadership update or board prep.
- Check policy review cadences. Any policies due for review in the upcoming month surface here; line up the work.

Quarterly — 2 to 4 hours

- Internal audit cycle (or external audit support). Quarterly is the typical cadence for an internal audit traverse; if you are audit-adjacent, this is your most-active week of the quarter.

- Trust Center review with sales engineering. The Trust Center reflects your external-facing posture; sales engineering benefits from a quarterly walkthrough of what customers and prospects will see.
- Framework review with leadership. Senior stakeholders typically want a quarterly view of overall posture, framework status, and risk trajectory. Most of this is generated from the platform; minimal authoring required.

If at any point the work feels harder than it should

Talk to your Tenant Admin first. The platform is designed to remove operational drag from compliance work; if drag returns, something is configurable. Most issues that produce drag are integration scope, notification preferences, or RBAC boundaries that need adjustment.

If your Tenant Admin cannot resolve it, escalate to your Kyūdō customer success engineer. Most customer-success issues resolve in a 30-minute call.

06 · HELP AND SUPPORT

Where to go when you have questions.

Three escalation paths, in order. Most questions are answered at level 1 or level 2; level 3 is for issues that affect tenant configuration or platform behavior.

Level 1 — in-product help

The fastest path. Click the question mark icon in the top-right corner of any screen. The contextual help panel surfaces articles, walkthroughs, and short videos relevant to the screen you are on. Search for any term; results are filtered to your role and your tenant's configuration.

In-product help also includes a Tour Mode that walks you through a guided overview of any module. If you skipped Phase 3 of this checklist or want a refresher, Tour Mode is the fastest way to get oriented.

Level 2 — your Tenant Admin

The person inside your organization who provisioned you. They know your tenant's configuration, your framework selection, your team's working patterns, and the institutional context the in-product help cannot capture.

Most questions about "why is my tenant configured this way" or "how does our team usually handle this" are answered fastest by your Tenant Admin. They are also the right escalation point for role assignments, integration questions, and access concerns.

Level 3 — Kyūdō customer success

For issues that go beyond your tenant configuration: platform behavior questions, suspected bugs, integration failures the Tenant Admin cannot resolve, capability questions about the platform itself.

Your Tenant Admin can route issues to customer success on your behalf. If you need to reach customer success directly, hello@kyudo.ai is the front door; your tenant ID and the screenshot of what you are seeing accelerate response.

Common questions

Question	Where to go
I cannot sign in.	Tenant Admin (verify Entra ID group assignment); then Kyūdō customer success if Entra is correct.
My role looks wrong.	Tenant Admin (Entra ID group mapping).

Question	Where to go
I do not see a module I expected.	Tenant Admin (RBAC role assignment); module visibility is role-driven.
I have a question about a specific framework.	Framework guide series at kyudo.ai/guides; for SOC 2, ISO 27001, NIST CSF, CMMC, or HIPAA, dedicated guides are published.
I want to suggest a feature.	In-product feedback (question mark icon > Send Feedback) or via your Tenant Admin to customer success.
I think I found a bug.	In-product feedback with screenshot; Tenant Admin for triage; customer success for resolution.
I need to do something my role does not allow.	Tenant Admin — either role adjustment or task delegation. Do not request expanded permissions without business justification.

APPENDIX A · QUICK REFERENCE

Common tasks. Common keyboard shortcuts.

Common tasks

Task	Path
Update your profile	Top-right role indicator > Profile
Change notification preferences	Profile > Notifications
Find evidence for a specific control	Controls Hub > control detail > Evidence tab
Generate a framework attestation	Controls Hub > framework filter > Generate Report
Pre-fill a customer questionnaire	Trust Center > Questionnaires > Pre-fill with AI
Update risk treatment status	Risk Management > risk detail > Treatment > Update
Author a new policy with AI	Policy Center > New Policy > Author with AI
Review a gap in policy coverage	Policy Center > Gap Analysis tab
See the audit-ready Evidence Hub view	Evidence Hub > switch to Auditor view (Auditor role only)
Open in-product help	Question mark icon, top-right corner
Sign out	Top-right role indicator > Sign Out

Keyboard shortcuts

Shortcut	Action
Ctrl/Cmd + K	Universal search across controls, evidence, policies, risks, vendors
Ctrl/Cmd + ,	Open Settings (if your role has Settings access)
Ctrl/Cmd + /	Open in-product help
Ctrl/Cmd + N	New (context-dependent: new policy, new risk, etc.)
Esc	Close the current modal or panel

APPENDIX B · GLOSSARY

Terms used in this checklist.

Term	Definition
Action Queue	Your personal task list inside Kyūdō. Every assignment, approval request, and reminder routed to you appears here.
Conditional Access	Microsoft Entra ID policies that govern when and how users can sign in (device compliance, MFA method, geographic restrictions). Most organizations have these configured for any access to sensitive systems including Kyūdō.
Confidence score	AI-computed score on every Kyūdō output. Indicates how strongly the source signals support the conclusion. Below the human-in-the-loop threshold of 0.7, outputs are flagged for human review.
Controls Hub	The Kyūdō module that holds every control mapped to your active frameworks. The Compliance Officer’s primary working surface.
Entra ID	Microsoft’s identity service (formerly Azure AD). The authentication source for Kyūdō in most deployments.
Evidence Hub	The Kyūdō module that holds every evidence artifact with hash, lineage, and confidence score. The Auditor’s and Compliance Officer’s most-visited view.
Framework	A compliance regime such as SOC 2, ISO 27001, NIST CSF, CMMC, or HIPAA. Multiple frameworks can be active in a single tenant; the same control set satisfies all of them via STRM.
HITL threshold	Human-in-the-Loop. The confidence threshold (0.7 default) below which AI-produced outputs are flagged for human review before they propagate.
MFA	Multi-factor authentication. Required for all Kyūdō access; configured by your organization through Microsoft Entra ID.
Policy Center	The Kyūdō module for AI-authored, control-aligned policy lifecycle management. The Policy Manager’s primary working surface.
Posture Summary	The role-specific dashboard view that surfaces your highest-priority items at the top of the home screen.
RBAC	Role-Based Access Control. Determines what you can see and do in the platform; mapped from Entra ID groups to Kyūdō roles.

Term	Definition
Risk Management	The Kyūdō module that holds your risk register, treatment workflow, and trajectory dashboards. The Risk Manager’s primary working surface.
Tenant Admin	The senior administrative role inside your organization. The person who provisioned you and who is your level-2 escalation path for any platform issue.
Trust Center	The Kyūdō module that provides external-facing posture visibility for customers, partners, and regulators. The portal customers see when they request transparency about your security posture.
VRM	Vendor Risk Management. The Kyūdō module for vendor inventory, third-party assessment, questionnaire automation, and continuous vendor posture monitoring.