

Running your own Compliance-as-a-Service

Your engagement model, your brand, your margin — our engine underneath it.

Most compliance practices are productised in the proposal and bespoke in the delivery. **A service you rebuild per client is one you cannot price with confidence, hand to a junior, or defend to an assessor a year later.** The Hub and the Third Party Risk Hub make the same engagement repeatable across a portfolio — and pull most of the evidence from the client's own tenant.

One portfolio

EVERY CLIENT IN ONE PLACE

25 end clients by default, raisable to 1,000. Each carries its own assessments, risks, evidence, suppliers, policies and integrations, isolated from every other client and from your own account. Invite colleagues as Editors or read-only Viewers, scoped to named clients where that fits.

One method

THE SAME QUESTIONS, EVERY TIME

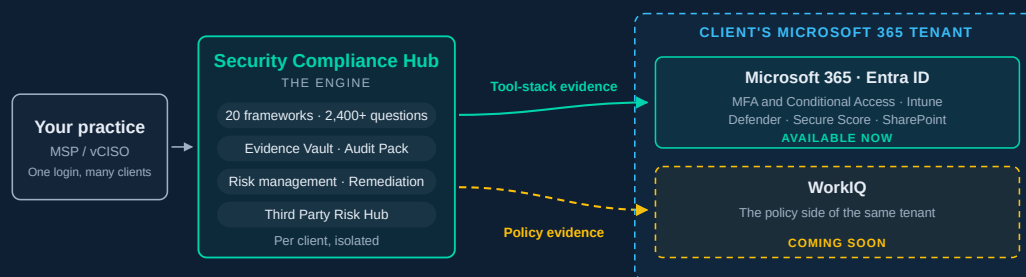
20 frameworks and more than 2,400 questions already authored, scored and cross-referenced — Cyber Essentials, ISO 27001, CAF, DORA, NIS2, GDPR, CMMC, FedRAMP and more. Consultants run the method rather than write it, so a new joiner delivers to the same standard.

One evidence trail

PROVABLE A YEAR LATER

Answers, evidence and analysis archived per run for three years. The Audit Pack exports a client's whole position as a ZIP with SHA-256 integrity hashes — the artefact that ends the "where did this come from" conversation.

MOST OF THE EVIDENCE IS ALREADY IN THEIR TENANT



Read-only, and scoped to one client. Each tenant is connected under its own administrator's consent. Nothing is written back, and no client's signals are mixed with another's or with yours.

BRANCH ONE — THE TOOL STACK

Live configuration, shown beside the question it answers: multi-factor registration *and* whether Conditional Access enforces it, Intune device compliance, open Defender alerts, Secure Score, risky users from Entra ID Protection — and SharePoint documents pulled into the Evidence Vault.

- ▶ **It suggests; it never answers for you.** Each signal is a note your consultant accepts or overrules.
- ▶ **It contradicts politely.** Where a live signal disagrees with the declared answer, the analysis says so.
- ▶ **Not only Microsoft.** Okta, CrowdStrike Falcon and Google Workspace connect the same way, per client.

BRANCH TWO — THE POLICY SIDE COMING SOON

The other half of an audit question is documentary: does the policy exist, was it approved, is it current. **WorkIQ is the branch that will cover that side of the same tenant.** It is not available yet, and nothing here should be read as a description of what it will do.

UNTIL IT LANDS

- ▶ **SharePoint import** already attaches the client's own policy documents to the question they support.
- ▶ **The Policy Generator** drafts from 20 templates, tailored to that client's gaps, for the documents that turn out not to exist.
- ▶ **Risk management** keeps each client's risk method, register and Statement of Applicability approved and current.

GETTING A PRACTICE ONTO IT

1 · Your portfolio

Your tenancy is created and your team invited — Editors or Viewers, all clients or named ones. MFA is mandatory for you and every Editor. Add clients as you win them.

2 · Per-client connection

Each client's administrator grants read-only consent once, from a link you send. Credentials for the non-Microsoft connectors are held encrypted under a UK-region key.

3 · Deliver, then retain

Run the engagement, export the Audit Pack, hand over the remediation tracker — and leave risk reviews, reassessment reminders, framework-change watch and supplier re-scans running under the retainer.

Commercially it is a revenue share, not a per-seat licence — tiered by the size of your book, with a per-client arrangement for smaller practices starting out. Terms are agreed per practice rather than published.

You keep the client relationship and the brand — including on the supplier-facing pages, which carry your logo and colour. What you charge your clients is yours to set. The Hub is deliberately the engine rather than the offer: it never sells to your clients.

WorkIQ is not yet available and shows the intended shape of the policy branch, not something that can be bought or scheduled today; everything else here is shipped and in use. Security Compliance Hub is a readiness and assurance platform — it does not certify, audit or issue an attestation, and connected-tool signals support a practitioner's judgement rather than replace it. Framework names belong to their owners; figures are current defaults and limits are set per tenancy. Talk to us:

sales@securitycompliancehub.io