Mabble Helix - CAIQ v4.0.3 Pre-Filled Responses

This document holds Mabble's responses to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) v4.0.3, mapped to the Cloud Controls Matrix (CCM) v4.0.

Each row contains: control ID, question, Yes/No/Not Applicable, notes that explain the answer, and the evidence pointer. Where a control is not yet implemented, the answer is "No" and the row says so. Where a row is unverifiable from code state (HR background checks, insurance limits, governance committee meeting frequency, etc.), the answer is **"Manual attestation required"** and the Compliance Office routes the row per `README.md §3` before submission.

A CSV companion of this file is at `CAIQ_v4.0.3_responses.csv` for import into TPRM tooling.

AAC - Audit Assurance & Compliance (4 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
AAC-01.1	Do you produce audit assertions using a structured industry-accepted format (e.g., CloudAudit/A6 URI Ontology, SCAP, CybOX, OCIL)?	No	Helix exposes audit data through purpose-built APIs (`/api/v1/audit/...`) rather than via CloudAudit/A6 today. RFC 6962 Merkle proofs are available per-event for tamper evidence. SCAP/CybOX mapping is a roadmap item.	`internal/api/v1/audit_handler.go`; `internal/research/20_helix_inventory.md §Audit`
AAC-02.1	Do you allow tenants to view your SOC 2 / ISO 27001 / equivalent independent third-party reports on request?	No	SOC 2 Type II auditor is not yet engaged. SOC 2 Type I has not yet been issued. Gap closure planned for the 6-month launch window. Customers receive instead: (a) the canonical control-mapping doc, (b) penetration test evidence when available, (c) BAA / DPA + sub-processor disclosure.	`internal/compliance/README.md §5`

AAC-02.2	Are reports of external audits made available to customers under NDA?	Not Applicable	No external attestation reports exist as of 2026-05-14. When SOC 2 Type II ships, this row becomes "Yes - under NDA via the Compliance Office."	`internal/compliance/README.md §5`
AAC-03.1	Do you map your internal compliance program to recognised frameworks (NIST 800-53, ISO 27001, CCM, HIPAA, PCI-DSS, etc.)?	Yes	HIPAA Security Rule §164.308 / §164.310 / §164.312 mapping is the primary control framework. GDPR Art. 28 / 32 mapping is the secondary framework. NIST 800-53 Rev.5 mapping is a roadmap item. PCI-DSS is out of scope (Helix does not process card data - billing is delegated to a future processor).	`docs/compliance/baa_template.md` Annex A; `internal/compliance/CAIQ_v4.0.3_responses.md` (this file)

AIS - Application & Interface Security (6 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
AIS-01.1	Do you use industry standards (OWASP ASVS, BSIMM) to build security into the SDLC?	Yes	OWASP ASVS Level 2 informs the test plan. Code review is mandatory per the contributor guide; security-sensitive changes require a second engineer signoff. Per GDPR Art. 32(1)(b) - ability to ensure ongoing confidentiality.	`CONTRIBUTING.md`; `internal/critics/30_cso_review.md`

AIS-01.2	Do you verify that all of your software suppliers adhere to industry standards for SDLC security?	Manual attestation required	Third-party supplier review process exists for sub-processors (see `docs/compliance/sub_processors.md §3`). Verification of the supplier's SDLC standards is not performed beyond reviewing their SOC 2 / equivalent attestation.	`docs/compliance/sub_processors.md §3`; Compliance Office attestation
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes	Helix does not grant a customer production access until: (a) BAA + DPA signed; (b) sub-processor disclosure acknowledged; (c) tenant provisioned with isolated key material (RLS + per-tenant DEK pool).	`docs/compliance/baa_template.md` Annex B; `internal/service/encryption/pool.go`
AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse?	Partial	AES-GCM authenticated encryption prevents undetected modification at rest (HIPAA §164.312(c)). Optimistic concurrency `version` on the `records` table prevents lost updates. Input validation at the API boundary uses protobuf schemas. Server-side schema validation of `vault.config` JSONB payload is a roadmap gap (G-1.1).	`internal/service/record/service.go`; `db/schema/cortex/04_vaults.sql`; `internal/research/20_helix_inventory.md §Dimension 1`

AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	Yes	CSA CCM v4 is the primary architecture reference. AWS Well-Architected Framework - Security pillar is the secondary. NIST SP 800-66 (HIPAA implementation guide) frames the HIPAA-specific architecture decisions.	`internal/research/10_truevault_capabilities.md`; `internal/research/20_helix_inventory.md`
AIS-04.2	Is each application or API access reviewed prior to granting access to ensure compatibility with security policies and integration requirements?	Yes	Capability tokens are issued only after a server-side scope check (`internal/service/capability/...`). No long-lived broad tokens. Per-RPC fail-closed authorization.	`internal/service/capability/service.go`; `internal/critics/30_cso_review.md §AuthZ`

BCR - Business Continuity & Operational Resilience (11 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
BCR-01.1	Do you have a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan?	Partial	Runbooks for individual failure scenarios exist (`mabble-runbooks/ir/`). A consolidated BCP/DR document is on the post-launch roadmap. RPO/RTO targets are documented in `docs/slo.md`.	`mabble-runbooks/ir/`; `docs/slo.md`
BCR-01.2	Do you have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?	Yes	RTO <= 4h for the primary user path; RPO <= 5 minutes (driven by RDS Multi-AZ + WAL-G PITR target).	`docs/slo.md`
BCR-01.3	Are tenants able to define their own RPO/RTO?	No	Tier-1 RPO/RTO is fixed at the platform level. Enterprise tenants may negotiate tighter targets contractually; this is not a self-service knob.	`docs/slo.md`

BCR-02.1	Are business continuity and disaster recovery plans tested at least annually?	Manual attestation required	Mabble engineering attestation needed. Sub-component tests (e.g., RDS failover on dev stack) are exercised informally; a full plan exercise has not yet been logged in 2026.	Compliance Office attestation
BCR-03.1	Does your data center have multiple physical infrastructure providers (e.g., diverse power, internet, etc.)?	Yes	AWS Multi-AZ across distinct AZs each with independent power and connectivity, per AWS data-center standard (SOC 2 + ISO 27001 documented). Helix does not operate its own data centers.	AWS SOC 2 report; `internal/research/20_helix_inventory.md §Reliability`
BCR-04.1	Are recovery and restoration capabilities documented and tested?	Partial	RDS automated backups + WAL-G PITR are configured and validated on the dev stack. A logged restoration drill in a clean account has not yet been completed.	`docs/slo.md`; Compliance Office attestation
BCR-05.1	Do you provide tenants with documentation showing the propagation of the AAA (authentication, authorization, and accounting) credentials across multiple data centers?	Yes	All authentication is centralised in the Helix identity service; capability scopes propagate via signed tokens consumed by RPCs in any AZ. Documented in `internal/research/20_helix_inventory.md §RBAC + Identity`.	`internal/service/auth/...`; `internal/research/20_helix_inventory.md`
BCR-06.1	Are physical security measures in place at the data centers used to host customer data (e.g., guards, surveillance, multi-factor entry, etc.)?	Yes	AWS data-center physical security per the AWS shared responsibility model and SOC 2 attestation. Helix has no physical premises hosting customer data.	AWS SOC 2 report; `docs/compliance/sub_processors.md`

BCR-07.1	Are there documented policies and procedures for the maintenance of equipment?	Yes - by AWS	Maintenance of physical equipment is AWS's responsibility under the shared responsibility model. Helix maintains its own software-only operational change-control process (see CCC).	AWS SOC 2 report; `internal/compliance/CAIQ_v4.0.3_responses.md` §CCC
BCR-08.1	Are uptime measurements published for tenant inspection?	Partial	An internal status page exists; a customer-facing status page is on the roadmap. SLO/SLI definitions are at `docs/slo.md`.	`docs/slo.md`
BCR-09.1	Do you have established policies and procedures around environmental and natural threats (fire, flood, etc.)?	Yes - by AWS	Per AWS SOC 2. Helix's own offices are remote-first; no customer data is held in office environments.	AWS SOC 2 report

---

CCC - Change Control & Configuration Management (5 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
CCC-01.1	Do you have a documented change management policy?	Yes	All production changes flow through Git -> PR review -> CI -> managed deploy. Database schema changes flow through `db/schema/cortex/` migration files. Per GDPR Art. 32(1)(d) - process for regular testing of effectiveness.	`db/schema/cortex/`; `CONTRIBUTING.md`
CCC-02.1	Is the use of unauthorised software prevented and detected?	Partial	Production runtime is container-image-based; only signed images deploy. Engineer endpoints are inventoried but not under enterprise MDM today (gap).	Compliance Office attestation

CCC-03.1	Are all changes tested prior to deployment to production?	Yes	CI runs unit + integration tests on every PR. Production deploys require green CI.	`.github/workflows/`; `CONTRIBUTING.md`
CCC-04.1	Are emergency changes authorised by an executive or change-control board?	Partial	Mabble engineering authorisation is required for an emergency production change. There is no formal change-control board at current company scale.	Compliance Office attestation
CCC-05.1	Are all configurations backed up and version-controlled?	Yes	Infra-as-code (Terraform / Helm / SQL migrations) is fully version-controlled in Git. AWS Config records resource state. Per HIPAA §164.308(a)(7)(ii)(D) - testing and revision.	`db/schema/cortex/`; Terraform configs in repo

---

DSI - Data Security & Information Lifecycle Management (7 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
DSI-01.1	Do you classify customer data based on sensitivity (e.g., public, internal, confidential, restricted)?	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 per HIPAA §164.502(b) / GDPR Art. 6(1) lawful-basis tagging.	`db/schema/cortex/05_records.sql`; `internal/research/20_helix_inventory.md §RBAC`

DSI-02.1	Do you support secure deletion (e.g., DOD 5220.22-M, NIST 800-88) of customer data?	Yes - via crypto-shred	Crypto-shred for GDPR Art. 17 erasure (R-P1.13) drops the wrapped DEK so the record becomes undecryptable. The mid-relationship 90-day backup residual exposure is disclosed in the BAA §11.3.1. Full key-rotation backup-aware erasure is available on customer request. NIST SP 800-88 Rev.1 media sanitisation applies at media end-of-life (handled by AWS).	`internal/service/encryption/...`; `docs/compliance/baa_template.md §11.3`
DSI-03.1	Do you have a data retention policy that allows tenants to define retention requirements?	Yes	Retention is enforced at row level: HIPAA 6-year default for audit logs, configurable per jurisdiction (R-P1.14). Vault records carry a `purge_after` field. DSAR fulfilment respects tenant-defined retention.	`db/schema/cortex/04_vaults.sql` (`purge_after`); `internal/research/20_helix_inventory.md §Audit`
DSI-04.1	Are all data lifecycles (creation, retention, use, secure destruction) documented?	Partial	Encryption + retention + crypto-shred are documented. A single canonical "data lifecycle map" is on the post-launch documentation roadmap.	`docs/compliance/baa_template.md §11`; `internal/research/20_helix_inventory.md`
DSI-05.1	Is production data ever used in non-production environments?	No	Dev/staging environments use synthetic data only. The dev AWS stack hosts test tenants belonging to Helix internal accounts (sales@mabble.ai system admin) and contains no customer PHI.	`internal/decisions/D-013_launch_timing_data_preservation.md`

DSI-06.1	Are tenant ownership rights documented and customer data accessible only to authorised personnel?	Yes	Per HIPAA §164.504(e), the customer (Covered Entity) is the owner of all uploaded PHI; Helix is the Business Associate. PostgreSQL RLS + FORCE RLS enforces tenant isolation at the database layer.	`db/schema/cortex/04_vaults.sql`; `docs/compliance/baa_template.md`
DSI-07.1	Do you support data residency / sovereignty controls?	Partial	Per-tenant Data Residency Registry (DRS, R-P1.22) is implemented. Default region is us-east-1. EU customer routing to eu-west-1 is supported on request. Cross-region failover within a residency boundary is the standard configuration.	`db/schema/cortex/...drs...`; `docs/compliance/sub_processors.md §5`

DCS - Datacenter Security (9 questions)

All datacenter physical security is fulfilled by AWS under the shared responsibility model. Helix does not operate its own data centers.

Control ID	Question	Yes/No	Notes	Evidence pointer
DCS-01.1	Are physical access controls in place at the data center?	Yes - by AWS	Documented in AWS's SOC 2 / ISO 27001 / PCI-DSS reports.	AWS SOC 2 report
DCS-02.1	Are visitor logs maintained and reviewed?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report
DCS-03.1	Are deliveries and physical equipment moves controlled?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report
DCS-04.1	Are equipment maintenance activities logged and supervised?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report
DCS-05.1	Are environmental controls (HVAC, fire suppression) in place?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report

DCS-06.1	Are environmental events monitored 24x7?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report
DCS-07.1	Are there documented destruction procedures for media at end-of-life?	Yes - by AWS	NIST SP 800-88 Rev.1 sanitisation, per AWS attestation. Helix layers crypto-shred on top at the application layer.	AWS SOC 2 report; `internal/service/encryption/...`
DCS-08.1	Are unauthorised attempts to access the data center logged and reviewed?	Yes - by AWS	Per AWS attestation.	AWS SOC 2 report
DCS-09.1	Are policies in place for the secure disposal of paper records containing customer data?	Not Applicable	Helix is software-only. No paper records contain customer data.	n/a

---

EKM - Encryption & Key Management (4 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
EKM-01.1	Are all encryption keys managed in a key management system (KMS)?	Yes	AWS KMS holds the root keys (CMKs). Per-tenant DEKs are envelope-wrapped under the tenant's CMK and stored in the application database; never persisted unwrapped. BYOK (R-P1.12) opt-in allows customer-managed CMKs. Per HIPAA §164.312(a)(2)(iv) - encryption and decryption. Per GDPR Art. 32(1)(a) - pseudonymisation and encryption.	`internal/service/encryption/pool.go`; `internal/service/encryption/rotate.go`; `internal/research/20_helix_inventory.md §Encryption`

EKM-02.1	Are keys rotated on a defined schedule?	Yes	DEKs are auto-rotated on usage threshold (modern table-backed pool: `RotationIntervalHours=24`). KMS root keys (CMKs) are subject to AWS KMS automatic annual rotation; manual rotation via `RotateRootKey` is supported as a transactional re-wrap of all tenant DEKs.	`internal/service/encryption/rotate.go` (`RotateRootKey` SerializableTx)
EKM-03.1	Is encryption used for data in transit (TLS 1.2 or above)?	Yes	TLS 1.3 enforced. TLS 1.2 deprecated. TLS 1.1 / 1.0 / SSL fully disabled. HSTS with preload on the customer-facing console.	TLS config (terminating LB); `internal/critics/30_cso_review.md`
EKM-04.1	Is the cryptographic algorithm strength sufficient for the data classification?	Yes	AES-256-GCM (authenticated encryption) per record. HMAC-SHAKE-256 for blind-index search tokens (PQ-ready primitive). Ed25519 for Sigstore Rekor audit-anchor signing. Argon2id for password hashing. Post-quantum hybrid key wrap is on the roadmap (R-P2.03) but not yet in production.	`internal/service/encryption/...`; `internal/research/20_helix_inventory.md §Encryption`

GRM - Governance & Risk Management (11 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer

GRM-01.1	Are policies for information security defined, documented, and approved by management?	Partial	Engineering and security practices are documented across `CLAUDE.md`, `docs/`, and `Mabble engineering/`. A single canonical "Information Security Policy" document approved with a signature block is on the post-launch roadmap. Mabble engineering currently serves as the approving authority.	Compliance Office attestation
GRM-02.1	Are policies reviewed at least annually or after a major change?	Manual attestation required	First annual review cycle starts in the launch quarter.	Compliance Office attestation
GRM-03.1	Is a senior management member responsible for the information security program?	Yes	The Mabble engineering is the executive owner of the information security program. A dedicated CISO role is on the post-launch hiring plan.	Compliance Office attestation
GRM-04.1	Are security responsibilities documented for all personnel with access to customer data?	Partial	All Helix engineers operate under the unified contributor guide and the security-sensitive change policy. Role-specific security responsibility statements (e.g., "the on-call engineer is responsible for X") are a roadmap gap.	`CONTRIBUTING.md`; Compliance Office attestation
GRM-05.1	Are security risks identified, assessed, and treated using a documented risk management program?	Partial	The Mabble engineering Gauntlet (`Mabble engineering/`) is the most recent formal risk assessment, producing 12-dimension scorecards + ~170 remediation items + a sequenced P0/P1/P2/P3 remediation plan. A continuous risk register with refresh cadence is a roadmap gap.	`Mabble engineering/reports/00_executive_summary.md`; `Mabble engineering/reports/50_remediation_to_100.md`

GRM-06.1	Are exceptions to security policy reviewed and approved?	Yes	Mabble engineering authorisation required. Exceptions are logged in the Mabble engineering's decisions index.	`internal/decisions/D-000_open_decisions.md`
GRM-07.1	Are violations of policy disciplinary action items?	Manual attestation required	HR policy document - Mabble engineering attestation needed.	Compliance Office attestation
GRM-08.1	Is an Information Security Management System (ISMS) defined and operated?	Partial	ISMS scope is documented (`internal/research/20_helix_inventory.md`). Formal ISO 27001 certification is not pursued in the current phase.	`internal/research/20_helix_inventory.md`
GRM-09.1	Are residual security risks accepted by management in writing?	Yes	Mabble engineering signs off on each release; residual risks are logged in `internal/decisions/`.	`internal/decisions/`
GRM-10.1	Is there an Acceptable Use Policy (AUP) covering Helix systems?	Partial	An informal AUP is communicated at onboarding. A formal signed AUP per employee is a roadmap gap.	Compliance Office attestation
GRM-11.1	Are independent risk assessments performed annually?	No	Pen test engagement and external risk assessment are not yet engaged. Planned for the 6-month launch window.	`internal/compliance/README.md §5`

HRS - Human Resources Security (11 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
HRS-01.1	Are background checks performed on all employees with access to customer data?	Manual attestation required	HR-controlled. Pre-launch headcount is small; background checks are performed informally by the Mabble engineering. Formalised vendor-run checks are a roadmap item.	Mabble engineering / HR attestation

HRS-02.1	Are non-disclosure agreements (NDAs) executed by all employees and contractors?	Yes	All employees and contractors sign an NDA + confidentiality agreement on the day of joining.	Mabble engineering / HR attestation
HRS-03.1	Are roles and responsibilities for security clearly defined in employment contracts?	Yes	Employment agreements reference the Helix Security & Acceptable Use Policy; obligations survive termination.	Mabble engineering / HR attestation
HRS-04.1	Are security awareness training programs delivered to all personnel?	Partial	Engineers complete onboarding security training (covers secure SDLC + HIPAA-aware data handling). Annual refresher is a roadmap item.	Compliance Office attestation
HRS-05.1	Are training records maintained for security awareness training?	Manual attestation required	HR-controlled; current state is informal.	Mabble engineering / HR attestation
HRS-06.1	Are mobile devices subject to a documented security policy?	Partial	Engineers operate on owned laptops; FileVault encryption + screen lock + automatic patching are required. Enterprise MDM enrolment is on the roadmap.	Compliance Office attestation
HRS-07.1	Is access revoked upon termination?	Yes	Identity provider revocation is the single source of truth; capability tokens issued to the user are revoked within <=5 seconds via CAEP-style propagation (MYC-5-08). Hardware return is part of the termination checklist.	`internal/service/auth/...` ; Mabble engineering / HR attestation
HRS-08.1	Is there a return-of-assets process at termination?	Yes	Hardware, credentials, and physical access are returned per the termination checklist.	Mabble engineering / HR attestation

HRS-09.1	Are employees informed that monitoring of their use of company systems may take place?	Yes	Stated in the employment agreement + acceptable use policy.	Mabble engineering / HR attestation
HRS-10.1	Are disciplinary processes defined for breach of security policy?	Yes	Documented in the employment agreement.	Mabble engineering / HR attestation
HRS-11.1	Is segregation of duties implemented to reduce risk of accidental or intentional misuse?	Partial	Table-owner role is split from app-runtime role at the database layer (per `Mabble engineering/reports/50_remediation_to_100.md` R-P0.05). Application-layer SoD (e.g., separate engineer pushes production schema changes vs application code) is informal at current company scale.	`db/schema/cortex/` role grants; Compliance Office attestation

---

IAM - Identity & Access Management (13 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
IAM-01.1	Is multi-factor authentication (MFA) required for all administrative access?	Yes	WebAuthn (passkey) is the preferred factor; TOTP is the fallback. SMS is supported but not encouraged for admin accounts. Helix uses Authenticator Method References (AMR) tagging on every session.	`internal/service/auth/sso/session.go`; `internal/research/20_helix_inventory.md §RBAC + Identity`
IAM-02.1	Are user accounts uniquely identifiable?	Yes	Each principal has a stable UUID (QID); usernames are not reused.	`db/schema/cortex/02_users.sql`

IAM-03.1	Are administrative accounts separated from regular user accounts?	Yes	`helix_admin` PostgreSQL role is separate from the runtime `helix` role; admin-level capabilities require explicit session elevation.	`db/schema/cortex/`
IAM-04.1	Is shared / generic account use prohibited?	Yes	All access is per-principal. Service identities use distinct credentials managed via AWS Secrets Manager + External Secrets Operator.	`internal/service/auth/...`; `internal/research/20_helix_inventory.md`
IAM-05.1	Are password / credential policies enforced (length, complexity, rotation)?	Yes	Argon2id hashing; minimum length and complexity enforced at the API boundary; password rotation enforced for high-privilege accounts via the identity provider. WebAuthn (passwordless) preferred for new users.	`internal/service/auth/...` ; `internal/research/20_helix_inventory.md §Identity`
IAM-06.1	Is access reviewed periodically?	Partial	RBAC entitlements are reviewable from `user_effective_roles` view at any time. Quarterly access review cadence is a roadmap item.	`db/schema/cortex/...rbac...`; Compliance Office attestation
IAM-07.1	Is privileged access logged and reviewed?	Yes	All capability-token issuance + use is audit-logged with the scope, principal, resource, and purpose-of-use (HIPAA §164.502(b)). Audit logs are immutable (RFC 6962 Merkle chain, R-P0.07).	`internal/service/audit/...`; `internal/service/capability/...`
IAM-08.1	Are tenants able to delegate access to their data without sharing credentials?	Yes	Customer admins manage their own users via SCIM/SAML/OIDC + the Helix console. Customer support access from Helix's side requires a separate scoped capability token.	`internal/service/auth/scim/...`

IAM-09.1	Are session timeouts enforced?	Yes	Sessions expire on a fixed window; idle inactivity triggers re-authentication. HTTP-only session cookies; no JWT in localStorage.	`internal/service/auth/sso/session.go`; `internal/research/20_helix_inventory.md`
IAM-10.1	Are user identity events logged and tamper-resistant?	Yes	Auth events (sign-in, sign-out, MFA challenge, password change) flow into the audit pipeline with Merkle anchoring.	`internal/service/audit/...`
IAM-11.1	Are federation protocols supported (SAML, OIDC, SCIM)?	Yes	SAML 2.0 (SP + IdP), OIDC, SCIM 2.0, WebAuthn, TOTP, Magic Link, Device Auth all supported.	`internal/research/20_helix_inventory.md §Identity`
IAM-12.1	Are role-based access control (RBAC) and least-privilege enforced?	Yes	Group RBAC + `user_effective_roles` view + capability token scopes; PostgreSQL RLS + FORCE RLS on every PII-bearing table. Per GDPR Art. 32(1)(b) - ongoing confidentiality.	`db/schema/cortex/` RLS policies; `internal/research/20_helix_inventory.md §RBAC`
IAM-13.1	Is there a documented process for handling identity-related security events (e.g., suspected account compromise)?	Yes	IR-003 (credential compromise) runbook at `mabble-runbooks/ir/ir-003-credential-compromise.md`.	`mabble-runbooks/ir/ir-003-credential-compromise.md`

IPY - Interoperability & Portability (5 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
IPY-01.1	Are standards-based formats (JSON, XML, etc.) supported for data import / export?	Yes	gRPC + JSON API for record CRUD; bulk export supports JSON line-delimited.	`api/proto/v1/record/record.proto`; `internal/api/v1/record_handler.go`
IPY-02.1	Are open APIs available for tenants to integrate with their existing systems?	Yes	gRPC + REST APIs covering vault, record, audit, DSAR, ROPA. Documentation lives at `docs-public/`.	`api/proto/v1/`; `docs-public/`

IPY-03.1	Is data portability supported (full export of customer data)?	Yes	DSAR fulfilment (R-P1.18) supports full subject-data export. Tenant-level full export via the bulk API is supported.	`internal/service/dsar/...`; `internal/api/v1/dsar_handler.go`
IPY-04.1	Are data and metadata returned to the tenant on termination?	Yes	Per BAA §11 - at termination Helix returns or destroys all PHI at the customer's option.	`docs/compliance/baa_template.md §11`
IPY-05.1	Are there documented schemas / data dictionaries for exported data?	Partial	Schema-level documentation exists in `api/proto/v1/`. A consolidated customer-facing data dictionary is on the roadmap.	`api/proto/v1/`

IVS - Infrastructure & Virtualization Security (13 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
IVS-01.1	Are network security controls (e.g., firewalls, IDS/IPS) in place?	Yes	AWS VPC + security groups + NACLs at the network layer; AWS WAF + CloudFront on the customer-facing console. Falco for runtime EBPF detection on production nodes is on the post-launch roadmap; today informal coverage.	Terraform configs in repo; `internal/critics/30_cso_review.md`
IVS-02.1	Is traffic between tenant environments isolated?	Yes	Logical tenant isolation enforced at the application layer (capability tokens scoped per-tenant) and at the database layer (PostgreSQL RLS + FORCE RLS on every PII-bearing table).	`db/schema/cortex/` RLS policies

IVS-03.1	Are intrusion detection systems deployed?	Partial	AWS GuardDuty enabled. Application-layer anomaly detection (e.g., honeytoken access alerting) per IR-001. Network-tier IDS (Suricata/Zeek) is not deployed.	`mabble-runbooks/ir/ir-001-data-breach.md`
IVS-04.1	Is host-based intrusion detection deployed?	Partial	Falco runtime detection is on the roadmap. Today AWS GuardDuty + immutable container runtime is the primary host layer.	Compliance Office attestation
IVS-05.1	Are vulnerability scans performed regularly?	Partial	Container image vulnerability scanning runs on every CI build (Trivy or equivalent). Network-layer external vulnerability scanning is on the post-launch roadmap.	`.github/workflows/`; `internal/compliance/README.md §5`
IVS-06.1	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`
IVS-07.1	Are virtual environments segmented based on data classification?	Yes	All customer PHI is in dedicated PHI-tier RDS + S3 buckets. Non-PHI operational telemetry is in separate buckets.	Terraform configs in repo
IVS-08.1	Are management interfaces (e.g., AWS console) protected by MFA?	Yes	AWS root account has hardware MFA; all IAM principals require MFA for console + API operations affecting production.	Mabble engineering attestation
IVS-09.1	Are network changes managed under the change-control process?	Yes	All network configuration is Terraform-managed; changes flow through PR review.	Terraform configs in repo

IVS-10.1	Are wireless networks protected by enterprise authentication?	Not Applicable	Helix is a remote-first company; no corporate-managed wireless. Engineers use their own networks; production access requires VPN + MFA + SSH bastion.	Mabble engineering attestation
IVS-11.1	Are time-synchronisation services (NTP) used across infrastructure?	Yes	AWS NTP service used cluster-wide. Audit-log timestamps rely on monotonic + wall-clock per the audit service implementation.	`internal/service/audit/...`
IVS-12.1	Are clocks accurate to within an acceptable tolerance?	Yes	Via AWS NTP; drift monitored.	AWS NTP attestation
IVS-13.1	Are infrastructure components hardened to industry benchmarks (CIS, etc.)?	Partial	Container base images use Distroless or minimal Alpine; AWS RDS is parameterised per Helix tuning guide (`Mabble engineering/reports/50_remediation_to_100.md` R-P0). CIS Benchmark formal audit is on the roadmap.	`Mabble engineering/reports/50_remediation_to_100.md`

MOS - Mobile Security (20 questions)

Helix does not currently offer a mobile application. The customer-facing console is a responsive web app accessed via mobile browsers. Mobile security controls relating to a Helix-published mobile binary are therefore **Not Applicable**.

When a Helix mobile app ships in the future, this section will be populated.

Control ID	Question	Yes/No	Notes	Evidence pointer
MOS-01.1	Is there a documented anti-malware policy for mobile devices?	Not Applicable	No Helix-published mobile app. Engineer endpoint policy lives under HRS-06.	n/a
MOS-02.1	Is application code signing required for mobile apps?	Not Applicable	No Helix-published mobile app.	n/a

MOS-03.1	Are approved mobile applications maintained on an inventory?	Not Applicable	No Helix-published mobile app.	n/a
MOS-04.1	Are mobile devices controlled via Mobile Device Management (MDM)?	Not Applicable - for customers	Customer access is via mobile browser; Helix has no control over the customer's mobile device. For Helix engineer endpoints, see HRS-06.	n/a
MOS-05.1	Are mobile device passwords enforced?	Not Applicable	No Helix-published mobile app.	n/a
MOS-06.1	Are remote-wipe capabilities supported on mobile devices accessing customer data?	Not Applicable	No Helix-published mobile app. Session revocation propagates within <=5 seconds on any device (CAEP propagation).	`internal/service/auth/sso/session.go`
MOS-07.1	Are mobile devices encrypted at rest?	Not Applicable	No Helix-published mobile app.	n/a
MOS-08.1	Are mobile device jailbreak / root detection mechanisms in place?	Not Applicable	No Helix-published mobile app.	n/a
MOS-09.1	Are mobile network connections protected (e.g., enterprise VPN)?	Not Applicable	No Helix-published mobile app.	n/a
MOS-10.1	Are mobile OS versions maintained at supported levels?	Not Applicable	No Helix-published mobile app.	n/a
MOS-11.1	Is mobile application security testing performed?	Not Applicable	No Helix-published mobile app.	n/a
MOS-12.1	Are mobile app data stores encrypted?	Not Applicable	No Helix-published mobile app.	n/a
MOS-13.1	Are mobile app crash-reporting tools scrubbed of PII?	Not Applicable	No Helix-published mobile app.	n/a
MOS-14.1	Are mobile apps subject to the same SDLC as other application code?	Not Applicable	No Helix-published mobile app.	n/a
MOS-15.1	Are mobile-only authentication flows MFA-protected?	Not Applicable	No Helix-published mobile app. WebAuthn passkeys are supported on mobile browsers.	`internal/service/auth/webauthn/...`

MOS-16.1	Are mobile push notifications scrubbed of PII before transit?	Not Applicable	No Helix-published mobile app or notification service.	n/a
MOS-17.1	Are mobile session timeouts enforced?	Not Applicable	No Helix-published mobile app. Web-session timeouts apply universally.	`internal/service/auth/sso/session.go`
MOS-18.1	Is biometric authentication supported on mobile?	Not Applicable - for native app	WebAuthn on a mobile browser supports the device's biometric (Touch ID / Face ID / Android biometric).	`internal/service/auth/webauthn/...`
MOS-19.1	Is data sharing between mobile apps and other apps on the device prevented?	Not Applicable	No Helix-published mobile app.	n/a
MOS-20.1	Are mobile app updates digitally signed?	Not Applicable	No Helix-published mobile app.	n/a

---

SEF - Security Incident Management, E-Discovery & Cloud Forensics (5 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
SEF-01.1	Is a security incident response policy documented?	Yes	IR runbooks at `mabble-runbooks/ir/` cover breach, credential compromise, insider threat. Public-disclosable runbook at `internal/compliance/breach_notification_runbook.md`.	`mabble-runbooks/ir/`
SEF-02.1	Are incident response procedures tested?	Partial	Sub-component tests (e.g., session revocation drill) are exercised informally. A full tabletop exercise has not yet been logged in 2026.	Compliance Office attestation
SEF-03.1	Are incidents documented and lessons-learned reviewed?	Yes	Post-incident review checklist in each IR runbook. Mabble engineering decisions log captures lessons learned.	`mabble-runbooks/ir/ir-001-data-breach.md §7`; `internal/decisions/`

SEF-04.1	Are e-discovery / legal hold capabilities supported?	Partial	Audit logs are retained 7 years (S3 Object Lock COMPLIANCE mode). Customer-initiated legal hold via API is on the roadmap.	`internal/research/20_helix_inventory.md §Audit`
SEF-05.1	Are breach notification commitments documented?	Yes	BAA §4 commits Helix to <=30 calendar days of discovery (shorter than HIPAA's 60-day default). GDPR Art. 33 (<=72 hours to supervisory authority) and Art. 34 (without undue delay to data subjects) commitments are in the customer-facing notification runbook.	`docs/compliance/baa_template.md §4`; `internal/compliance/breach_notification_runbook.md`

STA - Supply Chain Management, Transparency, and Accountability (9 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer
STA-01.1	Are sub-processors disclosed publicly?	Yes	Canonical list at `docs/compliance/sub_processors.md`. Phase 4 vendor monitoring (R-P4.1) provides snapshot + diff-alert per tenant.	`docs/compliance/sub_processors.md`; `db/schema/cortex/13c_vendor_snapshots.sql`
STA-02.1	Are sub-processors required to meet equivalent security controls?	Yes	Per BAA §5; sub-processors must sign written agreements imposing substantially the same obligations. Per GDPR Art. 28(4).	`docs/compliance/baa_template.md §5`
STA-03.1	Are sub-processor changes notified in advance?	Yes	>=30 days written notice before adding or replacing a sub-processor that processes PHI. Customer objection period 14 days; unresolved objections allow termination without penalty.	`docs/compliance/sub_processors.md §4`; `docs/compliance/baa_template.md §5.3`

STA-04.1	Is a software bill of materials (SBOM) produced for all releases?	Partial	CI generates SBOM for container images. Customer-facing SBOM publication is on the roadmap.	`.github/workflows/`; Compliance Office attestation
STA-05.1	Are open-source dependencies tracked and reviewed for vulnerabilities?	Yes	Dependabot + Trivy + Go module integrity checks.	`.github/workflows/`
STA-06.1	Are supply chain risks assessed for each new sub-processor?	Yes	Per `docs/compliance/sub_processors.md §3`, sub-processors must meet BAA + DPA + SOC 2 (or equivalent) + breach reporting + audit-right criteria.	`docs/compliance/sub_processors.md §3`
STA-07.1	Are software releases digitally signed?	Yes	Container images cosigned (Sigstore Cosign). Audit-log anchoring is Ed25519-signed and externally verified via Sigstore Rekor (D-005).	`internal/decisions/` D-005; `.github/workflows/`
STA-08.1	Are third-party code reviews performed (security assessments on critical components)?	Partial	Internal review by the Mabble engineering + critic skills before each release. External code review is not yet engaged.	`internal/critics/`
STA-09.1	Are right-to-audit clauses present in sub-processor contracts?	Yes	Per `docs/compliance/sub_processors.md §3` row 5: sub-processors must allow audit of relevant controls on reasonable notice (max 1x per year).	`docs/compliance/sub_processors.md §3`

TVM - Threat & Vulnerability Management (3 questions)

Control ID	Question	Yes/No	Notes	Evidence pointer

TVM-01.1	Are systems regularly scanned for vulnerabilities?	Partial	Container image scanning (Trivy) on every CI build. Application-tier static analysis (`go vet`, `gosec`) on every build. Network-tier external scanning is on the roadmap.	`.github/workflows/`
TVM-02.1	Are security patches applied within a defined SLA?	Yes	Critical vulnerabilities patched within 7 days; high within 30 days; medium within 90 days; low at the next planned release. Per GDPR Art. 32(1)(d).	Compliance Office attestation
TVM-03.1	Is there a vulnerability disclosure program (VDP) and / or bug bounty?	No	Draft VDP exists; not yet live. Planned for the 6-month launch window. Email today: sales@mabble.ai.	`internal/compliance/README.md §5`

Summary statistics

Domain	Total	Yes	Partial	No	Not Applicable	Manual Attestation
AAC	4	1	0	2	1	0
AIS	6	4	1	0	0	1
BCR	11	5	4	0	0	2
CCC	5	3	2	0	0	0
DSI	7	5	2	0	0	0
DCS	9	8	0	0	1	0
EKM	4	4	0	0	0	0
GRM	11	2	6	1	0	2
HRS	11	5	3	0	0	3
IAM	13	12	1	0	0	0
IPY	5	4	1	0	0	0
IVS	13	7	5	1	1	0 (Mabble engineering attest on 2)
MOS	20	0	0	0	20	0
SEF	5	3	2	0	0	0
STA	9	7	2	0	0	0
TVM	3	1	1	1	0	0

Total	**136**	**71**	**30**	**5**	**23**	**8**

(MOS bulk-marked Not Applicable; mobile-app-specific controls. Manual attestation count = Compliance Office + HR / Mabble engineering attestations required before submission.)

Change log

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