Cloud Security Alliance

CAIQ v4 - RiskAlign self-assessment

197 controls across 17 domains

Operator: RegAlign Limited (Jersey company no. 165263)
Product: RiskAlign - public surface riskalignplatform.com

Yes: 154 No: 5 Partial: 12 N/A: 26

Stage disclosure: pilot-stage product. CAIQ answers are self-assessed (CSA STAR Level 1). Third-party attestations are trigger-tied.

AA - Audit & Assurance

AA-01 — Yes

Audit and Assurance Policy and Procedures

Audit policy documented in `docs/canonical/30_Chain_Verifier_Auditor_Runbook.md` and `31_Pilot_Ready_Attestation.md`. Single-founder operation; written policy maintained in `docs/canonical/` and reviewed at every release. No formal annual sign-off cycle yet - planned post first paying pilot.

AA-02 — No

Independent Assessments

No third-party SOC 2 / ISO 27001 / STAR Level 2 yet. Pen-test SoW drafted (`19_Pen_Test_RFP.md`); execution planned post first paying pilot.

AA-03 — Yes

Risk Based Planning Assessment

Risk register maintained internally; SWOT v2 published (`01_SWOT_v2.md`). Re-reviewed every release.

AA-04 — Yes

Requirements Compliance

Compliance scope mapped in `25_Pilot_Prospectus.md` and `32_Trust_Pack.md` (JFSC AML/CFT/CPF, DPJL 2018, UK GDPR-aligned).

AA-05 — Partial

Audit Management Process

Internal audit only (founder-led, evidenced via hash-chained audit trail). External audit programme not yet established.

AA-06 — Yes

Remediation

Issues tracked in product `issues` table with status workflow, escalation, and audit-trailed remediation. See Trust Pack Sec.6.

AIS - Application & Interface Security

AIS-01 — Yes

Application and Interface Security Policy and Procedures

SDLC + interface security policy embedded in commit / review workflow; see `docs/canonical/architecture-overview.md`.

AIS-02 — Yes

Application Security Baseline Requirements

Baseline: TypeScript strict, RLS-by-default, no service-role on user paths, signed webhooks, CSP. Enforced in code review.

AIS-03 — Partial

Application Security Metrics

Dependency-scan + lint metrics in CI; no formal monthly metrics report yet.

AIS-04 Yes

Secure Application Design and Development

Threat modelling at architecture-change time; secure-by-default patterns documented in `architecture-overview.md`.

AIS-05 Partial

Automated Application Security Testing

Dependency-scan automated in CI; SAST coverage limited. DAST / pen-test deferred to `19_Pen_Test_RFP.md` engagement.

AIS-06 Yes

Automated Secure Application Deployment

Lovable-managed CI/CD; every deploy is git-tracked and reproducible; rollback by re-deploy of prior commit.

AIS-07 Yes

Application Vulnerability Remediation

Public Vulnerability Disclosure Policy at `riskalignplatform.com/vdp` (see `28_Vulnerability_Disclosure_Policy.md`); SLAs documented.

BCR - Business Continuity Management & Operational Resilience

BCR-01 Yes

Business Continuity Management Policy and Procedures

BCP outline at `07_BCP_Outline.md`. Reviewed at every major release.

BCR-02 Yes

Risk Assessment and Impact Analysis

BIA documented in BCP outline; RTO 8h / RPO 24h for tenant data (mirrors Trust Pack Sec.8).

BCR-03 Yes

Business Continuity Strategy

Strategy: rely on managed-platform multi-AZ + daily DB snapshots; founder-led incident response. See `07_BCP_Outline.md`.

BCR-04 Yes

Business Continuity Planning

Plan documented; named successor scoped in `16_Successor_Role_Spec.md`.

BCR-05 Yes

Documentation

All BCP/DR docs in `docs/canonical/`; published Trust Pack Sec.7.

BCR-06 No

Business Continuity Exercises

No live BCP exercise executed yet. Tabletop scheduled for Q3 2026 once first pilot live.

BCR-07 Yes

Communication

Status page at `riskalignplatform.com/status`; incident communication via direct email to tenant admins.

BCR-08 Yes

Backup

Lovable Cloud (Supabase EU) daily automated backups; point-in-time recovery enabled. See Trust Pack Sec.2.

BCR-09 Yes

Disaster Response Plan

DR plan documented in `07_BCP_Outline.md`; relies on managed-platform multi-AZ failover.

BCR-10 — No

Response Plan Exercise

Not yet exercised; planned alongside BCR-06.

BCR-11 — N/A

Equipment Redundancy

Managed platform (Cloudflare + Supabase EU) provides infrastructure redundancy. RiskAlign owns no physical equipment.

CCC - Change Control & Configuration Management

CCC-01 — Yes

Change Management Policy and Procedures

Every change is a git commit with reviewer + deploy audit trail. Lovable-managed deploys.

CCC-02 — Yes

Quality Testing

Type-check + lint + Vitest required on every change; visual QA before publish.

CCC-03 — Yes

Change Management Technology

Git + Lovable CI/CD. Append-only audit-trail with SHA-256 hash chain; per-page verifier at `riskalignplatform.com/verify`. See Trust Pack Sec.6.

CCC-04 — Yes

Unauthorized Change Protection

Only the founder can deploy; MFA-enforced on Lovable account. Branch protection on `main`.

CCC-05 — Yes

Change Agreements

Pilot Agreement (`05_Pilot_Agreement_Scaffold.md`) covers change-notification cadence.

CCC-06 — Yes

Change Management Baseline

Baseline = current `main` branch + last deployed commit SHA; reproducible by checkout.

CCC-07 — Partial

Detection of Baseline Deviation

Git tracks code drift; runtime config drift caught manually. Automated config-drift alerting deferred.

CCC-08 — Yes

Exception Management

Exceptions logged as issues; require sign-off + audit-trail entry.

CCC-09 — Yes

Change Restoration

Rollback by re-deploying prior commit; DB rollback via Supabase PITR. RTO < 1h.

CEK - Cryptography, Encryption & Key Management

CEK-01 — Yes

Encryption and Key Management Policy and Procedures

TLS 1.2+ in transit, AES-256 at rest (Lovable Cloud managed). Key custody is sub-processor side - see Trust Pack Sec.2/Sec.3.

CEK-02 — Yes

CEK Roles and Responsibilities

Founder owns key-lifecycle decisions; day-to-day key custody is delegated to sub-processors (Cloudflare, Supabase).

CEK-03 Yes

Data Encryption

TLS 1.2+ in transit, AES-256 at rest (Lovable Cloud managed). Key custody is sub-processor side - see Trust Pack Sec.2/Sec.3.

CEK-04 Yes

Encryption Algorithm

AES-256 at rest, TLS 1.2+ (incl. TLS 1.3) in transit. No proprietary crypto.

CEK-05 Yes

Encryption Change Management

Crypto changes flow through normal CCC change process; sub-processor crypto changes tracked via vendor advisories.

CEK-06 Yes

Encryption Change Cost Benefit Analysis

Documented when crypto is changed; default = use sub-processor managed crypto, which has independent CBA.

CEK-07 Yes

Encryption Risk Management

Crypto-risk reviewed at architecture-change time; logged in risk register.

CEK-08 No

CSC Key Management Capability

Bring-your-own-key not supported and not on the near-term roadmap. Customer keys are not separable from managed-platform encryption at this stage; a true BYOK answer would require application-layer envelope encryption we have not built. Tracked openly at /security/roadmap (trigger: enterprise procurement requirement).

CEK-09 Partial

Encryption and Key Management Audit

Internal review only; relies on sub-processor SOC 2 / ISO 27001 attestations.

CEK-10 Yes

Key Generation

Keys generated by sub-processors (Cloudflare, Supabase); no founder-managed long-lived keys other than API/webhook secrets.

CEK-11 Yes

Key Purpose

Each key has a single purpose (TLS cert, DB encryption, webhook HMAC, API key signing).

CEK-12 Yes

Key Rotation

Sub-processor keys rotated per their published schedule. Tenant API keys / webhook secrets rotatable on demand via `/admin/api-keys`.

CEK-13 Yes

Key Revocation

API keys revocable instantly via operator UI; HTTP 401 returned on next call.

CEK-14 Yes

Key Destruction

Revoked keys are deleted, not just disabled; sub-processor key destruction per their procedures.

CEK-15 Yes

Key Activation

API keys active on creation; sub-processor keys per their lifecycle.

CEK-16 Yes

Key Suspension

API keys can be disabled (suspended) before deletion via operator UI.

CEK-17 Yes

Key Deactivation

Deactivation is identical to revocation for API keys; sub-processor lifecycle per their controls.

CEK-18 N/A

Key Archival

RiskAlign-issued keys are not archived (no need: re-issue is one click). Sub-processor practice per their controls.

CEK-19 Yes

Key Compromise

Suspected compromise ? revoke + re-issue + audit-trail entry + tenant-admin notification.

CEK-20 N/A

Key Recovery

Tenant API keys cannot be recovered after revocation; sub-processor key recovery per their controls.

CEK-21 Yes

Key Inventory Management

Active keys listed at `/admin/api-keys` per tenant; webhook secrets at `/admin/regulator-endpoints`.

DCS - Datacenter Security

DCS-01 N/A

Off-Site Equipment Disposal Policy and Procedures

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-02 N/A

Off-Site Transfer Authorization Policy and Procedures

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-03 N/A

Secure Area Policy and Procedures

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-04 N/A

Secure Media Transportation Policy and Procedures

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-05 Yes

Assets Classification

Logical asset classification (data classification at table level, sensitivity tagged via `data_classification` column). Physical-asset classification N/A.

DCS-06 Yes

Assets Cataloguing and Tracking

Logical asset inventory in `data-model-map.md` and `architecture-overview.md`. Physical assets N/A.

DCS-07 N/A

Controlled Access Points

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-08 N/A

Equipment Identification

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-09 N/A

Secure Area Authorization

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-10 N/A

Surveillance System

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-11 N/A

Unauthorized Access Response Training

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-12 N/A

Cabling Security

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-13 N/A

Environmental Systems

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-14 N/A

Secure Utilities

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DCS-15 N/A

Equipment Location

N/A - RiskAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DSP - Data Security & Privacy Lifecycle Management

DSP-01 Yes

Security and Privacy Policy and Procedures

Published privacy notice + DPIA template (`06_DPIA_Template.md`); JOIC-registered controller/processor (No. 103914).

DSP-02 Yes

Secure Disposal

Tenant deletion = hard delete + audit-trail entry. Backups expire per `15_Data_Retention_and_Deletion.md`.

DSP-03 Yes

Data Inventory

Full data inventory in `data-model-map.md`; per-table sensitivity tagging.

DSP-04 **Yes**

Data Classification

`data_classification` column on tenant rows; `live_PROHIBITED` on pilot/sandbox tenants until uplift.

DSP-05 **Yes**

Data Flow Documentation

Data flow diagram + sub-processor map in `architecture-overview.md` and `14_Sub_Processor_List.md`.

DSP-06 **Yes**

Data Ownership and Stewardship

Tenant = data owner; RiskAlign = processor for tenant data, controller for account data. Documented in Pilot Agreement Sec.3.

DSP-07 **Yes**

Data Protection by Design and Default

RLS-by-default on every table; tenant isolation enforced at query layer.

DSP-08 **Yes**

Data Privacy by Design and Default

Minimum-necessary data collection; no special-category data accepted (enforced via upload guards).

DSP-09 **Yes**

Data Protection Impact Assessment

DPIA template provided to every tenant (`06_DPIA_Template.md`); founder DPIA performed at architecture-change time.

DSP-10 **Yes**

Sensitive Data Transfer

All transfers TLS 1.2+; EU-only sub-processors for data path.

DSP-11 **Yes**

Personal Data Access, Reversal, Rectification and Deletion

Operator UI supports DSAR / rectification / erasure; export at `/admin/data-export`.

DSP-12 **Yes**

Limitation of Purpose in Personal Data Processing

Documented in Pilot Agreement Sec.3; tenant data not used for product improvement without explicit consent.

DSP-13 **Yes**

Personal Data Sub-processing

Public sub-processor list at `riskalignplatform.com/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement Sec.7.

DSP-14 **Yes**

Disclosure of Data Sub-processors

Public sub-processor list at `riskalignplatform.com/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement Sec.7.

DSP-15 **Yes**

Limitation of Production Data Use

Production data never used in dev/test; pilot/sandbox tenants flagged with `live_PROHIBITED` and enforce upload guards.

DSP-16 **Yes**

Data Retention and Deletion

Published policy at `15_Data_Retention_and_Deletion.md`; tenant-level retention overrideable per Pilot Agreement.

DSP-17 **Yes**

Sensitive Data Protection

No special-category data accepted; enforced by upload guards + onboarding checklist.

DSP-18 Yes

Disclosure Notification

Breach-notification SLA: 24h to tenant + JOIC per DPJL 2018; documented in BCP outline and Pilot Agreement Sec.8.

DSP-19 Yes

Data Location

All tenant data resides in EU (Lovable Cloud EU region). Cloudflare edge does not persist tenant data.

GRC - Governance, Risk & Compliance

GRC-01 Yes

Governance Program Policy and Procedures

Governance documented in `docs/canonical/` (Trust Pack, Sub-processor list, BCP, DPIA, Retention, VDP, AI-use disclosure).

GRC-02 Yes

Risk Management Program

Internal risk register + SWOT (`01_SWOT_v2.md`); reviewed every release.

GRC-03 Yes

Organizational Policy Reviews

Canonical docs reviewed at every release; review log in `.lovable/handover/`.

GRC-04 Yes

Policy Exception Process

Exceptions logged in `issues` with sign-off + audit-trail; documented in Pilot Agreement Sec.6.

GRC-05 Yes

Information Security Program

Trust Pack (`32_Trust_Pack.md`) is the published programme summary.

GRC-06 Yes

Governance Responsibility Model

Founder is accountable owner; successor role scoped in `16_Successor_Role_Spec.md`.

GRC-07 Yes

Information System Regulatory Mapping

Regulatory mapping per `25_Pilot_Prospectus.md` (JFSC AML/CFT/CPF, DPJL 2018) and the in-product Compass methodology.

GRC-08 Yes

Special Interest Groups

Founder participates in CSA / FCA / JFSC discussion channels; subscribes to ENISA + NCSC advisories.

HRS - Human Resources Security

HRS-01 N/A

Background Screening Policy and Procedures

N/A - single founder; no employees. Will adopt policy at first hire.

HRS-02 Yes

Acceptable Use of Technology Policy and Procedures

Acceptable-use embedded in founder operating procedure; will formalise at first hire.

HRS-03 Yes

Clean Desk Policy and Procedures

Founder operates browser-only; no printed customer data; locked workspace when away.

HRS-04 Yes

Remote and Home Working Policy and Procedures

Single home-office; disk-encrypted laptop; MFA on every privileged account.

HRS-05 N/A

Asset returns

N/A - no employees / no issued assets.

HRS-06 N/A

Employment Termination

N/A - no employees yet.

HRS-07 N/A

Employment Agreement Process

N/A - no employees yet.

HRS-08 N/A

Employment Agreement Content

N/A - no employees yet. Sub-processor contracts cover equivalent obligations.

HRS-09 Yes

Personnel Roles and Responsibilities

Founder role + successor role spec in `16_Successor_Role_Spec.md`. Second-operator brief in `17_Second_Operator_Brief.md`.

HRS-10 Yes

Non-Disclosure Agreements

Mutual NDA template available; signed with every pilot prospect before sharing diligence pack.

HRS-11 Yes

Security Awareness Training

Founder maintains CPD; will formalise programme at first hire.

HRS-12 Yes

Personal and Sensitive Data Awareness and Training

Founder DPO-equivalent; maintains data-protection CPD.

HRS-13 Yes

Compliance User Responsibility

Tenant user responsibilities documented in Pilot Agreement Sec.4 and the in-product onboarding checklist.

IAM - Identity & Access Management

IAM-01 Yes

Identity and Access Management Policy and Procedures

Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack Sec.4.

IAM-02 Yes

Strong Password Policy and Procedures

Supabase Auth password policy: min 12 chars, breach-list check via HIBP, no max length.

IAM-03 Yes

Identity Inventory

All identities in `auth.users` + `public.tenant_users`; operator review at `/admin/tenant-users`.

IAM-04 **Yes**

Separation of Duties

Maker-checker workflow on regulatory adoption; admin / cco / mlro / board roles separated. Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack Sec.4.

IAM-05 **Yes**

Least Privilege

Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack Sec.4.

IAM-06 **Yes**

User Access Provisioning

Tenant-admin invites + named roles; audit-trailed.

IAM-07 **Yes**

User Access Changes and Revocation

Role changes + offboarding via `/admin/tenant-users`; immediate effect; audit-trailed.

IAM-08 **Yes**

User Access Review

Quarterly access review prompt on `/admin/tenant-users`; results captured in audit trail.

IAM-09 **Yes**

Segregation of Privileged Access Roles

`sandbox_admin` (founder cross-tenant) is separate from per-tenant `admin`.

IAM-10 **Yes**

Management of Privileged Access Roles

Privileged roles grant logged in `user_roles` + audit-trailed; manual approval required.

IAM-11 **Yes**

CSCs Approval for Agreed Privileged Access Roles

Founder cross-tenant access is documented in Pilot Agreement Sec.5; tenant can revoke at any time.

IAM-12 **Yes**

Safeguard Logs Integrity

Append-only audit-trail with SHA-256 hash chain; per-page verifier at `riskalignplatform.com/verify`. See Trust Pack Sec.6.

IAM-13 **Yes**

Uniquely Identifiable Users

Every action stamped with `auth.uid()` + tenant; no shared accounts.

IAM-14 **Yes**

Strong Authentication

MFA-enforced for founder accounts (RiskAlign). MFA-enforced for tenant admins on roadmap (queued).

IAM-15 **Yes**

Passwords Management

Supabase Auth; bcrypt-hashed; reset via verified email; no plaintext storage.

IAM-16 **Yes**

Authorization Mechanisms

RLS + has_role() security-definer functions; documented in `architecture-overview.md`.

IPY - Interoperability & Portability

IPY-01 **Yes**

Interoperability and Portability Policy and Procedures

Documented data-export commitment in Pilot Agreement Sec.9.

IPY-02 **Yes**

Application Interface Availability

Public REST API v1 at `/api/public/v1/*`; contract PDF in `public/downloads/canonical/public-api-contract.pdf`.

IPY-03 **Yes**

Secure Interoperability and Portability Management

API authenticated with bearer tokens; webhooks signed HMAC-SHA256.

IPY-04 **Yes**

Data Portability Contractual Obligations

Pilot Agreement Sec.9 commits to CSV/JSON export of all tenant data on request, format documented in `public-api-contract.md`.

IVS - Infrastructure & Virtualization Security

IVS-01 **Yes**

Infrastructure and Virtualization Security Policy and Procedures

Infrastructure offloaded to Cloudflare Workers + Lovable Cloud (Supabase EU). RiskAlign-side policy in `architecture-overview.md`.

IVS-02 **Yes**

Capacity and Resource Planning

Managed-platform auto-scale (Cloudflare Workers, Supabase). Capacity review at every architecture change.

IVS-03 **Yes**

Network Security

Cloudflare WAF + DDoS protection; TLS-only ingress; egress to known sub-processors only.

IVS-04 **N/A**

OS Hardening and Base Controls

N/A - no host OS managed by RiskAlign. Workers + managed Postgres.

IVS-05 **Yes**

Production and Non-Production Environments

Separate Lovable preview + published environments; pilot/sandbox tenants flagged `live_PROHIBITED`.

IVS-06 **Yes**

Segmentation and Segregation

Multi-tenant logical segregation via RLS; no shared schema for tenant data without `tenant_id` scoping.

IVS-07 **N/A**

Migration to Cloud Environments

N/A - cloud-native since inception; no on-prem migration.

IVS-08 **Yes**

Network Architecture Documentation

Documented in `architecture-overview.md` and `data-model-map.md`.

IVS-09 **Yes**

Network Defense

Cloudflare WAF + bot mitigation; Sentry alerting on server errors; rate-limiting on `/api/public/*`.

LOG - Logging & Monitoring

LOG-01 **Yes**

Logging and Monitoring Policy and Procedures

Logging policy: every state-changing action audit-trailed; security events to Sentry. Append-only audit-trail with SHA-256 hash chain; per-page verifier at `riskalignplatform.com/verify`. See Trust Pack Sec.6.

LOG-02 Yes

Audit Logs Protection

Append-only + SHA-256 hash chain (sealed). Tampering detectable at `/verify`.

LOG-03 Yes

Security Monitoring and Alerting

Sentry (browser + server); founder receives alert on errors and suspicious patterns.

LOG-04 Yes

Audit Logs Access and Accountability

Audit-trail read scoped by RLS to tenant admins + sandbox_admin; every read is itself audit-trailed for privileged roles.

LOG-05 Yes

Audit Logs Monitoring and Response

Founder reviews critical audit events daily; alerts via Sentry.

LOG-06 Yes

Clock Synchronization

All timestamps from managed-platform NTP (Cloudflare, Supabase). UTC stored, UI localises.

LOG-07 Yes

Logging Scope

Audit scope: auth events, role changes, data CRUD, exports, adoptions, escalations, attestation pack composition, key issuance/revocation.

LOG-08 Yes

Log Records

Per-event record: actor (`auth.uid()`), tenant, entity, action, timestamp, prior-hash, current-hash.

LOG-09 Yes

Log Protection

Append-only audit-trail with SHA-256 hash chain; per-page verifier at `riskalignplatform.com/verify`. See Trust Pack Sec.6.

LOG-10 Partial

Encryption Monitoring and Reporting

TLS health monitored by Cloudflare; at-rest encryption status reported by Supabase. No internal crypto-monitoring dashboard yet.

LOG-11 Yes

Transaction/Activity Logging

Append-only audit-trail with SHA-256 hash chain; per-page verifier at `riskalignplatform.com/verify`. See Trust Pack Sec.6.

LOG-12 Yes

Access Control Logs

Role grants/revocations + auth events captured in audit trail + Supabase Auth logs.

LOG-13 Yes

Failures and Anomalies Reporting

Sentry captures errors; weekly review by founder; high-severity alerts immediate.

SEF - Security Incident Management, E-Discovery & Cloud Forensics

SEF-01 Yes

Security Incident Management Policy and Procedures

Documented in BCP outline; 24h tenant notification SLA per Pilot Agreement Sec.8.

SEF-02 Yes

Service Management Policy and Procedures

Status page + incident comms via direct tenant-admin email.

SEF-03 Yes

Incident Response Plans

IR plan in `07_BCP_Outline.md`; founder = on-call; successor role spec in `16_Successor_Role_Spec.md`.

SEF-04 No

Incident Response Testing

Not yet tested live. Tabletop exercise scheduled Q3 2026.

SEF-05 Partial

Incident Response Metrics

Sentry MTTA/MTTR available; formal monthly metric report deferred.

SEF-06 Yes

Event Triage Processes

Sentry severity ? founder triage within 1 business hour during working hours.

SEF-07 Yes

Security Breach Notification

DPJL 2018 / UK GDPR-aligned: 72h to JOIC, 24h to tenants. Documented in Pilot Agreement Sec.8.

SEF-08 Yes

Points of Contact Maintenance

Security contact published at `riskalignplatform.com/vdp` and `riskalignplatform.com/trust`; tenant emergency contact captured at onboarding.

STA - Supply Chain Management, Transparency & Accountability

STA-01 Yes

SSRM Policy and Procedures

Shared-responsibility model documented in Trust Pack Sec.3 and `architecture-overview.md`.

STA-02 Yes

SSRM Supply Chain

Public sub-processor list at `riskalignplatform.com/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement Sec.7.

STA-03 Yes

SSRM Guidance

Pilot Agreement Sec.3 + Trust Pack Sec.3 spell out what RiskAlign vs the tenant is responsible for.

STA-04 Yes

SSRM Control Ownership

RACI documented in Trust Pack Sec.3.

STA-05 Yes

SSRM Documentation Review

Reviewed at every release + every sub-processor change.

STA-06 Yes

SSRM Control Implementation

Controls implemented per Trust Pack Sec.4-Sec.7; evidence in `docs/canonical/`.

STA-07 Yes

Supply Chain Inventory

Public sub-processor list at `riskalignplatform.com/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement Sec.7.

STA-08 Yes

Supply Chain Risk Management

Sub-processor risk reviewed before onboarding; certifications + region + SLAs captured in `14_Sub_Processor_List.md`.

STA-09 Yes

Primary Service and Contractual Agreement

Pilot Agreement scaffold at `05_Pilot_Agreement_Scaffold.md`.

STA-10 Yes

Supply Chain Agreement Review

Sub-processor contracts reviewed at renewal; security addenda in place where required.

STA-11 Partial

Internal Compliance Testing

Internal self-assessment (this document). External testing per AA-02.

STA-12 Yes

Supply Chain Service Agreement Compliance

Sub-processor SLAs monitored via status pages + Sentry.

STA-13 Yes

Supply Chain Governance Review

Sub-processor list reviewed quarterly; changes notified 30 days in advance per Pilot Agreement Sec.7.

STA-14 Yes

Supply Chain Data Security Assessment

Sub-processor security posture captured in `14_Sub_Processor_List.md`; only EU-region processors on data path.

TVM - Threat & Vulnerability Management

TVM-01 Yes

Threat and Vulnerability Management Policy and Procedures

Public VDP at `riskalignplatform.com/vdp`; remediation SLAs documented in `28_Vulnerability_Disclosure_Policy.md`.

TVM-02 N/A

Malware Protection Policy and Procedures

N/A - no host OS managed by RiskAlign; no user-uploaded executables; sub-processor anti-malware applies.

TVM-03 Yes

Vulnerability Remediation Schedule

Critical: 7 days; High: 30 days; Medium: 90 days; Low: best-effort. Per `28_Vulnerability_Disclosure_Policy.md`.

TVM-04 Yes

Detection Updates

Dependency-vulnerability scan in CI; managed-platform patching by sub-processors.

TVM-05 Yes

External Library Vulnerabilities

Dependency-scan on every build (npm audit + Lovable dependency scanner).

TVM-06 Partial

Penetration Testing

Continuous automated security scanning via Aikido (SAST, SCA, secrets, IaC, surface monitoring) is in place and clean of critical findings. Independent third-party human penetration test deferred until first paying pilot or named prospect request - see /security/roadmap and the engagement runbook at .lovable/pentest/runbook.md.

TVM-07 Yes

Vulnerability Identification

Dependency scan in CI + VDP submissions + Sentry error patterns.

TVM-08 Yes

Vulnerability Prioritization

CVSS-aligned; remediation slotted per TVM-03 schedule.

TVM-09 Partial

Vulnerability Management Reporting

Internal reporting only; formal report cadence deferred until first paying pilot.

TVM-10 Partial

Vulnerability Management Metrics

MTTR captured per VDP submission; broader metric reporting deferred.

UEM - Universal Endpoint Management

UEM-01 Yes

Endpoint Devices Policy and Procedures

Founder laptop only - disk encryption (FileVault), screen lock, OS auto-update, MFA on every privileged login. Limited applicability - RiskAlign has no employee fleet. Founder laptop only, with disk encryption + browser-only operator access. No MDM at this scale.

UEM-02 Yes

Application and Service Approval

Founder approves all software/services in use; documented in operating procedure.

UEM-03 Yes

Compatibility

Browser-only operator surface; supported in modern Chromium/Firefox/Safari.

UEM-04 Yes

Endpoint Inventory

Single founder endpoint inventoried. Tenant endpoints out-of-scope (tenant-managed).

UEM-05 Yes

Endpoint Management

Manual management on single founder endpoint. Limited applicability - RiskAlign has no employee fleet. Founder laptop only, with disk encryption + browser-only operator access. No MDM at this scale.

UEM-06 Yes

Automatic Lock Screen

Founder laptop auto-locks after 5 min inactivity.

UEM-07 Yes

Operating Systems

macOS current major release; auto-update enabled.

UEM-08 Yes

Storage Encryption

FileVault enabled on founder laptop.

UEM-09 Yes

Anti-Malware Detection and Prevention

macOS Gatekeeper + XProtect + System Integrity Protection.

UEM-10 Yes

Software Firewall

macOS application firewall enabled.

UEM-11 Partial

Data Loss Prevention

Operator surface is browser-only; no bulk export from founder endpoint. Formal DLP tooling N/A at single-founder scale.

UEM-12 N/A

Remote Locate

N/A - single founder endpoint; Find My Mac enabled for personal device recovery.

UEM-13 Yes

Remote Wipe

Find My Mac remote wipe enabled on founder laptop.

UEM-14 N/A

Third-Party Endpoint Security Posture

N/A - no third-party endpoints provisioned by RiskAlign.