ASSESS ONCE — EVIDENCE EVERYWHERE

Map a control once. Prove it across thirteen rulebooks and standards.

A single workspace for the CBB Bahrain and VARA Dubai rulebooks, PCI DSS, ISO 27001 and ISO 42001 — with the cross-framework mappings already built, so a status you set in one standard flows to its equivalents in the rest.

2,098	496	13	41
controls pre-loaded	cross-framework mappings	standards unified	control categories

ONE MAPPED CLUSTER — THEME: **ROLES, RESPONSIBILITIES & RISK GOVERNANCE**

PCI DSS v4.0.1	ISO/IEC 27001:2022	ISO/IEC 42001:2023
1.1.1	5.3	A.3.2

The CBB Bahrain and VARA Dubai rulebooks are cross-referenced by compliance category on the Category rollup rather than clause by clause: a clause-level equivalence between a regulator's rulebook and a security standard is a matter of professional judgement, so it is stated as a category overlap and not auto-applied. Set 1.1.1 to **Full** in PCI DSS and the other two update in step. Multiply by 496.

Kim — I built KUAIGRC after years of running the same controls through a different spreadsheet for every framework, rulebook and standard. It is designed, maintained and supported by me, from the Kingdom of Bahrain. Questions before you start? Email me directly.

5-day free trial Annual · $833 per seat, 3-seat minimum · card & PayPal kim_abdalian@yahoo.com

© 2026 Kim

WHY MULTI-FRAMEWORK PROGRAMMES DRIFT

The same control lives in five places — and every copy drifts.

Access reviews sit in your PCI DSS tracker, your ISO 27001 Statement of Applicability, your ISO 42001 readiness sheet, your CBB cyber-security notes and a spreadsheet someone owns. Update one, forget the others, and by audit season nothing agrees.

WHAT CHANGES

01

Assess once, propagate

Set a control's status and it flows to its mapped equivalents across the other standards — automatically, and only where you haven't set something by hand.

02

Evidence that follows the map

Attach a file to one control and it appears on every crosswalk-linked control, tagged with where it came from. Remove it once, it's gone everywhere.

03

Pick a baseline standard

Work one framework end to end, then push its statuses and evidence to the other twelve in a single action. Manual overrides are preserved.

04

Board-ready in minutes

A PDF and a CSV for any selection of standards, with pie charts, a category roll-up and an optional control-by-control annex. Add your organisation's logo, header title and footer line — they print on every page. Then email it to the auditor, CC the board, without leaving the tool.

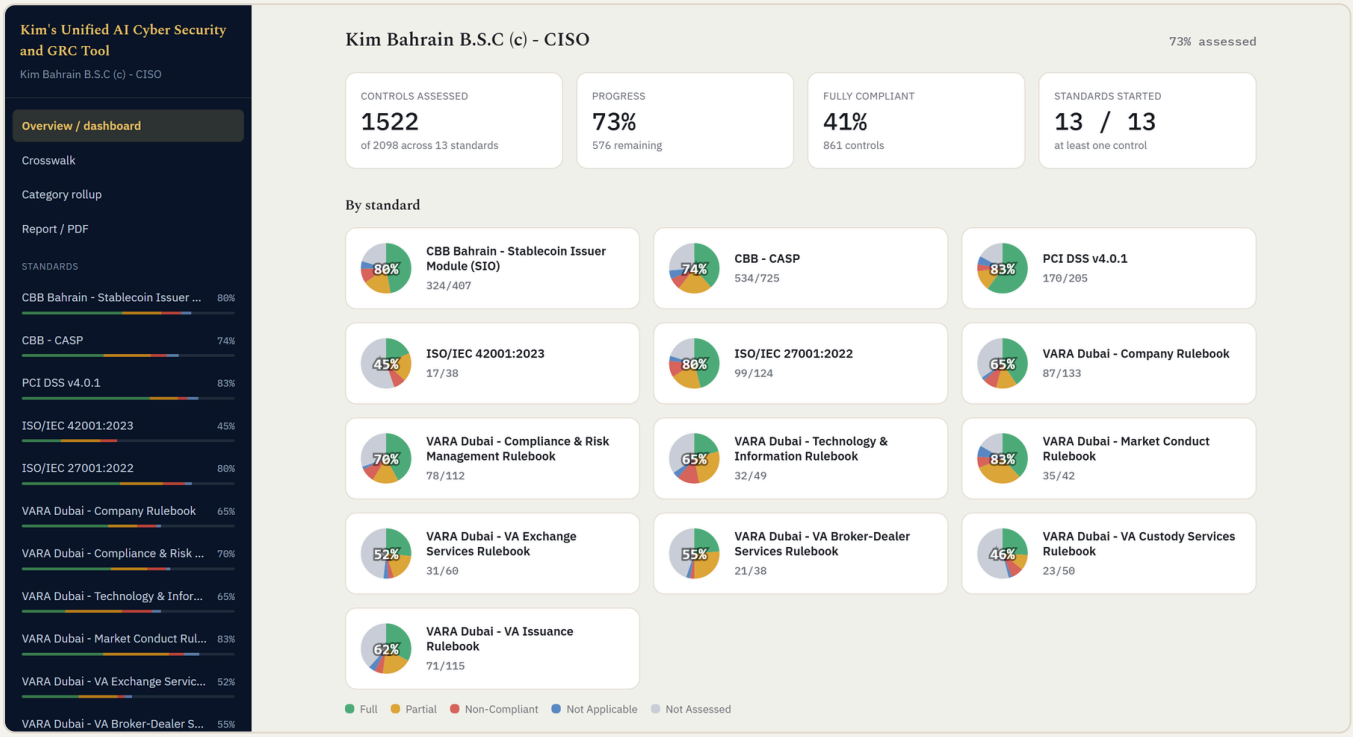
© 2026 Kim

THE DASHBOARD — AND THE REVIEW THAT FILLS IT

See the whole programme at a glance.

Every standard gets a live compliance pie the moment you start assessing. Nothing to configure and no evidence collector to wire up — the control library and the crosswalk ship loaded.

THE OVERVIEW DASHBOARD — A LIVE COMPLIANCE PIE PER STANDARD



OVERVIEW PAGE, A WORKSPACE MID-ASSESSMENT — ILLUSTRATIVE DATA

THE REVIEW, IN FOUR STEPS

01

Assess your strongest framework. Work PCI DSS v4.0.1's 205 requirements — status, owner note, evidence.

02

Push it across the crosswalk. One action fills the mapped controls in the other standards; hand-set values are kept.

03

Attach evidence once. A record on `PCI 1.1.1` appears on `ISO 27001 5.3` and `ISO 42001 A.3.2`.

04

Export the report. Pick standards, add the client name and logo, download the PDF or email it to the auditor; CSV for the workpapers.

ONE CROSSWALK CLUSTER AS LOADED — THE THREE STANDARDS MAPPED CLAUSE TO CLAUSE

PCI DSS	ISO 27001	ISO 42001
1.1.1	5.3	A.3.2

© 2026 Kim

HOW A MULTI-TENANT SAAS KEEPS TENANTS APART

One database. Every workspace fenced off in it.

A shared-schema, single-database design: every tenant row carries an `org_id`, and PostgreSQL Row-Level Security — not application code alone — makes a query unable to cross organisations.

CLIENT

Any modern browser · HTTPS / TLS only, HSTS, strict security headers

↓

EDGE & APP — VERCEL

Next.js App Router. Edge middleware refreshes the session, enforces the 2FA step-up and the 30-minute idle timeout, and gates every `/app` route before it renders. Server Actions re-check role and membership on every write.

↓

Auth — Supabase

Hashed passwords (never seen by us), signed http-only session cookies, TOTP two-factor with a required AAL2 step-up at sign-in.

Postgres — Row-Level Security

Every tenant table has `org_id`; policies allow `is_org_member()` to read and `can_write_org()` to write, via `SECURITY DEFINER` helpers. The 2,098 controls and 496 mappings are shared, read-only reference data.

Storage — Supabase

Private bucket; each object's path starts with the workspace id, governed by the same RLS helpers. Downloads only via a 60-second signed URL.

OFF TO THE SIDE

Lemon Squeezy — Merchant of Record. Cards are entered on Lemon Squeezy; we receive only a subscription record over a signed (HMAC-SHA256) webhook. No card data on our servers.

WHY ONE TENANT CAN'T SEE ANOTHER

- **The fence is in the database.** A query runs as the signed-in user and RLS filters every row by `org_id` — an app bug can't widen access.
- **Files inherit the same fence.** Evidence is addressed by a path that starts with the workspace id, so workspace A can't list, open or guess a file in workspace B.
- **Least privilege, enforced in the DB.** Owner / editor / viewer per workspace; seat and billing limits are database rules, not just hidden UI.
- **Backed up & recoverable.** Managed Postgres and storage, daily backups with point-in-time recovery on the production tier.

© 2026 Kim

SIGN-IN, EVIDENCE AND CHANGE HISTORY

Signed in securely. Ready for the auditor.

- **Account security.** Two-factor authentication with any authenticator app (Google, Microsoft, 1Password, Authy…), a 30-minute idle timeout, and a 12-character password policy with reuse history and lock-out after repeated failures.
- **Encryption & evidence.** TLS in transit, encrypted at rest. Evidence sits in a private store; every download is a fresh 60-second signed link, never a public URL.
- **Audit trail.** Every status change is recorded — who changed what, from what value, and when.
- **White-label reports.** Every PDF carries your organisation's logo, header title and footer line on every page — a consultancy hands each client a report in that client's own livery.
- **Payments.** Card and PayPal via a Merchant of Record; global VAT and sales tax handled; no card data on our servers.

STANDARDS COVERED

$833 per seat / year

5-day free trial. Three-seat minimum — $2,499 for the first year. Add or remove seats one at a time, pro-rated to your renewal date; seats are reassignable within the term at no extra cost. Cancel from the Billing page; access runs to the end of the paid year.

Start the free trial

kimuaigrc.app · Kim · kim_abdalian@yahoo.com · +973-3671-9993

© 2026 Kim. All rights reserved. "Kim's Unified AI Cyber Security and GRC Tool" and its structure, control taxonomy, category framework and cross-standard crosswalk are proprietary and confidential — licensed, not sold. This tool organises and tracks compliance work; it does not provide legal or audit advice and does not by itself confer certification.