ASSESS ONCE — EVIDENCE EVERYWHERE

Audit the site you actually have. Prove it across eight standards.

Every physical and environmental requirement from PCI DSS, ISO 27001, NIST CSF, SOC 2, GDPR and three more — banded by Uptime Institute Tier I–IV and scoped to the building in front of you, whether that is a Tier IV hall, a cupboard with three servers in it, or the recovery site behind both.

608	76	8	37
controls pre-loaded	cross-standard checkpoints	standards unified	control categories

ONE CHECKPOINT — TIER I · **ACCESS CONTROL, AT THE PRODUCTION SITE**

PCI DSS v4.0.1 9.2 / 9.3	ISO/IEC 27001:2022 A.7.1 / A.7.2	NIST CSF 2.0 PR.AA-06
SOC 2 (TSC) CC6.4	GDPR (EU 2016/679) Art. 32(1)(b)	ISO/IEC 27701 A.7.1 via PIMS
ISO 22301:2019 8.3.3	Secure Controls Fwk PES-02	

Set this checkpoint to **Full** once and the other seven standards follow. Multiply by 76 — and it is asked again, separately, of the comms room and the DR site.



Kim — I built KDCCR 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.

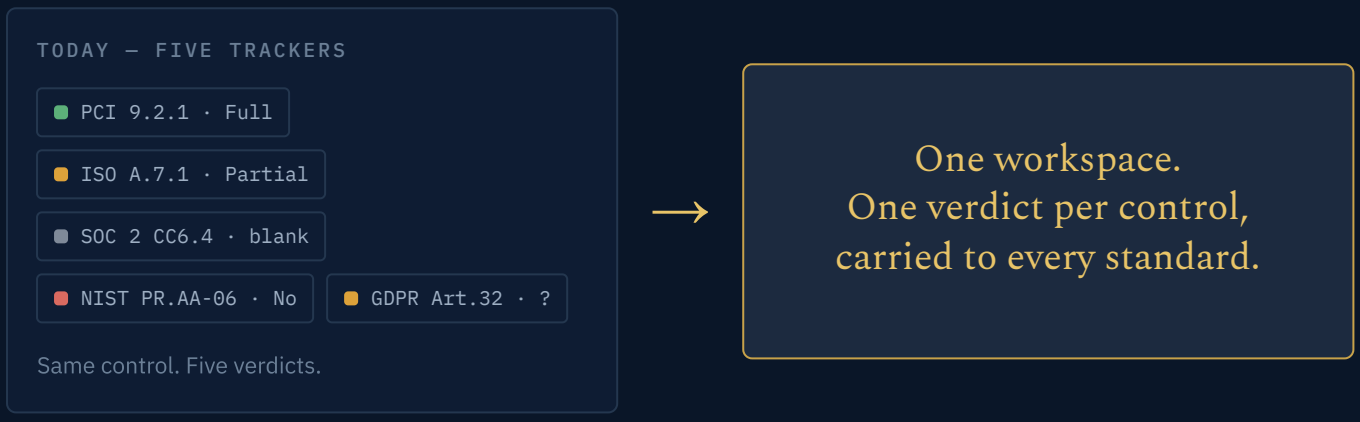
5-day free trial Annual · $500 per seat, no minimum · card & PayPal kim_abdalian@yahoo.com

© 2026 Kim

WHY ONE CHECKLIST NEVER FITS THREE BUILDINGS

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

Who may enter the room sits in your PCI DSS tracker, your ISO 27001 Statement of Applicability, your SOC 2 readiness sheet, your GDPR Article 32 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 76 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 standard end to end, then push its statuses and evidence to the other seven 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

ONE TOOL, THREE SEPARATE AUDITS

The recovery site is not the production floor.

Most compliance material hands a small business a Tier IV checklist and lets it fail, then totals every site into a single score. This library is built the other way round: three audits of three buildings, each charted, totalled and reported on its own.

01

Production data centre — 24 checkpoints

Banded Uptime Institute Tier I–IV, so you assess against the level the site is genuinely built to rather than the largest one imaginable. Each tier carries its own definition on the row, and the rest is recorded as out of scope.

02

Server & comms rooms — 14 checkpoints

States what still applies, what reduces in scope, and what does not apply at all — each exclusion with its reason attached. Four items appear that a large facility never needs: lockable racks, room segregation, coordination with the host building, and leak risk from shared plumbing.

03

DR site — 38 checkpoints

The 24 production checkpoints re-asked of the recovery site, which has its own tier and is usually a lower one — that gap is the finding. Plus 14 that exist nowhere else: separation from the primary risk zone, utility independence, replication and achieved RPO, recovery time against target, capacity parity, failover and failback testing, runbooks, restore testing, network cutover, invocation authority, staffing and access, configuration drift, and what an outsourced DR contract guarantees during a regional event.

04

Never averaged together

A Tier IV production floor and a Tier I recovery site merged into one number produce a comfortable score and hide the thing an auditor is looking for. Each scope gets its own tab, its own pies and its own section in the report — and a verdict set on one site never propagates to another.

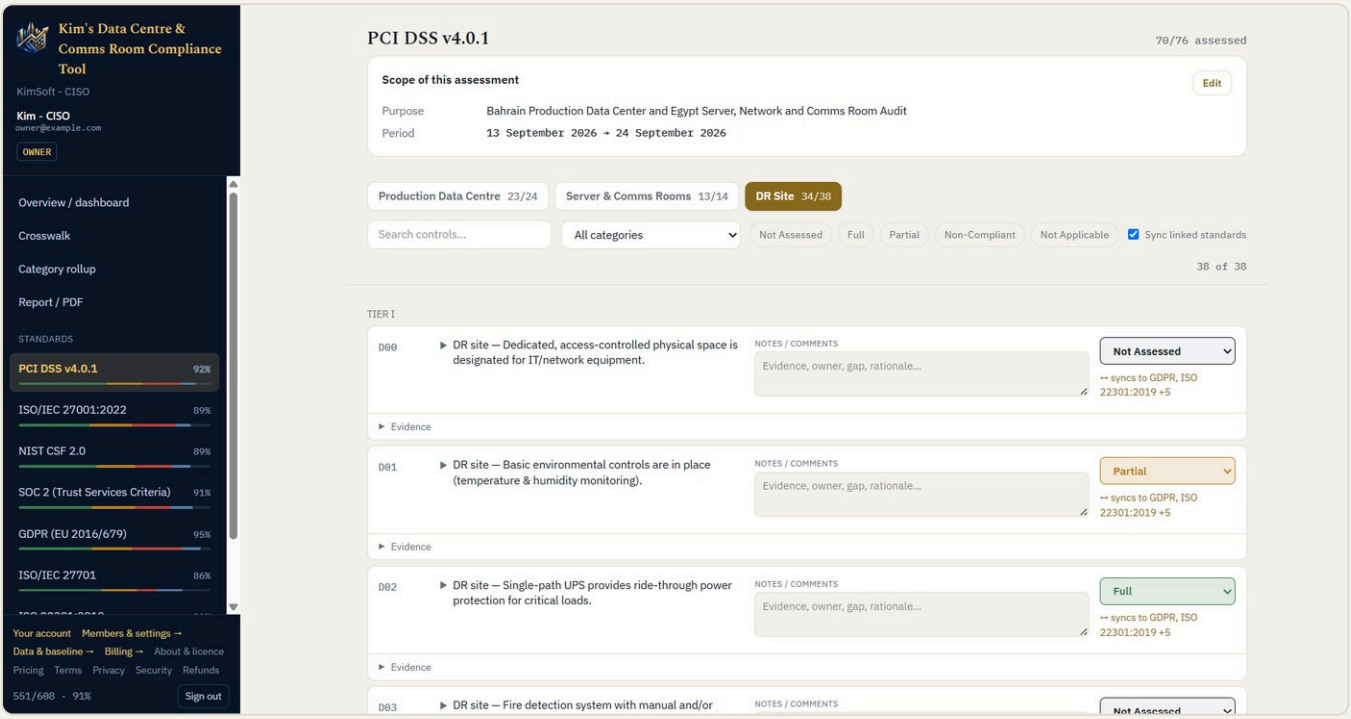
© 2026 Kim

THE DASHBOARD — AND THE REVIEW THAT FILLS IT

Every standard, asked of every site.

A standard opens with one tab per site, each carrying its own progress, so it is never in doubt which building you are assessing. Every control has a status, a note and its own evidence, and the clause reference for that standard sits on the row. Nothing to configure and no evidence collector to wire up: the control library and the crosswalk ship loaded.

A STANDARD SHEET — THE THREE SITE TABS, DR SITE SELECTED



ACTUAL SCREEN — PCI DSS V4.0.1 ON THE DR SITE TAB, WITH THE TIER I CHECKPOINTS RE-ASKED OF THE RECOVERY SITE

THE REVIEW, IN FOUR STEPS

01

Assess your strongest standard. Work PCI DSS v4.0.1's 76 checkpoints — status, owner note, evidence.

02

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

03

Attach evidence once. A photo of the rack lock on PCI 9.2 appears on ISO 27001 A.7.1, NIST PR.AA-06 and five more.

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 CHECKPOINT AS LOADED — TIER I · ACCESS CONTROL, ACROSS ALL EIGHT

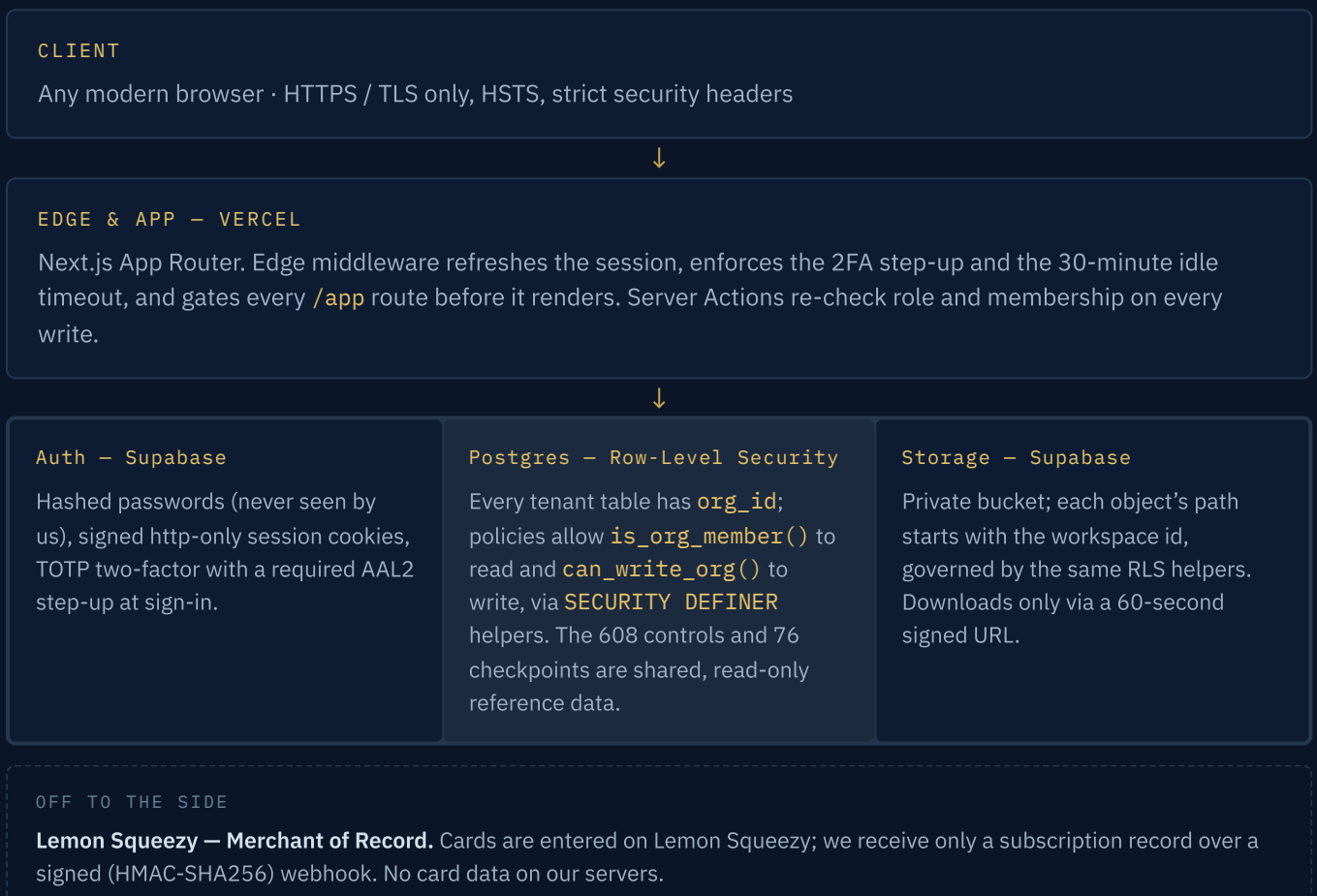
PCI DSS	ISO 27001	NIST CSF	SOC 2	GDPR	ISO 27701	ISO 22301	SCF
9.2 / 9.3	A.7.1 / A.7.2	PR.AA-06	CC6.4	Art. 32(1)(b)	A.7.1 via PIMS	8.3.3	PES-02

© 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.



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



$500 per seat / year

5-day free trial. No minimum — buy a single seat. 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

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

© 2026 Kim. All rights reserved. "Kim's Data Centre & Comms Room Compliance 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.