Mabble Helix - SIG-Lite Pre-Filled Responses

This document holds Mabble's responses to the Shared Assessments Standardized Information Gathering Questionnaire - Lite (SIG-Lite) 2026 edition. SIG-Lite is the abbreviated form of the full SIG questionnaire and is the most common TPRM artefact requested by enterprise prospects in the United States.

Each row contains: question ID, question, Yes/No/Partial/N/A, supporting note, and the evidence pointer. Where a row cannot be auto-answered from code state, the answer is **"Manual attestation required"** and the Compliance Office routes the row per `README.md §3` before submission.

Cross-references to the CAIQ pack (`CAIQ_v4.0.3_responses.md`) appear in the Evidence column where the underlying control is the same; this avoids duplication.

A - Enterprise Risk Management

ID	Question	Answer	Notes	Evidence pointer
A.1.1	Is there a documented Enterprise Risk Management (ERM) programme?	Partial	The Mabble engineering Gauntlet (`Mabble engineering/`) is the most recent formal risk assessment, producing 12-dimension scorecards plus a sequenced P0/P1/P2/P3 remediation plan. A continuous risk register with a documented refresh cadence is a roadmap gap.	`Mabble engineering/reports/00_executive_summary.md`; `Mabble engineering/reports/50_remediation_to_100.md`
A.1.2	Is the ERM programme reviewed at least annually by senior management?	Manual attestation required	First annual review cycle starts in the launch quarter.	Compliance Office attestation

A.1.3	Is there a documented Information Security Policy (ISP) approved by senior management?	Partial	Engineering and security practices are documented across `CLAUDE.md`, `docs/`, and `Mabble engineering/`. A single canonical ISP document with an approval signature block is on the post-launch roadmap. Mabble engineering currently serves as the approving authority.	Compliance Office attestation; CAIQ GRM-01
A.1.4	Are key information security risks formally identified and treated?	Yes	Mabble engineering Gauntlet output identifies ~170 remediation items across 12 dimensions; the prioritised P0 / P1 backlog drives the engineering plan.	`Mabble engineering/reports/50_remediation_to_100.md`
A.1.5	Is cyber-insurance coverage in place?	Manual attestation required	Finance / Legal-controlled. Mabble engineering attestation needed before disclosure.	Mabble engineering / Finance attestation
A.1.6	Are exceptions to security policy logged and approved?	Yes	Mabble engineering authorisation required; exceptions are logged in `internal/decisions/`.	`internal/decisions/`

B - Security Policy

ID	Question	Answer	Notes	Evidence pointer
B.1.1	Is there a documented and approved Information Security Policy?	Partial	See A.1.3.	Compliance Office attestation
B.1.2	Are security policies communicated to all employees and contractors?	Yes	Onboarding requires acknowledgement of the contributor guide and security-sensitive change policy.	`CONTRIBUTING.md`; Mabble engineering / HR attestation
B.1.3	Are security policies reviewed at least annually?	Manual attestation required	First annual review starts in the launch quarter.	Compliance Office attestation

B.1.4	Are acceptable-use rules defined for all company systems?	Partial	An informal Acceptable Use Policy is communicated at onboarding. A formal signed AUP per employee is a roadmap gap.	Compliance Office attestation
B.1.5	Are violations of policy subject to disciplinary action?	Yes	Documented in the employment agreement.	Mabble engineering / HR attestation

C - Organisational Security

ID	Question	Answer	Notes	Evidence pointer
C.1.1	Is a senior executive accountable for information security?	Yes	The Mabble engineering is the executive owner of the information security programme. A dedicated CISO role is on the post-launch hiring plan.	Mabble engineering attestation
C.1.2	Are roles and responsibilities for information security clearly defined?	Partial	Engineering security responsibilities are documented in the contributor guide. Role-specific written statements for every role are a roadmap gap.	`CONTRIBUTING.md`; Compliance Office attestation
C.1.3	Is segregation of duties enforced?	Partial	Database `helix_admin` role is separate from the runtime `helix` role; admin elevation requires explicit session elevation. Application-layer SoD is informal at current company scale.	`db/schema/cortex/`; CAIQ HRS-11
C.1.4	Is contact with relevant authorities maintained (e.g., HHS OCR, EU DPAs)?	Yes	The Compliance Office maintains the contact list and is the single named contact in the BAA and DPA. EU customers are served via the interim DPO function (Compliance Office).	`docs/compliance/baa_template.md §13`; CAIQ §11

D - Asset and Information Management

ID	Question	Answer	Notes	Evidence pointer
D.1.1	Is there an inventory of all hardware and software assets?	Partial	Production infrastructure is enumerated in Terraform; container images carry their SBOM. Engineer endpoint inventory is informal at current company scale.	Terraform configs in repo; Compliance Office attestation
D.1.2	Is information classified by sensitivity?	Yes	All customer-uploaded vault data is treated as PHI / personal data and classified at the highest sensitivity tier by default. Records carry `purpose_of_use` and `jurisdiction` tags.	`db/schema/cortex/05_records.sql`; CAIQ DSI-01
D.1.3	Is data handling guidance documented?	Yes	The `docs/compliance/baa_template.md` Annex A enumerates permitted uses of PHI under HIPAA §164.504(e). Internal handling rules track the same enumeration.	`docs/compliance/baa_template.md`
D.1.4	Are removable media restricted?	Manual attestation required	Engineer endpoint policy item; current state is informal.	Compliance Office attestation
D.1.5	Is data labelled / marked in storage and transit?	Yes	Records carry tenant ID + `purpose_of_use` + `jurisdiction`; audit events carry the same.	`db/schema/cortex/05_records.sql`

E - Endpoint Security

Helix is a SaaS platform. Customer endpoints (laptops, mobile devices used to access the Helix console) are not under Helix's control. The following responses cover Helix-issued engineering endpoints; controls on the customer's own endpoints are the customer's responsibility.

ID	Question	Answer	Notes	Evidence pointer

E.1.1	Are anti-malware controls deployed on company-issued endpoints?	Partial	Engineer endpoints run macOS XProtect + Gatekeeper. Centrally managed EDR (CrowdStrike or equivalent) is on the post-launch roadmap.	Compliance Office attestation
E.1.2	Are company-issued endpoints subject to full-disk encryption?	Yes	FileVault encryption required on all engineer-issued / engineer-owned laptops; verified at onboarding.	Mabble engineering / HR attestation
E.1.3	Are company-issued endpoints centrally patched?	Partial	macOS automatic updates required; quarterly patch check performed informally. Centralised MDM-enforced patching is on the roadmap.	Compliance Office attestation
E.1.4	Are mobile device management (MDM) controls applied?	Partial	Enterprise MDM enrolment is on the post-launch roadmap. Current population of devices is small enough for manual oversight.	Compliance Office attestation
E.1.5	Are removable media controls applied on endpoints?	Manual attestation required	Endpoint policy item; current state is informal.	Compliance Office attestation
E.1.6	Do customer endpoints access the platform via secure channels (TLS)?	Yes	TLS 1.3 enforced on all customer-facing endpoints.	CAIQ EKM-03
E.1.7	Is endpoint access to customer data tracked and audited?	Yes	Capability-token issuance and use is audit-logged with the principal, scope, and purpose-of-use.	`internal/service/audit/...`; CAIQ IAM-07
E.1.8	Are endpoint configurations hardened to industry benchmarks (CIS, etc.)?	Partial	Container base images use Distroless or minimal Alpine. Engineer endpoint hardening to CIS macOS Benchmark is on the roadmap.	`Mabble engineering/reports/50_remediation_to_100.md`

F - Network Security

ID

Question

Answer

Notes

	Evidence pointer

F.1.1	Are network boundaries protected by firewalls?	Yes	AWS VPC + security groups + NACLs at the network layer; AWS WAF + CloudFront on the customer-facing console.	Terraform configs in repo; CAIQ IVS-01
F.1.2	Are intrusion detection / prevention systems deployed?	Partial	AWS GuardDuty enabled. Application-layer anomaly detection per IR-001. Falco runtime EBPF detection on production nodes is on the roadmap.	`mabble-runbooks/ir/ir-001-data-breach.md`; CAIQ IVS-03
F.1.3	Is network traffic encrypted in transit?	Yes	TLS 1.3 on all customer-facing endpoints. Internal mesh (RPC) traffic is encrypted via AWS PrivateLink + TLS.	CAIQ EKM-03
F.1.4	Are network segments isolated by sensitivity?	Yes	PHI-tier RDS, S3, and ElastiCache live in private subnets; only the API tier has egress.	Terraform configs in repo; CAIQ IVS-07
F.1.5	Are wireless networks protected by enterprise authentication?	N/A	Remote-first company; no corporate-managed wireless.	CAIQ IVS-10
F.1.6	Are remote access connections protected (VPN, bastion)?	Yes	Production access requires VPN + MFA + SSH bastion.	Mabble engineering attestation
F.1.7	Are DDoS protections in place?	Yes	AWS Shield Standard is automatic; AWS Shield Advanced is on the upgrade list for the launch quarter. AWS WAF + CloudFront absorbs Layer 7 traffic.	Terraform configs in repo
F.1.8	Are DNS configurations protected?	Yes	DNS managed via AWS Route 53 with DNSSEC enabled on customer-facing domains.	Terraform configs in repo

F.1.9	Are firewall and network rules reviewed periodically?	Partial	All network configuration is Terraform-managed; rule changes flow through PR review. Periodic full-rule audit is a roadmap item.	Terraform configs in repo

---

G - Identity and Access Management

ID	Question	Answer	Notes	Evidence pointer
G.1.1	Is multi-factor authentication required for administrative access?	Yes	WebAuthn passkey preferred; TOTP fallback; SMS supported but discouraged for admins. AMR tagging on every session.	CAIQ IAM-01
G.1.2	Is MFA available to customer end users?	Yes	All MFA factors are available to end users; customer admins may enforce MFA per tenant.	CAIQ IAM-01
G.1.3	Are user identities uniquely assigned?	Yes	Each principal has a stable QID; usernames are not reused.	`db/schema/cortex/02_users.sql`; CAIQ IAM-02
G.1.4	Are administrative accounts separated from regular user accounts?	Yes	`helix_admin` PostgreSQL role is separate from the runtime `helix` role.	`db/schema/cortex/`; CAIQ IAM-03
G.1.5	Are shared accounts prohibited?	Yes	All access is per-principal. Service identities use distinct credentials managed via AWS Secrets Manager.	CAIQ IAM-04
G.1.6	Are password policies enforced?	Yes	Argon2id hashing; minimum length and complexity at the API boundary; rotation for high-privilege accounts. WebAuthn passwordless preferred.	CAIQ IAM-05

G.1.7	Is access reviewed periodically?	Partial	RBAC entitlements are reviewable from `user_effective_roles` view at any time. Quarterly cadence is a roadmap item.	`db/schema/cortex/...rbac...`; CAIQ IAM-06
G.1.8	Is privileged access logged?	Yes	All capability-token issuance and use is audit-logged with scope, principal, resource, and purpose-of-use.	CAIQ IAM-07
G.1.9	Are session timeouts enforced?	Yes	Fixed-window expiry plus idle-inactivity re-auth. HTTP-only session cookies; no JWT in localStorage.	CAIQ IAM-09
G.1.10	Are federation protocols supported (SAML, OIDC, SCIM)?	Yes	SAML 2.0 (SP + IdP), OIDC, SCIM 2.0 supported.	CAIQ IAM-11
G.1.11	Is access provisioning and de-provisioning automated?	Yes	SCIM 2.0 in production; on customer termination, SCIM `active=false` revokes within <=5 seconds via CAEP-style propagation.	CAIQ HRS-07
G.1.12	Are dormant accounts disabled?	Partial	The identity provider is the single source of truth; customer admins are responsible for dormant-account lifecycle on the customer-tenant side. Helix internal account lifecycle is Mabble engineering-managed.	Mabble engineering attestation
G.1.13	Is least privilege enforced (RBAC)?	Yes	Group RBAC + `user_effective_roles` view + capability token scopes; PostgreSQL RLS + FORCE RLS on every PII-bearing table.	`db/schema/cortex/` RLS policies; CAIQ IAM-12

G.1.14	Is just-in-time (JIT) privileged access supported?	Yes	Admin operations require a capability-token elevation flow scoped to the operation. Long-lived broad admin tokens are not issued.	`internal/service/capability/...`

H - Application Security

ID	Question	Answer	Notes	Evidence pointer
H.1.1	Does the SDLC follow an industry framework (OWASP ASVS, BSIMM)?	Yes	OWASP ASVS Level 2 informs the test plan.	`CONTRIBUTING.md`; CAIQ AIS-01
H.1.2	Are security requirements defined for each release?	Partial	Critic skills run pre-release (`internal/critics/30_cso_review.md`). A formal per-release security requirements matrix is a roadmap item.	`internal/critics/30_cso_review.md`
H.1.3	Are secure coding practices documented?	Yes	The contributor guide enforces secure-coding rules: parameterised SQL, no string concatenation in queries, capability-token scope checks per RPC, no PII in logs.	`CONTRIBUTING.md`
H.1.4	Is code reviewed before merge?	Yes	All PRs require a reviewer signoff. Security-sensitive changes require a second engineer signoff.	`CONTRIBUTING.md`
H.1.5	Are static analysis tools (SAST) used?	Yes	`go vet`, `gosec`, Trivy, and Dependabot run on every PR.	`.github/workflows/`; CAIQ TVM-01
H.1.6	Are dynamic application security tests (DAST) performed?	No	DAST is on the post-launch roadmap.	`internal/compliance/README.md §5`

H.1.7	Are penetration tests performed at least annually?	No	External pen test is not yet engaged. Planned for the 6-month launch window.	`internal/compliance/README.md §5`; CAIQ IVS-06
H.1.8	Are third-party libraries tracked for vulnerabilities?	Yes	Dependabot + Trivy + Go module integrity checks.	`.github/workflows/`; CAIQ STA-05
H.1.9	Are application secrets stored securely?	Yes	AWS Secrets Manager via External Secrets Operator. No secrets in environment files committed to Git.	`internal/research/20_helix_inventory.md §Secrets`
H.1.10	Are input validation and output encoding enforced?	Yes	Protobuf schemas validate every API input; output is canonical JSON. Server-side schema validation of `vault.config` JSONB payload is the named gap (G-1.1).	`api/proto/v1/`; CAIQ AIS-03
H.1.11	Are CSRF / XSS / injection protections in place?	Yes	HTTP-only cookies, SameSite=Lax, Content Security Policy on the console, parameterised SQL throughout. Output encoded via React's default escaping.	`apps/console/`; CAIQ AIS-03
H.1.12	Is software bill of materials (SBOM) produced for releases?	Partial	CI generates SBOM for container images. Customer-facing SBOM publication is on the roadmap.	CAIQ STA-04
H.1.13	Are releases digitally signed?	Yes	Container images cosigned (Sigstore Cosign).	CAIQ STA-07

I - Data Security

ID	Question	Answer	Notes	Evidence pointer
I.1.1	Is customer data classified by sensitivity?	Yes	All customer-uploaded data classified at the highest sensitivity tier by default.	CAIQ DSI-01

I.1.2	Is data isolation enforced between tenants?	Yes	PostgreSQL RLS + FORCE RLS on every PII-bearing table; per-tenant DEK pool; capability-token scoping per RPC.	`db/schema/cortex/` RLS policies; CAIQ IVS-02
I.1.3	Is data retention enforced per a documented policy?	Yes	HIPAA 6-year default for audit logs (7-year actual retention with S3 Object Lock COMPLIANCE). Vault records carry a `purge_after` field. Per-jurisdiction retention via R-P1.14.	CAIQ DSI-03
I.1.4	Is data destruction performed at end of retention?	Yes - via crypto-shred	Crypto-shred for GDPR Art. 17 erasure (R-P1.13). Mid-relationship 90-day backup residual exposure disclosed in BAA §11.3.1.	CAIQ DSI-02
I.1.5	Are backup copies of data encrypted?	Yes	AWS RDS encrypted snapshots + S3 SSE-KMS on archived backups.	Terraform configs in repo
I.1.6	Is production data used in non-production?	No	Synthetic data only in dev / staging.	CAIQ DSI-05
I.1.7	Is data residency / sovereignty supported?	Partial	Per-tenant Data Residency Registry (DRS, R-P1.22) implemented. Default us-east-1; EU routing to eu-west-1 on request.	CAIQ DSI-07
I.1.8	Is a DSAR / subject-rights workflow available?	Yes	Full DSAR workflow (Phase 1-1.7): subject lookup, package, redact, deliver, audit.	`internal/service/dsar/...`
I.1.9	Are tenants able to extract their data on demand?	Yes	Bulk export via the gRPC and REST API.	CAIQ IPY-03
I.1.10	Is data returned or destroyed on contract termination?	Yes	Per BAA §11 - at customer's option.	`docs/compliance/baa_template.md §11`

J - Encryption and Key Management

ID	Question	Answer	Notes	Evidence pointer
J.1.1	Is data encrypted at rest?	Yes	AES-256-GCM per-record application-layer encryption plus AWS-managed disk encryption underneath.	CAIQ EKM-01
J.1.2	Is data encrypted in transit?	Yes	TLS 1.3 customer-facing; TLS internal RPC.	CAIQ EKM-03
J.1.3	Are encryption keys managed in a KMS?	Yes	AWS KMS holds root CMKs. Per-tenant DEKs envelope-wrapped, stored in app DB, never persisted unwrapped.	CAIQ EKM-01
J.1.4	Are keys rotated on a schedule?	Yes	DEKs auto-rotated; KMS CMKs on AWS annual rotation; manual `RotateRootKey` for transactional re-wrap.	CAIQ EKM-02
J.1.5	Are cryptographic algorithms approved (e.g., FIPS 140-2 / 140-3)?	Yes	AES-256-GCM, HMAC-SHAKE-256, Ed25519, Argon2id. AWS KMS HSM-backed root keys are FIPS 140-3 validated by AWS.	CAIQ EKM-04
J.1.6	Is Bring Your Own Key (BYOK) supported?	Yes - opt-in	BYOK (R-P1.12) opt-in per tenant; default keys remain Helix-managed.	`internal/service/encryption/pool.go`
J.1.7	Is Hold Your Own Key (HYOK) / external HSM supported?	Partial	AWS CloudHSM (FIPS 140-3 L3) is an opt-in for BYOK customers. Customer-hosted HSM (true HYOK) is not yet supported.	`internal/compliance/README.md §6`
J.1.8	Is post-quantum cryptography on the roadmap?	Yes	Post-quantum hybrid key wrap (R-P2.03) on the roadmap. HMAC-SHAKE-256 for blind-index search tokens is a PQ-ready primitive in production today.	`Mabble engineering/reports/50_remediation_to_100.md`

J.1.9	Are encryption controls verifiable by the customer?	Yes - via audit log	Audit events record encryption operations; Merkle proofs available per event; external anchoring via Sigstore Rekor (D-005).	`internal/decisions/` D-005

K - Logging and Monitoring

ID	Question	Answer	Notes	Evidence pointer
K.1.1	Are security-relevant events logged?	Yes	Authentication, authorisation, record CRUD, capability-token issuance / use, configuration changes - all logged.	`internal/service/audit/...`
K.1.2	Are logs tamper-resistant?	Yes	RFC 6962 Merkle chain anchored daily to Sigstore Rekor (D-005). Immutable trigger + TRUNCATE block on the underlying table (R-P0.05).	CAIQ IAM-10
K.1.3	Are logs centralised?	Yes	All audit events flow into the central audit pipeline backed by the outbox pattern (R-P0.08) and durable NATS (R-P1.11).	`internal/service/audit/...`
K.1.4	Are logs retained for a defined period?	Yes	7-year retention with S3 Object Lock COMPLIANCE.	CAIQ DSI-03
K.1.5	Are logs monitored for anomalies?	Partial	SLO + alerts (R-P1.20) on operational metrics. Application-layer anomaly detection (e.g., abnormal access patterns) is partial; full SIEM is on the post-launch roadmap.	`docs/slo.md`; `mabble-runbooks/ir/ir-001-data-breach.md`
K.1.6	Are administrator actions logged separately?	Yes	Admin-level capability-token issuance is flagged in the audit pipeline.	CAIQ IAM-07

K.1.7	Is time synchronisation maintained on all log sources?	Yes	AWS NTP service used cluster-wide.	CAIQ IVS-11

L - Incident Response

ID	Question	Answer	Notes	Evidence pointer
L.1.1	Is there a documented incident response plan?	Yes	IR runbooks at `mabble-runbooks/ir/` cover breach, credential compromise, insider threat. Public-disclosable runbook at `internal/compliance/breach_notification_runbook.md`.	CAIQ SEF-01
L.1.2	Is the incident response plan tested?	Partial	Sub-component drills run informally. A full tabletop exercise has not yet been logged in 2026.	CAIQ SEF-02
L.1.3	Are incidents tracked from detection to closure?	Yes	Incident ticketing + after-action review per IR runbook. Breach incident workflow (R-P1.19) supports end-to-end tracking with regulatory deadline timers.	`mabble-runbooks/ir/`; CAIQ SEF-03
L.1.4	Are breach notification commitments documented?	Yes	BAA §4 - <=30 calendar days. GDPR Art. 33 (<=72 hours to supervisory authority) and Art. 34 (without undue delay to data subjects).	`docs/compliance/baa_template.md §4`; `internal/compliance/breach_notification_runbook.md`
L.1.5	Are incident lessons-learned documented?	Yes	Post-incident review checklist per IR runbook; lessons captured in `internal/decisions/`.	`internal/decisions/`; CAIQ SEF-03
L.1.6	Is there 24x7 on-call coverage?	Partial	Informal coverage today; formal paid pager rotation planned post-launch.	`internal/compliance/README.md §5`

L.1.7	Are forensic capabilities documented?	Partial	Audit log + Merkle proofs provide non-repudiable evidence of system-level events. End-to-end forensic playbook is a roadmap item.	`internal/service/audit/...`; CAIQ SEF-04

M - Business Continuity and Disaster Recovery

ID	Question	Answer	Notes	Evidence pointer
M.1.1	Is there a documented Business Continuity Plan (BCP)?	Partial	Runbooks for individual failure scenarios exist; consolidated BCP document is on the post-launch roadmap.	CAIQ BCR-01
M.1.2	Is there a documented Disaster Recovery (DR) Plan?	Partial	Per-scenario DR runbooks exist. Consolidated DR plan is on the roadmap.	CAIQ BCR-01
M.1.3	Are RPO / RTO targets defined?	Yes	RTO <= 4h primary path; RPO <= 5 min via RDS Multi-AZ + WAL-G PITR.	`docs/slo.md`; CAIQ BCR-01
M.1.4	Are BCP / DR plans tested at least annually?	Manual attestation required	Mabble engineering attestation. Sub-component drills informal; full plan exercise not yet logged in 2026.	CAIQ BCR-02
M.1.5	Are backups encrypted and tested?	Yes / Partial	Backups encrypted with AWS KMS. Logged restoration drill in a clean account not yet completed (named gap).	CAIQ BCR-04
M.1.6	Are alternate processing facilities available?	Yes	AWS Multi-AZ within the primary region. Cross-region failover available on request (within the residency boundary).	CAIQ BCR-05
M.1.7	Is the BCP / DR plan updated after each material change?	Manual attestation required	Compliance Office attestation.	Compliance Office attestation

N - Compliance and Audit

ID	Question	Answer	Notes	Evidence pointer
N.1.1	Is the platform mapped to recognised compliance frameworks?	Yes	HIPAA Security Rule §164.308 / §164.310 / §164.312 (primary). GDPR Art. 28 / Art. 32 (secondary). CSA CCM v4 (architecture).	CAIQ AAC-03
N.1.2	Is SOC 2 Type II audit available?	No - not yet issued	SOC 2 Type II auditor not yet engaged. Planned for the 6-month launch window. Type I has not yet been issued either.	`internal/compliance/README.md §5`
N.1.3	Is ISO/IEC 27001 certification held?	No	Not pursued in the current phase.	`internal/compliance/README.md §5`
N.1.4	Is HITRUST CSF certification held?	No	Not pursued.	`internal/compliance/README.md §5`
N.1.5	Is PCI-DSS scope applicable?	N/A	Helix does not process card data. Billing is delegated.	CAIQ AAC-03
N.1.6	Are HIPAA Privacy / Security Rule obligations met?	Yes - as Business Associate	Helix is a Business Associate per §164.502(e); BAA template at `docs/compliance/baa_template.md`.	`docs/compliance/baa_template.md`
N.1.7	Are GDPR Art. 28 obligations met?	Yes - as Processor	Helix is a Processor for customer-uploaded personal data. DPA cover letter at `DPA_cover_letter.md`; SCC Module 2 supported.	`internal/compliance/DPA_cover_letter.md`
N.1.8	Are CCPA / CPRA obligations met (where applicable)?	Yes - as Service Provider	Service Provider status under CCPA §1798.140(ag). DSAR workflow supports right-to-know and deletion.	`internal/service/dsar/...`
N.1.9	Is an external audit programme in place?	No	Pen test, SOC 2, and external risk assessment not yet engaged. Planned for the 6-month launch window.	`internal/compliance/README.md §5`

N.1.10	Are sub-processors disclosed?	Yes	Canonical list at `docs/compliance/sub_processors.md`; Phase 4 vendor monitoring (R-P4.1) with diff alerts per tenant.	CAIQ STA-01

O - Third-Party / Sub-Processor Management

ID	Question	Answer	Notes	Evidence pointer
O.1.1	Is there a documented sub-processor / vendor management process?	Yes	`docs/compliance/sub_processors.md §3` sets the criteria. Phase 4 ROPA + vendor monitoring (R-P4) operationalises the diff-alert process.	`docs/compliance/sub_processors.md §3`; CAIQ STA-06
O.1.2	Are sub-processors required to meet equivalent security standards?	Yes	Per BAA §5 and GDPR Art. 28(4). Substantially the same obligations imposed in writing.	`docs/compliance/baa_template.md §5`; CAIQ STA-02
O.1.3	Are sub-processor changes notified to customers in advance?	Yes	>=30 days written notice; 14-day objection window; termination right on unresolved objection.	`docs/compliance/sub_processors.md §4`; CAIQ STA-03
O.1.4	Are sub-processor SOC 2 or equivalent reports reviewed?	Yes	Per onboarding criteria; reviewed annually or on material change.	`docs/compliance/sub_processors.md §3`
O.1.5	Is a right-to-audit clause present in sub-processor contracts?	Yes	Per `docs/compliance/sub_processors.md §3` row 5.	CAIQ STA-09
O.1.6	Are vendor data flows mapped?	Yes - at ROPA level	ROPA (R-P4 Phase 4) captures purpose, lawful basis, categories of data, sub-processors, retention, transfers.	`db/schema/cortex/14a_ropa_*.sql`
O.1.7	Are vendor risk tiers assigned?	Yes	See `internal/compliance/vendor_risk_matrix.md`.	`internal/compliance/vendor_risk_matrix.md`

P - Privacy

ID	Question	Answer	Notes	Evidence pointer
P.1.1	Is a Privacy Notice published?	Yes	Privacy Notice with version history (Phase 2).	Public-facing notice; ROPA reference
P.1.2	Is consent collected where required?	Yes	Consent Management Platform (CMP) with consent receipts, Global Privacy Control (GPC), and 13-month TTL (Phase 3).	`db/schema/cortex/15a_consent_*.sql`
P.1.3	Are data subject rights supported?	Yes	DSAR workflow (Phase 1-1.7): access, rectification, erasure (Art. 17), portability (Art. 20), restriction (Art. 18), objection (Art. 21).	`internal/service/dsar/...`
P.1.4	Is a Data Protection Officer (DPO) appointed?	Partial	Interim DPO function is performed by the Compliance Office (sales@mabble.ai). A formally appointed EU-resident DPO is planned for the launch quarter.	`internal/compliance/README.md §5`
P.1.5	Is a Record of Processing Activities (ROPA) maintained?	Yes	ROPA Art. 30 with draft / published / retired states (Phase 4).	`db/schema/cortex/14a_ropa_*.sql`
P.1.6	Are international data transfers covered by an appropriate transfer mechanism?	Yes	EU Standard Contractual Clauses Module 2 (Commission Implementing Decision (EU) 2021/914) covers Controller -> Processor transfers. UK IDTA available for UK transfers.	`internal/compliance/SCC_module_2_cover_letter.md`
P.1.7	Is a Transfer Impact Assessment (TIA) performed for each transfer?	Partial	Schrems II TIA template is in the DPIA framework. TIA is performed on customer request; standing TIA per region is a roadmap item.	`internal/compliance/DPIA_template.md`

P.1.8	Are DPIAs performed for high-risk processing?	Yes - process	DPIA template at `internal/compliance/DPIA_template.md`. Filled DPIAs archived in `internal/compliance/dpias/`.	`internal/compliance/DPIA_template.md`
P.1.9	Are purpose-of-use restrictions enforced?	Yes	Records carry `purpose_of_use` enum tags; capability tokens carry purpose-of-use scope; queries audit-logged with the purpose.	`db/schema/cortex/05_records.sql`
P.1.10	Are minors' data treated under special-category rules where applicable?	Yes	Lawful-basis tagging supports the special-category flag; consent requirements for minors apply under jurisdiction tagging (COPPA / Art. 8 GDPR).	`db/schema/cortex/...lawful_basis...`

Q - Personnel Security

ID	Question	Answer	Notes	Evidence pointer
Q.1.1	Are background checks performed on personnel with access to customer data?	Manual attestation required	HR-controlled. Informal at current company scale; formalised vendor-run checks are a roadmap item.	Mabble engineering / HR attestation
Q.1.2	Are non-disclosure agreements signed by all personnel?	Yes	NDA + confidentiality agreement signed on day of joining.	Mabble engineering / HR attestation
Q.1.3	Is security training delivered at onboarding?	Yes	Onboarding security training covers secure SDLC + HIPAA-aware data handling.	CAIQ HRS-04
Q.1.4	Is annual security training delivered?	Partial	Annual refresher is a roadmap item.	CAIQ HRS-04
Q.1.5	Are training records maintained?	Manual attestation required	HR-controlled; informal today.	Mabble engineering / HR attestation
Q.1.6	Are HR exit procedures defined?	Yes	Termination checklist: identity provider revocation, hardware return, access removal.	CAIQ HRS-07

Q.1.7	Are sanctions defined for security policy breaches?	Yes	Documented in the employment agreement.	Mabble engineering / HR attestation
Q.1.8	Are roles requiring elevated access subject to additional scrutiny?	Partial	Mabble engineering authorisation is required for production-prod database write access. Formal differentiated background checks for elevated roles are a roadmap item.	Mabble engineering / HR attestation

---

Summary statistics

Section	Total	Yes	Partial	No	N/A	Manual Attestation
A - Enterprise Risk Management	6	2	1	0	0	3
B - Security Policy	5	2	2	0	0	1
C - Organisational Security	4	2	2	0	0	0
D - Asset and Information Management	5	3	1	0	0	1
E - Endpoint Security	8	2	5	0	0	1
F - Network Security	9	6	2	0	1	0
G - Identity and Access Management	14	12	2	0	0	0
H - Application Security	13	9	2	2	0	0
I - Data Security	10	8	1	1	0	0
J - Encryption and Key Management	9	8	1	0	0	0
K - Logging and Monitoring	7	6	1	0	0	0
L - Incident Response	7	3	4	0	0	0

M - Business Continuity and DR	7	2	3	0	0	2
N - Compliance and Audit	10	5	0	4	1	0
O - Third-Party Management	7	7	0	0	0	0
P - Privacy	10	8	2	0	0	0
Q - Personnel Security	8	3	2	0	0	3
Total	**129**	**88**	**31**	**7**	**2**	**11**

(Manual attestation count = Compliance Office or HR / Mabble engineering attestation required before submission.)

Change log

Version	Date	Change
0.1.0	2026-05-14	Initial Track C publication.