Kyūdō

SOVEREIGNTY-GRADE AI · GRC

Kyūdō in Two Pages

A board-ready summary of the program your CISO or compliance officer is proposing.

The financial case. The risk case. The regulatory case. No jargon.

PRESENTED BY

John Haifa – Co-founder & CEO

Kyūdō

3525-265 Hyland Avenue · Costa Mesa, CA 92626 · 949.288.4875

jhaifa@kyudo.ai

kyudo.ai · May 9, 2026

CLASSIFICATION: FOR BOARD DISCUSSION

Kyūdō

FOR THE BOARD

What you are being asked to approve

Your CISO, Compliance Officer, or Risk Lead is proposing to deploy Kyūdō. This page explains what it is and why now. The next page makes the case in three frames: the financial case, the risk case, and the regulatory case.

The plain-English version

The company spends a lot of time and money proving to auditors, customers, and regulators that its security and compliance are in order. Most of that work is manual. People rebuild the same evidence binders every audit cycle. The Microsoft security tools the company already pays for are producing the right signals, but those signals are not being converted into the records auditors actually want to see.

Kyūdō sits inside the company's own Microsoft Azure environment and does that conversion continuously. Controls, evidence, policies, vendor risk, and AI governance run as one system, all the time, instead of being reassembled before each audit.

> **The one-sentence version**
>
> Kyūdō turns the security stack the company already owns into continuous proof that the company is well-run, so audits become a confirmation instead of a fire drill.

Why this matters now

- Audit cycles are getting longer and more expensive. Each new customer or framework adds another one.
- New AI regulations are arriving on a fixed clock. The EU AI Act's August 2026 deadline applies to any company offering high-risk AI systems into the EU market.
- Cyber insurance carriers and enterprise customers are demanding evidence faster, more often, and in more detail than they did two years ago.

Where Kyūdō is different

Most compliance software lives in the vendor's cloud and pulls the company's data out to do its work. Kyūdō is deployed inside the company's own Azure tenant. The data never leaves. The vendor cannot see it. That matters for regulated industries, for hard customer questions, and for the company's own legal exposure.

Kyūdō

THE THREE CASES

Why the board should approve this

01 · The financial case

Hidden compliance labor for a regulated mid-market organization typically runs $150K to $400K per year. Kyūdō removes most of it:

- Outside audit-prep consulting ($80K to $150K per year) drops to targeted advisory; the annual rebuild stops.
- The lightweight SaaS GRC tool that mostly stores documents goes away. One platform runs the program, and the 5 to 15 hours per audit pulled from IT, legal, and business owners disappears.
- Trust Center and questionnaire automation cut security-review response from weeks to hours, moving deals through procurement faster.

Bottom line. The platform pays for itself in the first audit cycle through reduced labor, faster deal closure, and the consultant rebuild that no longer happens.

02 · The risk case

Between audits, the company has limited visibility into whether controls are still working. A control that passed in March can drift in April and stay broken until the next audit catches it.

- Control drift becomes visible. Maturity is scored continuously, so a weakened control or stale policy shows up in days, not at the next audit.
- Vendor risk gets quantified. Third-party exposure moves out of a spreadsheet of self-reported scores into a structured inventory with ongoing monitoring.
- AI risk gets governed. The company's AI systems are inventoried and monitored against the same control set as everything else, with traceable evidence on every artifact.

Bottom line. The biggest risk is what changed between audits. That gap is what regulators, customer procurement teams, and cyber insurance underwriters ask about first.

03 · The regulatory case

- SOC 2, ISO 27001, HIPAA, and HITRUST run on one control set with automatic crosswalks. Evidence is current at audit time, not reconstructed.
- CMMC 2.0 is now in defense contract clauses. Methodology and artifacts are C3PAO-recognized.
- EU AI Act (Aug 2, 2026 deadline; up to 15M EUR or 3% of global turnover), ISO 42001, and NIST AI RMF run on the same platform as cyber.

Bottom line. The choice is a platform that absorbs the next framework as a configuration change, or consultants who rebuild the program every time a new acronym arrives.