FIMIL, INC.

CAIQ v4 v4.0

Cloud Security Alliance Consensus Assessments Initiative Questionnaire — 261 questions across 17 security domains aligned with the Cloud Controls Matrix.

March 20, 2026

Security Questionnaire Response

trust.fimil.dev

security@fimil.dev

Response Summary

Answer	Count	Percentage
Yes	171	65.5%
Partial	53	20.3%
No	12	4.6%
N/A	25	9.6%
Total	261	100%

A&A — Audit & Assurance

2/8 controls satisfied

ID	Question	Answer	Explanation
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	YES	ISMS Policy (FIMIL-ISMS-001) and the compliance documentation suite establish audit and assurance policies. Statement of Applicability (FIMIL-SOA-001) tracks control implementation status, and the Compliance Register monitors regulatory compliance.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies. Policies are version-controlled in Git for auditability.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	NO	No independent external security audit, penetration test, or third-party assurance assessment has been conducted. This is the single remaining FAIL in the ISO 27001 assessment (A.5.35).
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	NO	No independent audits have been performed yet. A formal Risk Assessment (FIMIL-RISK-001) exists and would inform audit planning, but no external audit engagement has occurred.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements?	PARTIAL	Compliance Register (FIMIL-CLR-001) tracks GDPR, CCPA/CPRA, and other regulatory requirements. Internal compliance verification is conducted, but no independent external compliance verification has been performed.
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, and remediation?	PARTIAL	Risk Assessment (FIMIL-RISK-001) provides a risk framework with a 5x5 likelihood-impact matrix. Statement of Applicability tracks control gaps. CSA STAR Level 1 self-assessment completed. Continuous monitoring plan (FIMIL-CONMON-001) provides ongoing assurance. However, no formal audit management process with external audit scheduling and tracking is in place.
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	PARTIAL	Risk Assessment documents 15 identified risks with treatment plans and timelines (Q2-Q4 2026). The COMPLIANCE.md Top 10 Gaps list prioritizes remediation. However, these are internal findings, not from independent audits.
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	PARTIAL	Statement of Applicability and Compliance Register track implementation and remediation status. Currently sole founder serves as both assessor and stakeholder, limiting independent oversight.

AIS — Application & Interface Security

11/11 controls satisfied

ID	Question	Answer	Explanation
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	YES	Change Management & Secure Development Lifecycle Policy (FIMIL-CHG-001) documents SDLC security integration. OWASP-aware implementation includes CSRF protection, input validation, parameterized queries, rate limiting, and secret redaction.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Secure Development Lifecycle Policy. Policies are version-controlled in Git.
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	YES	Application security baselines are enforced via CI pipeline (linting, testing, type checking, SAST), pre-commit hooks, container scanning with Trivy, SPDX SBOMs, Cosign container signing, and GitHub Actions build provenance attestation. OWASP-aligned requirements cover CSRF, SQL injection, XSS, input validation, and authentication. Documented in the Change Management Policy.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives and security requirements?	YES	API metrics (response time percentiles, error rates) collected via Redis-backed middleware. Health monitoring tracks scanner success/failure rates, Celery queue depths, database latency, and Redis hit rates. Security metrics include brute force attempts, credential stuffing detection rates, and alert counts.
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation?	YES	Change Management & Secure Development Lifecycle Policy (FIMIL-CHG-001) documents the full SDLC with change classification, CI pipeline gates, container scanning, Helm atomic deployments with rollback, and feature flag staged rollout.
AIS-05.1	Does the testing strategy outline criteria to accept new systems, upgrades, and versions?	YES	CI pipeline enforces acceptance criteria: linting, unit tests, type checking, build verification, and Trivy container scanning that blocks deployment on critical vulnerabilities. Frontend coverage thresholds enforced at 80%.
AIS-05.2	Is testing automated when applicable and possible?	YES	Automated testing is extensive: backend pytest suite, frontend Vitest with MSW mocks, pre-commit hooks, CI pipeline on every push/PR, Trivy image scanning in deployment pipeline, and security-specific tests in api/tests/security/.
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code securely?	YES	Helm atomic deployments with automatic rollback on failure. Container images signed with Cosign (keyless via Sigstore) with SPDX SBOMs and GitHub Actions build provenance attestation. Sealed secrets for credential management. Branch protection enforces GPG-signed commits. Manual workflow_dispatch provides human gate for deployment. Database migrations run as separate job before Helm upgrade.
AIS-06.2	Is the deployment and integration of application code automated where possible?	YES	GitHub Actions CI/CD pipeline automates build, test, container scanning, and deployment. Helm manages Kubernetes deployments. Feature flags enable staged rollout with rollout percentages.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	YES	Trivy scanning in CI/CD blocks critical vulnerabilities from deployment. The platform itself orchestrates 12 security scanners for vulnerability detection. Risk Assessment documents treatment plans for identified vulnerabilities with timelines.
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	YES	Trivy blocks critical container vulnerabilities automatically. Semgrep provides autofix suggestions. Dependabot is configured across all repositories for automated dependency updates. Container images include SPDX SBOMs and are signed with Cosign via Sigstore for supply chain integrity. DAST is not yet implemented but is not required for a "yes" on automated remediation where possible.

BCR — Business Continuity Management & Operational Resilience

16/18 controls satisfied

ID	Question	Answer	Explanation
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	YES	Business Continuity Plan (FIMIL-BCP-001) documents RTO of 4 hours and RPO of 24 hours, six disaster scenarios with recovery procedures, and maintenance mode middleware for planned disruptions.
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Business Continuity Plan. Policies are version-controlled in Git.
BCR-02.1	Are criteria for developing business continuity strategies established based on business disruption and risk impacts?	YES	Risk Assessment (FIMIL-RISK-001) identifies business disruption risks including platform unavailability, vendor dependency, and DDoS using a 5x5 likelihood-impact matrix. BCP strategies are aligned to these risk assessments.
BCR-03.1	Are strategies developed to reduce impact of, withstand, and recover from business disruptions?	YES	BCP documents six disaster scenarios with specific recovery procedures. Technical resilience includes HPA autoscaling, circuit breakers, retry logic, Pod Disruption Budgets, rolling updates, and Helm atomic deployments with automatic rollback.
BCR-04.1	Are operational resilience strategies incorporated to establish, document, approve, communicate a business continuity plan?	YES	Business Continuity Plan (FIMIL-BCP-001) is formally documented and approved by CEO & CISO. It incorporates resilience strategies including maintenance mode, graceful degradation, and automated rollback.
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity plans?	YES	Comprehensive operational documentation exists: backup/restore procedures, monitoring guide, upgrade guide, security hardening guide, and incident response runbook. All stored in docs/operations/ and version-controlled.
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	YES	All documentation is stored in version-controlled repositories accessible to authorized personnel. Operational procedures are documented in docs/operations/ and CLAUDE.md.
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	YES	ISMS Policy defines an annual review cadence. Documentation is version-controlled in Git with change history. Risk Assessment is scheduled for annual review.
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually?	YES	DR test successfully conducted in March 2026 with verified backup restore. Helm atomic deployments with automatic rollback are tested operationally during every deployment. Semi-annual DR testing cadence established.
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	YES	Incident Response Plan defines communication procedures during disruptions. Maintenance mode middleware returns 503 with Retry-After header. Announcement system enables system-wide communications. Email and Slack notifications alert stakeholders.
BCR-08.1	Is cloud data periodically backed up?	YES	Nightly PostgreSQL and Redis backups to S3 via comprehensive backup scripts supporting both Docker Compose and Kubernetes deployments. Metadata tracking includes timestamp, deployment type, and version.
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	YES	Backups are compressed with gzip, uploaded to S3 for offsite storage, and include metadata tracking. Restore scripts include verification steps. Access to backup storage is restricted.
BCR-08.3	Can backups be restored appropriately for resiliency?	YES	Restore scripts exist with verification, service stop/restart, and migration execution. Documentation provided in docs/operations/backup-restore.md. DR test in March 2026 successfully validated backup restore procedures.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained?	YES	Business Continuity Plan (FIMIL-BCP-001) documents six disaster scenarios with specific recovery procedures, RTO of 4 hours, and RPO of 24 hours. Approved by CEO & CISO.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	YES	ISMS Policy defines an annual review cadence for all compliance documentation. BCP is version-controlled and updated as infrastructure changes occur.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	YES	DR test successfully conducted in March 2026 with verified backup restore and recovery procedures. Helm rollback capabilities are tested operationally during every deployment. Semi-annual DR testing cadence established.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	NA	Cloud-hosted on DigitalOcean. No physical facilities requiring coordination with local emergency authorities.
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located?	PARTIAL	Multiple replicas via HPA with Pod Disruption Budgets and anti-affinity for zone spreading. However, deployment is single-region only with no multi-region failover, no Redis HA, and single primary PostgreSQL relying on DigitalOcean managed database failover.

CCC — Change Control & Configuration Management

11/11 controls satisfied

ID	Question	Answer	Explanation
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets established, documented, approved, communicated, applied, evaluated and maintained?	YES	Change Management Policy (FIMIL-CHG-001) documents change classification (Standard, Normal, Emergency), approval workflows, and risk assessment criteria. Risk Assessment (FIMIL-RISK-001) provides the risk framework.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Change Management Policy. Policies are version-controlled in Git.
CCC-02.1	Is a defined quality change control, approval and testing process followed?	YES	CI pipeline gates on linting, tests, type checking, and container scanning. Branch protection enforces GPG-signed commits, CI checks required, and enforce admins. Manual workflow_dispatch provides human gate for deployment. Helm atomic deployments with automatic rollback. CODEOWNERS file governs code change approval.
CCC-03.1	Are risks associated with changing organizational assets managed?	YES	Change Management Policy defines risk assessment criteria by change type. Helm atomic deployments auto-rollback failed changes. Feature flags enable staged rollout to limit blast radius. Database migrations run as a separate job before Helm upgrade.
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	YES	Branch protection enforces GPG-signed commits, required CI checks, and enforce admins. Sealed secrets encrypt production credentials. Deployment only via Helm with version-tagged, Cosign-signed images. CODEOWNERS restricts code changes. Falco runtime monitoring detects unexpected binary execution, filesystem writes, and container image drift.
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments included within service level agreements?	YES	SLA published at /legal/sla. Maintenance windows communicated via the announcement system. Maintenance mode middleware blocks non-admin traffic with Retry-After header during planned changes.
CCC-06.1	Are change management baselines established for all relevant authorized changes?	YES	Helm values files provide declarative configuration baselines. Pod annotations with config/secret checksums detect configuration drift. Falco image drift detection CronJob compares running images against expected tags every 30 minutes.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	YES	Falco runtime monitoring detects unauthorized changes: unexpected processes, filesystem writes, network violations, privilege escalation, config file modifications (FIM), and image drift. Alerts surface to admin dashboard.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	YES	Change Management Policy defines Emergency change type with expedited approval and post-implementation review. Helm rollback provides rapid reversion. Maintenance mode enables emergency operational changes.
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04 policy exception process?	YES	ISMS Policy establishes a formal policy exception process. Emergency changes in the Change Management Policy follow the same documented exception and approval framework.
CCC-09.1	Is a process to proactively roll back changes to a previously known good state defined and implemented?	YES	Helm atomic deployments (--atomic --wait) automatically roll back on failure. Manual rollback via helm rollback command. Database migration rollback scripts available. Version-tagged container images allow pinning to known-good versions.

CEK — Cryptography, Encryption & Key Management

11/23 controls satisfied

ID	Question	Answer	Explanation
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	YES	ISMS Policy and Access Control Policy (FIMIL-ACP-001) document cryptographic requirements. MultiFernet (AES-128-CBC + HMAC-SHA256) with versioned key rotation for encryption at rest, Argon2id (memory-hard) for password hashing, SHA256 for token hashing, HMAC-SHA256 for webhook verification, and HS256 for JWT signing.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies. Cryptographic controls are documented in the compliance policy suite and version-controlled.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	PARTIAL	ISMS Policy designates CEO & CISO with security responsibilities including key management. However, sole founder currently holds all key management authority with no separation of duties for cryptographic operations.
CEK-03.1	Are data at-rest and in-transit cryptographically protected using certified cryptographic libraries?	YES	Data at rest: MultiFernet encryption (AES-128-CBC + HMAC-SHA256) with versioned key rotation for OAuth tokens, Argon2id (memory-hard) for passwords, SHA256 for API tokens. Data in transit: TLS enforced in production, SMTP supports STARTTLS/SSL, session cookies use Secure flag. All use standard certified Python cryptographic libraries (cryptography, pwdlib).
CEK-04.1	Are appropriate data protection encryption algorithms used?	YES	Industry-standard algorithms: AES-128-CBC + HMAC-SHA256 (MultiFernet) for symmetric encryption with versioned key rotation, Argon2id (memory-hard, OWASP-recommended) for password hashing, SHA256 for token hashing, HMAC-SHA256 for webhook verification, HS256 for JWT signing, secrets.token_urlsafe for random token generation.
CEK-05.1	Are standard change management procedures established to review, approve, implement cryptography changes?	YES	Change Management Policy governs all infrastructure and software changes, including cryptographic configurations. Production enforcement requires non-default SECRET_KEY. CI pipeline gates prevent unauthorized changes.
CEK-06.1	Are changes to cryptography systems managed accounting for downstream effects?	YES	MultiFernet versioned encryption keys enable seamless key rotation without data loss. Re-encryption tooling migrates all encrypted data from old keys to the current key. Downstream effects are fully managed — new data uses the latest key while old data remains decryptable via the key chain.
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained?	YES	Risk Assessment identifies cryptographic risks with treatment plans. MultiFernet versioned key rotation with re-encryption tooling addresses the previously identified key rotation gap. STRIDE threat model covers cryptographic threats. Continuous monitoring plan (FIMIL-CONMON-001) includes cryptographic controls. HSM/KMS integration remains a future enhancement for FIPS 140-2 compliance.
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	NO	Fimil does not currently offer customer-managed encryption keys (CMEK/BYOK). Encryption keys are managed by the platform using MultiFernet with server-side versioned keys.
CEK-09.1	Are encryption and key management systems audited with frequency proportional to risk exposure?	PARTIAL	Internal compliance assessment reviewed cryptographic controls. No independent external audit of encryption and key management systems has been conducted.
CEK-09.2	Are encryption and key management systems audited preferably continuously but at least annually?	PARTIAL	Internal review has been conducted. CI pipeline validates cryptographic configurations in production (non-default SECRET_KEY required). However, no recurring formal audit schedule is in place.
CEK-10.1	Are cryptographic keys generated using approved cryptographic libraries?	YES	Keys and tokens are generated using Python's secrets module (secrets.token_urlsafe) and the cryptography library (Fernet). These are industry-standard, certified cryptographic libraries.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	YES	MultiFernet versioned encryption keys managed for data encryption. Separate JWT signing key. API tokens use separate SHA256 hashing. Session IDs use independent secrets.token_urlsafe generation. Sealed secrets encrypt credentials in Kubernetes. Container images signed with Cosign via Sigstore.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated?	PARTIAL	MultiFernet versioned encryption keys support key rotation with re-encryption tooling. Keys can be rotated without data loss. However, no formal cryptoperiod is defined and rotation is performed manually rather than on an automated schedule tied to a calculated cryptoperiod.
CEK-13.1	Are cryptographic keys revoked and removed before the end of cryptoperiod?	PARTIAL	MultiFernet key rotation allows old keys to be superseded by new keys, and re-encryption tooling can migrate all data to the current key, after which old keys can be removed. However, no formal cryptoperiods are defined and no automated key revocation schedule is implemented.
CEK-14.	Are processes, procedures and technical	NO	No formal key destruction process is defined. Key management lifecycle

ID	Question	Answer	Explanation
1	measures to destroy unneeded keys defined?		tooling is an identified gap targeted for remediation with KMS integration.
CEK-15.1	Are processes, procedures, and technical measures to create keys in pre-activated state defined?	NO	No key pre-activation state management exists. Key lifecycle management is an identified gap targeted for remediation with KMS integration.
CEK-16.1	Are processes, procedures, and technical measures to monitor key transitions defined?	NO	No key transition monitoring exists. Key lifecycle management is an identified gap targeted for remediation with KMS integration.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys defined?	NO	No key deactivation process is defined. Key lifecycle management is an identified gap targeted for remediation with KMS integration.
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys defined?	NO	No key archival process is defined. Key lifecycle management is an identified gap targeted for remediation with KMS integration.
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios defined?	YES	Data Governance Policy classifies data into four levels with encryption requirements per level. Restricted data (OAuth tokens, API credentials) uses MultiFernet encryption with versioned key rotation. TLS enforced for all data in transit. Session cookies use Secure flag.
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks defined?	YES	MultiFernet versioned key rotation with re-encryption tooling eliminates the previously identified operational continuity risk of key changes breaking encrypted data. Risk Assessment documents cryptographic risks with treatment plans. Business Continuity Plan addresses recovery scenarios including data recovery. DR test in March 2026 validated recovery procedures.
CEK-21.1	Are key management system processes to track and report all cryptographic materials defined?	NO	No centralized key management system or cryptographic material inventory exists. Cryptographic materials are managed at the application level without formal tracking or reporting.

DCS — Datacenter Security

0/23 controls satisfied

ID	Question	Answer	Explanation
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside premises established?	NA	Cloud-hosted on DigitalOcean. Physical equipment disposal is the cloud provider's responsibility under the shared responsibility model.
DCS-01.2	Is a data destruction procedure applied that renders information recovery impossible?	NA	Cloud-hosted on DigitalOcean. Physical data destruction for hardware is the cloud provider's responsibility. Logical data disposal is handled at the application level.
DCS-01.3	Are policies and procedures for secure equipment disposal reviewed and updated at least annually?	NA	Cloud-hosted on DigitalOcean. Physical equipment disposal policies are the cloud provider's responsibility.
DCS-02.1	Are policies and procedures for relocation or transfer of hardware, software, or data established?	NA	Cloud-hosted on DigitalOcean. Physical hardware relocation is the cloud provider's responsibility.
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	Cloud-hosted on DigitalOcean. Physical hardware transfer authorization is the cloud provider's responsibility.
DCS-02.3	Are policies and procedures reviewed and updated at least annually?	NA	Cloud-hosted on DigitalOcean. Physical transfer policies are the cloud provider's responsibility.
DCS-03.1	Are policies and procedures for maintaining safe and secure working environments established?	NA	Cloud-hosted on DigitalOcean. Physical datacenter working environment safety is the cloud provider's responsibility.
DCS-03.2	Are policies and procedures reviewed and updated at least annually?	NA	Cloud-hosted on DigitalOcean. Physical working environment policies are the cloud provider's responsibility.
DCS-04.1	Are policies and procedures for secure transportation of physical media established?	NA	Cloud-hosted on DigitalOcean. Physical media transportation is the cloud provider's responsibility.
DCS-04.2	Are policies and procedures reviewed and updated at least annually?	NA	Cloud-hosted on DigitalOcean. Physical media transportation policies are the cloud provider's responsibility.
DCS-05.1	Is the classification and documentation of physical and logical assets based on business risk?	NA	Cloud-hosted on DigitalOcean. Physical asset classification in datacenters is the cloud provider's responsibility.
DCS-06.1	Are all relevant physical and logical assets cataloged and tracked?	NA	Cloud-hosted on DigitalOcean. Physical datacenter asset tracking is the cloud provider's responsibility.
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data?	NA	Cloud-hosted on DigitalOcean. Physical security perimeters are the cloud provider's responsibility.
DCS-07.2	Are physical security perimeters established between administrative areas and data storage?	NA	Cloud-hosted on DigitalOcean. Physical security perimeter segregation is the cloud provider's responsibility.
DCS-08.1	Is equipment identification used as a method for connection authentication?	NA	Cloud-hosted on DigitalOcean. Physical equipment identification for datacenter connections is the cloud provider's responsibility.
DCS-09.1	Are solely authorized personnel able to access secure areas?	NA	Cloud-hosted on DigitalOcean. Physical access control to secure datacenter areas is the cloud provider's responsibility.
DCS-09.2	Are access control records retained periodically?	NA	Cloud-hosted on DigitalOcean. Physical access control record retention is the cloud provider's responsibility.
DCS-10.1	Are datacenter surveillance systems implemented at ingress and egress points?	NA	Cloud-hosted on DigitalOcean. Datacenter surveillance is the cloud provider's responsibility.
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access?	NA	Cloud-hosted on DigitalOcean. Datacenter personnel training is the cloud provider's responsibility.
DCS-12.1	Are processes defined to ensure risk-based protection of power and telecommunication cables?	NA	Cloud-hosted on DigitalOcean. Physical cable protection is the cloud provider's responsibility.
DCS-13.1	Are data center environmental control systems designed to monitor temperature and humidity?	NA	Cloud-hosted on DigitalOcean. Environmental monitoring in the datacenter is the cloud provider's responsibility.
DCS-14.	Are utility services secured, monitored,	NA	Cloud-hosted on DigitalOcean. Datacenter utility services are the cloud

ID	Question	Answer	Explanation
1	maintained, and tested?		provider's responsibility.
DCS-15.1	Is business-critical equipment segregated from high-probability environmental risk locations?	NA	Cloud-hosted on DigitalOcean. Physical equipment siting and environmental risk segregation are the cloud provider's responsibility.

DSP — Data Security & Privacy Lifecycle Management

20/24 controls satisfied

ID	Question	Answer	Explanation
DSP-01.1	Are policies and procedures established for classification, protection, and handling of data throughout lifecycle?	YES	Data Governance Policy (FIMIL-DGP-001) establishes a four-level classification scheme (Public, Internal, Confidential, Restricted) with handling requirements for storage, transmission, access, and disposal at each level.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Data Governance Policy. Policies are version-controlled in Git.
DSP-02.1	Are industry-accepted methods applied for secure data disposal?	YES	Data Governance Policy documents retention schedules and disposal procedures by classification level. Source code is ephemeral (clone-scan-delete). Sessions expire after 24 hours. OAuth state tokens have 10-minute TTL. API tokens stored as irreversible SHA256 hashes.
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information?	YES	Formal asset register (FIMIL-AM-001) with 26-row inventory cataloging all information assets including sensitive and personal data. Data Governance Policy classifies data types with four-level classification scheme. Privacy Policy documents collected personal information categories.
DSP-04.1	Is data classified according to type and sensitivity levels?	YES	Four-level classification: Public (marketing content), Internal (operational data), Confidential (user PII, scan results), Restricted (encryption keys, OAuth tokens, API credentials). Technical controls enforce classification at each level.
DSP-05.1	Is data flow documentation created to identify what data is processed and where?	PARTIAL	Data Governance Policy documents data categories and handling. Architecture documentation describes data flows between components. However, no formal data flow diagram mapping all personal data processing activities exists.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually?	PARTIAL	ISMS Policy defines annual review cadence for all documentation. Data Governance Policy is version-controlled. However, formal data flow documentation is not yet comprehensive enough for a meaningful annual review.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	PARTIAL	Data Governance Policy defines data categories with handling requirements. ISMS Policy designates CEO & CISO with data governance responsibilities. However, no individual data asset ownership register exists.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	PARTIAL	ISMS Policy defines annual review cadence. Data Governance Policy is reviewed as part of the policy suite. However, formal data ownership documentation is not yet comprehensive.
DSP-07.1	Are systems, products, and business practices based on security principles by design?	YES	Defense-in-depth architecture with security at every layer: network isolation, container hardening (non-root, read-only, cap_drop ALL), RBAC, tenant isolation, CSRF protection, rate limiting, input validation, encrypted fields, and ephemeral source code processing.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design?	YES	Source code is ephemeral (clone-scan-delete, never persisted). Data minimization in user model. Cookie consent with accept/reject/customize options. Do Not Track signal respected. PostHog analytics blocked until consent granted.
DSP-08.2	Are systems' privacy settings configured by default?	YES	Privacy-protective defaults: analytics blocked until explicit consent, Do Not Track respected as automatic opt-out, minimal data collection, and ephemeral source code processing by default.
DSP-09.1	Is a data protection impact assessment conducted when processing personal data?	YES	Formal DPIA process established with standardized template and DPIA register. Data Governance Policy documents GDPR obligations including DPIA requirements. Risk Assessment evaluates data protection risks. DPIAs are conducted for personal data processing activities as required by GDPR Article 35.
DSP-10.1	Are processes defined to ensure any transfer of personal or sensitive data is protected?	YES	TLS enforced in production. Webhook signatures verified with HMAC-SHA256. SMTP supports STARTTLS/SSL. Session cookies use Secure, HttpOnly, SameSite flags. Data Processing Agreement published at /legal/dpa. Vendor DPAs executed with all providers.
DSP-11.1	Are processes defined to enable data subjects to request access, modify, or delete personal data?	YES	Admin API implements DSAR automation: data export endpoint for Article 15 (right of access) and data erasure endpoint for Article 17 (right to erasure). Privacy Policy and Data Governance Policy document GDPR/CCPA data subject rights. Compliance Register tracks DSAR obligations.
DSP-12.1	Are processes defined to ensure personal data is processed for declared purposes?	YES	Privacy Policy declares data processing purposes. Cookie consent mechanism restricts analytics until consent. Data Governance Policy defines purpose limitations for each data category. Data minimization principle applied.
DSP-13.	Are processes defined for transfer and	YES	Data Processing Agreement at /legal/dpa governs customer data

ID	Question	Answer	Explanation
1	sub-processing of personal data?		processing. Vendor Risk Management Policy tracks all sub-processors. DPAs executed with all critical and significant vendors (DigitalOcean, GitHub, Stripe, Cloudflare, Resend, PostHog).
DSP-14.1	Are processes defined to disclose details of personal data access by sub-processors?	YES	Vendor Risk Management Policy documents all sub-processors with tier classification. Privacy Policy discloses third-party data sharing. DPA provides transparency on sub-processor access to customer data.
DSP-15.1	Is authorization from data owners obtained before replicating production data?	YES	Tests use synthetic fixtures (in-memory SQLite, no production data). Source code is ephemeral and never replicated. Backups are stored in access-controlled S3 storage. No production data replication for non-production purposes.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements and regulations?	YES	Data Governance Policy documents retention schedules for all data categories. Report retention configurable at 30 days. Sessions expire after 24 hours. Source code is immediately deleted after scanning. Compliance Register tracks GDPR and CCPA retention obligations.
DSP-17.1	Are processes defined and implemented to protect sensitive data throughout lifecycle?	YES	Sensitive data protection at every stage: MultiFernet encryption with versioned key rotation for Restricted data at rest, Argon2id for password hashing, TLS for data in transit, RBAC and tenant isolation for access control, SHA256 hashing for tokens, secret redaction in scanner findings, and ephemeral source code processing.
DSP-18.1	Does the CSP have procedures to manage and respond to law enforcement data disclosure requests?	YES	Incident Response Plan includes regulatory notification procedures. Compliance Register tracks legal obligations. Privacy Policy addresses law enforcement requests. Data Governance Policy documents disclosure procedures.
DSP-18.2	Does the CSP give special attention to notification procedures to interested CSCs?	YES	Incident Response Plan defines customer notification procedures for data breaches with GDPR 72-hour and CCPA timelines. Announcement system enables system-wide customer notifications.
DSP-19.1	Are processes defined to specify and document physical data locations?	YES	Vendor Risk Management Policy documents DigitalOcean as the infrastructure provider. Data Processing Agreement specifies data processing locations. Infrastructure is deployed on DigitalOcean Kubernetes in documented regions.

GRC — Governance, Risk Management & Compliance

8/9 controls satisfied

ID	Question	Answer	Explanation
GRC-01.1	Are information governance program policies and procedures established, documented, approved?	YES	Comprehensive policy suite: ISMS Policy, Access Control Policy, Data Governance Policy, Incident Response Plan, Change Management Policy, People Security Policy, and Vendor Risk Management Policy. All formally approved by CEO & CISO.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies. Policies are version-controlled in Git with change history and formal approval records.
GRC-02.1	Is there an established formal, documented, leadership-sponsored enterprise risk management program?	YES	Risk Assessment (FIMIL-RISK-001) establishes a formal risk management program with a 5x5 likelihood-impact matrix, 15 identified risks, and treatment plans with timelines. Sponsored by CEO & CISO.
GRC-03.1	Are all relevant organizational policies reviewed at least annually or when substantial changes occur?	YES	ISMS Policy mandates annual review of all policies. Change Management Policy triggers review when significant changes occur. All policies are version-controlled for traceability.
GRC-04.1	Is an approved exception process established and followed whenever policy deviation occurs?	YES	ISMS Policy establishes a formal policy exception process. Change Management Policy defines Emergency change type with expedited approval and post-implementation review for exception handling.
GRC-05.1	Has an information security program been developed and implemented?	YES	ISMS Policy (FIMIL-ISMS-001) establishes the information security program. System Security Plan (FIMIL-SSP-001) maps to NIST 800-53 Low baseline. Continuous monitoring plan (FIMIL-CONMON-001) provides ongoing assurance. STRIDE threat model covers 3 areas with 16 identified threats. CSA STAR Level 1 self-assessment completed. Statement of Applicability maps all ISO 27001 controls.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing governance defined?	PARTIAL	ISMS Policy designates CEO & CISO roles. People Security Policy documents role-based security responsibilities. Application RBAC enforces authority levels. However, sole founder fills all roles; organizational governance structure to scale with team growth.
GRC-07.1	Are all relevant standards, regulations, legal/contractual requirements identified and documented?	YES	Compliance & Legal Requirements Register (FIMIL-CLR-001) tracks GDPR, CCPA/CPRA, Delaware corporate law, Nevada business licensing, CAN-SPAM, and DMCA with compliance status and planned actions.
GRC-08.1	Is contact established and maintained with cloud-related special interest groups?	YES	CSA STAR Level 1 self-assessment completed, establishing active engagement with the Cloud Security Alliance. Platform consumes EPSS data from FIRST.org. SECURITY.md provides external security reporting channel. Federal incident reporting includes CISA/CIRCIA contacts in the Incident Response Plan.

HRS — Human Resources

6/20 controls satisfied

ID	Question	Answer	Explanation
HRS-01.1	Are background verification policies and procedures of all new employees established?	PARTIAL	People Security Policy (FIMIL-PPL-001) documents pre-employment screening requirements including background verification, reference checks, and identity verification. Currently sole founder; framework ready for implementation when hiring begins.
HRS-01.2	Are background verification policies designed according to local laws and regulations?	PARTIAL	People Security Policy specifies that screening should be proportional to role sensitivity and compliant with applicable laws. Compliance Register tracks relevant regulations. However, policies not yet exercised in practice.
HRS-01.3	Are background verification policies reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the People Security Policy. Policies are version-controlled.
HRS-02.1	Are policies and procedures for acceptable use of organizationally-owned assets established?	YES	Acceptable Use Policy published at /legal/acceptable-use. People Security Policy documents acceptable use requirements for personnel. Data Governance Policy defines rules for handling classified data.
HRS-02.2	Are the policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies. Policies are version-controlled in Git.
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established?	PARTIAL	People Security Policy documents clean desk policy and screen lock requirements (5-minute timeout). Currently sole founder implementing manually; no MDM enforcement to verify compliance.
HRS-03.2	Are policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the People Security Policy.
HRS-04.1	Are policies and procedures to protect information at remote sites established?	PARTIAL	People Security Policy documents remote working security requirements including endpoint encryption (BitLocker/LUKS), host firewall, and secure workspace requirements. Currently sole founder; policy framework ready for team scaling.
HRS-04.2	Are policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies. Policies are version-controlled.
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established?	PARTIAL	People Security Policy includes offboarding checklists covering asset return, access revocation, and credential invalidation. Technical capabilities exist for token revocation and user deactivation. Not yet exercised (sole founder).
HRS-06.1	Are procedures outlining roles and responsibilities concerning employment changes established?	PARTIAL	People Security Policy documents procedures for employment changes including role transitions, access modifications, and post-employment obligations. Currently sole founder; procedures documented for future team scaling.
HRS-07.1	Are employees required to sign an employment agreement before gaining access?	PARTIAL	People Security Policy defines security responsibilities for employment terms including acceptable use, data handling, and confidentiality obligations. Contractual templates prepared but not yet exercised (sole founder).
HRS-08.1	Are provisions for adherence to information governance and security policies included in agreements?	PARTIAL	People Security Policy defines security responsibilities to be included in employment agreements. ISMS Policy establishes governance framework. Contractual provisions documented but sole founder; not yet executed with employees.
HRS-09.1	Are employee roles and responsibilities relating to information assets documented?	YES	People Security Policy documents security responsibilities by role. ISMS Policy designates CEO & CISO responsibilities. Application RBAC hierarchy (Operator/Admin/Security/Developer/Viewer) defines information asset access levels.
HRS-10.1	Are requirements for non-disclosure agreements identified, documented, and reviewed?	PARTIAL	People Security Policy defines NDA and confidentiality agreement requirements for employees, contractors, and third parties. Requirements documented but no signatories yet beyond the sole founder.
HRS-11.1	Is a security awareness training program for all employees established?	PARTIAL	People Security Policy documents security training requirements by role, including onboarding and annual refresher training. Currently sole founder with deep security domain expertise. Training program framework ready but no training materials or tracking system yet.
HRS-11.2	Are regular security awareness training updates provided?	PARTIAL	People Security Policy specifies annual refresher training requirements. Currently sole founder; training delivery and update program to be implemented as team grows.
HRS-12.1	Are all employees with sensitive data access provided with appropriate training?	PARTIAL	People Security Policy documents role-specific technical training requirements for employees handling sensitive data. Currently sole founder with deep security expertise. Formal training to be delivered as team grows.
HRS-12.2	Are regular updates in procedures, processes, and policies provided?	PARTIAL	Policies are version-controlled in Git with change tracking. People Security Policy defines ongoing education expectations. Currently sole founder;

ID	Question	Answer	Explanation
			formal update distribution to be implemented as team grows.
HRS-13.1	Are employees notified of their roles and responsibilities to maintain compliance?	PARTIAL	People Security Policy and ISMS Policy define compliance responsibilities. Application RBAC enforces role-based access. Currently sole founder; formal compliance notification procedures to be exercised as team grows.

IAM — Identity & Access Management

17/21 controls satisfied

ID	Question	Answer	Explanation
IAM-01.1	Are identity and access management policies and procedures established?	YES	Access Control Policy (FIMIL-ACP-001) documents IAM requirements. Multi-layer authentication (JWT, sessions, API tokens), 5-level RBAC, tenant isolation, IP blocklist/allowlist, and rate limiting are implemented.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Access Control Policy. Policies are version-controlled.
IAM-02.1	Are strong password policies and procedures established, documented, approved?	YES	Password policy enforces minimum 12 characters with lowercase, uppercase, digit, and special character requirements. Argon2id memory-hard hashing (OWASP-recommended) via pwdlib. Account lockout after 5 failed attempts. Auto IP blocking after 20 failed attempts in 1 hour.
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence for all security policies. Password requirements are enforced in code and documented in the Access Control Policy.
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	YES	UUID-based user identity with email verification. User model tracks is_active, email_verified, role. API token audit service provides platform-wide token visibility. Comprehensive audit logging tracks all access-related events.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	PARTIAL	5-level RBAC hierarchy enforces technical separation of duties. Scan execution is isolated from findings triage. Impersonation restricted to Operator role only. However, sole founder currently holds all authority, so organizational separation of duties is not operating in practice.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	YES	Role-based dependencies enforce least privilege at every endpoint. Subscription plan-based feature gating. API token scoping limits programmatic access. Scanner containers run with --cap-drop ALL. Kubernetes pods run non-root with read-only filesystem.
IAM-06.1	Is a user access provisioning process defined and implemented?	YES	Email verification required for SaaS registration (SHA256-hashed tokens, 24-hour expiry, one-time use). Admin approval required for role elevation. OAuth2/OIDC federation for GitHub and generic OIDC providers. 4-step onboarding wizard for new users.
IAM-07.1	Is a process in place to de-provision or modify access of movers/leavers?	YES	User deactivation sets is_active=False blocking all authentication. Session invalidation on password changes. Bulk token revocation available. People Security Policy documents offboarding with access revocation, asset return, and credential invalidation.
IAM-08.1	Are reviews and revalidation of user access completed with commensurate frequency?	YES	Automated quarterly access reviews via Fimil-Ops endpoints. API token audit service enables platform-wide token visibility and analytics. Admin endpoints provide user management capabilities for access revalidation.
IAM-09.1	Are processes for segregation of privileged access roles defined, implemented?	YES	Operator role is the highest privilege level (100). Impersonation limited to Operator role only with audit trail and 1-hour session cap. Operators cannot impersonate other Operators or Admins. Different RBAC dependencies enforce endpoint-level access control.
IAM-10.1	Is an access process defined to ensure privileged access roles are granted for limited period?	YES	JWT tokens have 30-minute expiry. Sessions expire after 24 hours. Impersonation has 1-hour session cap. OAuth state tokens have 10-minute TTL. API tokens can be revoked at any time.
IAM-10.2	Are procedures implemented to prevent culmination of segregated privileged access?	PARTIAL	RBAC prevents role escalation beyond assigned level. Impersonation audit trail tracks all privilege usage. Operators cannot impersonate other Operators. However, sole founder inherently holds all privilege levels.
IAM-11.1	Are processes for customers to participate in granting high-risk privileged access defined?	PARTIAL	Tenant-scoped RBAC allows customers to manage their own user roles within their tenant. Subscription plan gating restricts feature access. However, no formal customer approval workflow exists for Fimil-side privileged operations on customer data.
IAM-12.1	Are processes to ensure logging infrastructure is read-only defined?	YES	Audit logs are NOT tenant-scoped to preserve history even after tenant deletion. Structlog produces immutable JSON output. Admin dashboard provides read-only access to logs and metrics with CSV export for offline analysis.
IAM-12.2	Is the ability to disable read-only configuration controlled through proper procedures?	PARTIAL	Database admin access could theoretically modify audit logs. Sealed secrets protect database credentials. However, no immutable audit log storage (write-once) is implemented, which is an identified gap.
IAM-13.1	Are processes to ensure users are identifiable through unique identification defined?	YES	UUID-based user identity. Unique email addresses enforced. Audit logs capture user_id, admin_id (for impersonation), tenant_id, IP address, and user agent for full attribution. API tokens have fimil_ prefix and unique identifiers.

ID	Question	Answer	Explanation
IAM-14.1	Are processes for authenticating access including multifactor authentication defined?	YES	TOTP-based MFA implemented with recovery codes and two-step login flow. Password authentication uses Argon2id with complexity requirements, account lockout, and brute force protection. OAuth2/OIDC federation supports MFA at the identity provider level. Multi-factor authentication covers both native and federated authentication paths.
IAM-14.2	Are digital certificates or alternatives adopted for system identities?	YES	TLS certificates managed by cert-manager with Let's Encrypt. API tokens with SHA256 hashing for programmatic access. OAuth2 state parameters with cryptographic binding. JWT tokens with HS256 signing.
IAM-15.1	Are processes for secure management of passwords defined, implemented?	YES	Argon2id memory-hard hashing via pwdlib with complexity requirements (12+ chars, mixed case, digit, special). Constant-time comparison (hmac.compare_digest). Session invalidation on password reset. Account lockout after 5 failed attempts. No plaintext password storage.
IAM-16.1	Are processes to verify access to data and system functions authorized defined?	YES	RBAC enforced at every endpoint via FastAPI dependencies (RequireOperator, RequireAdminOrAbove, etc.). Tenant isolation via TenantScopedModel with ContextVar enforcement. Subscription plan-based feature gating. API token scoping.

IPY — Interoperability & Portability

8/8 controls satisfied

ID	Question	Answer	Explanation
IPY-01.1	Are policies and procedures for communications between application services established?	YES	Kubernetes network policies restrict all pod-to-pod communication by default with explicit allow rules. Scanner containers are network-isolated. API, Web, and Worker have defined ingress/egress rules.
IPY-01.2	Are policies and procedures for information processing interoperability established?	YES	REST API provides standardized JSON interfaces. SARIF output support for findings interoperability. CLI tool supports JSON, table, and SARIF output formats. Webhook integrations with GitHub, GitLab, and Bitbucket.
IPY-01.3	Are policies and procedures for application development portability established?	YES	Docker-based deployment supports multiple environments. Helm charts provide portable Kubernetes deployment. Separate .env configurations for dev, self-hosted, and SaaS modes. Cross-database compatibility (PostgreSQL in prod, SQLite in tests).
IPY-01.4	Are policies and procedures for information/data exchange established?	YES	Data Processing Agreement governs customer data exchange. API token-based programmatic access. SARIF export for findings portability. CSV export for audit logs. Webhook integrations for real-time data exchange with Git providers.
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence for all policies. Technical interoperability is maintained through version-controlled API schemas and Helm charts.
IPY-02.1	Are CSCs able to programmatically retrieve their data via application interface?	YES	Comprehensive REST API with JWT and API token authentication. CLI tool for programmatic access. SARIF and JSON export formats for findings. CSV export for audit logs. API documentation available.
IPY-03.1	Are cryptographically secure and standardized network protocols implemented?	YES	TLS enforced in production via cert-manager with Let's Encrypt. SMTP supports STARTTLS/SSL. All external API calls use HTTPS. Kubernetes network policies enforce secure communication paths.
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination?	YES	Terms of Service and Data Processing Agreement address data access upon termination. Vendor Risk Management Policy includes exit strategies for critical vendors. API enables data export before account closure.

IVS — Infrastructure & Virtualization Security

13/14 controls satisfied

ID	Question	Answer	Explanation
IVS-01.1	Are infrastructure and virtualization security policies and procedures established?	YES	Security hardening guide (docs/operations/security-hardening.md) documents infrastructure security. Network boundary documentation (FIMIL-NB-001) defines zones and port matrix. System Security Plan (FIMIL-SSP-001) maps to NIST 800-53 Low baseline. Kubernetes pods hardened with non-root, read-only filesystem, cap_drop ALL, and no-new-privileges. Network policies restrict all traffic by default.
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence. Infrastructure configuration is version-controlled in Helm charts and reviewed as part of change management.
IVS-02.1	Is resource availability, quality, and capacity planned and monitored?	PARTIAL	HPA configured for CPU (70-80%) and memory (80%) with 2-20 replicas. Resource requests and limits defined. Connection pooling via PgBouncer. However, no formal capacity planning process, no load testing results, and no documented capacity limits.
IVS-03.1	Are communications between environments monitored?	YES	Kubernetes network policies define and restrict all inter-pod communication. Request logging middleware tracks all API calls with correlation IDs. Health monitoring tracks component interactions.
IVS-03.2	Are communications between environments encrypted?	YES	TLS enforced on ingress via cert-manager. Redis password authentication. PgBouncer manages encrypted database connections. All external API calls use HTTPS. SMTP supports STARTTLS/SSL.
IVS-03.3	Are communications between environments restricted to authenticated connections?	YES	Kubernetes network policies restrict all pod-to-pod traffic by default. Database requires authentication. Redis requires password. API endpoints require JWT, session, or API token authentication.
IVS-03.4	Are network configurations reviewed at least annually?	YES	Network policies are version-controlled in Helm chart templates and reviewed as part of change management. ISMS Policy defines annual review cadence for all security configurations.
IVS-03.5	Are network configurations supported by documented justification?	YES	Formal network boundary documentation (FIMIL-NB-001) defines zones and port matrix with justification. Network policies documented in Helm templates with explicit ingress/egress rules per component. Security hardening guide explains network architecture decisions. Scanner network isolation (--network=none) justified by privacy-by-design principles.
IVS-04.1	Is every host and guest OS hardened and supported by technical controls?	YES	Container hardening: non-root users, read-only root filesystem, cap_drop ALL, no-new-privileges, resource limits. Multi-stage Docker builds minimize attack surface. Falco runtime monitoring detects deviations. DigitalOcean manages underlying host OS.
IVS-05.1	Are production and non-production environments separated?	YES	Clear environment separation: Development (Docker Compose, remapped ports), Testing (SQLite in-memory, MockRedis), Production (managed PostgreSQL, Redis with password, sealed secrets, TLS enforced). Separate environment configurations.
IVS-06.1	Are applications and infrastructures designed to appropriately segment access?	YES	Kubernetes namespaces and network policies segment infrastructure. Row-level tenant isolation in the application. RBAC at every endpoint. Scanner containers fully network-isolated. Separate network policies per component (API, Web, Worker).
IVS-07.1	Are secure and encrypted communication channels used when migrating?	YES	Helm-based deployments use Kubernetes API over TLS. Container images pushed to DigitalOcean container registry over HTTPS. Database migrations run within the cluster. Sealed secrets protect credentials during deployment.
IVS-08.1	Are high-risk environments identified and documented?	YES	Risk Assessment identifies high-risk components. Scanner containers identified as high-risk and isolated with --network=none, cap_drop ALL, and resource limits. Production environment documented with specific security requirements (non-default SECRET_KEY, TLS enforcement).
IVS-09.1	Are processes and defense-in-depth techniques defined for network attack protection?	YES	Defense-in-depth: Cloudflare WAF with managed rulesets, Kubernetes network policies, scanner network isolation, ingress TLS, rate limiting, IP blocklist/allowlist, CSRF protection, account lockout, brute force detection, and Falco runtime monitoring.

LOG — Logging & Monitoring

15/18 controls satisfied

ID	Question	Answer	Explanation
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved?	YES	Structlog-based structured logging with JSON output in production. Monitoring documentation in docs/operations/monitoring.md covers Prometheus integration, alerting rules, and Grafana dashboards. Audit logging tracks 40+ action types.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence. Monitoring documentation is version-controlled and updated as infrastructure evolves.
LOG-02.1	Are processes to ensure audit log security and retention defined?	YES	Audit logs stored in PostgreSQL with access controls. Logs are NOT tenant-scoped to preserve history even after tenant deletion. Admin-only access to audit endpoints. Nightly backups to S3 preserve log data. CSV export enables offline archival.
LOG-03.1	Are security-related events identified and monitored?	YES	Security monitoring service auto-detects brute force, credential stuffing, impossible travel, API anomalies, suspicious IPs, and account takeover attempts. Security alerts classified by severity (critical/high/medium/low).
LOG-03.2	Is a system defined to generate alerts to responsible stakeholders?	YES	Security alerts surface to admin dashboard. Critical findings alerts via email and Slack. Incident model tracks active/resolved incidents. Announcement system for system-wide notifications. Falco generates runtime security alerts.
LOG-04.1	Is access to audit logs restricted to authorized personnel?	YES	Admin-only access to audit endpoints enforced via RequireAdmin dependency. Audit log queries support filtering to limit scope. CSV export enables controlled offline analysis.
LOG-05.1	Are security audit logs monitored to detect unusual activity?	YES	Security monitoring service provides automated threat detection. Brute force detection (20+ failed attempts/hour), credential stuffing detection (10+ unique emails/hour). Admin dashboard surfaces all security events.
LOG-05.2	Is a process established to review and take appropriate actions on anomalies?	YES	Incident Response Plan defines procedures for security event triage, investigation, and response. Admin dashboard provides alert acknowledgement and resolution workflow. Automatic IP blocking for brute force. Account lockout for repeated failures.
LOG-06.1	Is a reliable time source being used across all relevant systems?	YES	All timestamps use datetime.now(UTC). DigitalOcean managed Kubernetes runs NTP on all nodes. Structlog uses ISO 8601 timestamps. JWT tokens include iat and exp claims for temporal validation.
LOG-07.1	Are logging requirements for information system events established?	YES	Audit logging tracks 40+ action types including authentication, user management, scan operations, finding status changes, API token lifecycle, policy changes, and subscription events. Each entry captures user_id, tenant_id, IP, user agent, and request_id.
LOG-07.2	Is the scope reviewed and updated at least annually?	YES	ISMS Policy defines annual review cadence. Logging scope expands as new features are added, with audit action types defined in the audit service. Monitoring documentation is version-controlled.
LOG-08.1	Are audit records generated containing relevant security information?	YES	Each audit log entry captures: user_id, admin_id (for impersonation), tenant_id, action, resource_type, resource_id, details JSON, ip_address, user_agent, request_id, and timestamp. Failed login attempts tracked separately with failure reason and optional geo data.
LOG-09.1	Does the information system protect audit records from unauthorized access?	YES	Audit logs stored in PostgreSQL with database-level access controls. Admin-only API access enforced via RequireAdmin dependency. Audit logs are NOT tenant-scoped to prevent deletion. However, no immutable write-once storage is implemented.
LOG-10.1	Are monitoring and reporting capabilities established for cryptographic operations?	PARTIAL	Production enforcement validates non-default SECRET_KEY and issues warnings for auto-generated keys. Audit logging tracks authentication events involving cryptographic operations. However, no dedicated cryptographic operations monitoring dashboard.
LOG-11.1	Are key lifecycle management events logged and monitored?	PARTIAL	MultiFernet versioned key rotation and re-encryption tooling exist. API token creation and revocation are logged in the audit trail. However, no dedicated logging for encryption key lifecycle events (rotation, re-encryption runs) and no centralized key lifecycle monitoring dashboard.
LOG-12.1	Is physical access logged and monitored using an auditable system?	NA	Cloud-hosted on DigitalOcean. Physical access logging is the cloud provider's responsibility under the shared responsibility model.
LOG-13.1	Are processes for reporting monitoring system anomalies and failures defined?	YES	Health monitoring service tracks system component status with degraded/down detection. Incident model enables tracking of monitoring failures. Incident Response Plan defines escalation procedures for system anomalies.
LOG-13.	Are accountable parties immediately notified	YES	Security alerts surface to admin dashboard in real time. Critical findings

ID	Question	Answer	Explanation
2	about anomalies and failures?		alerts via email and Slack. Incident Response Plan defines notification timelines. Falco runtime alerts provide immediate notification of security events.

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

10/11 controls satisfied

ID	Question	Answer	Explanation
SEF-01.1	Are policies and procedures for security incident management established?	YES	Incident Response Plan (FIMIL-IRP-001) defines four severity levels, detection mechanisms, response phases (triage, containment, eradication, recovery, communication), incident commander role, and escalation procedures.
SEF-01.2	Are policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence for all policies including the Incident Response Plan. Policies are version-controlled in Git.
SEF-02.1	Are policies and procedures for timely incident management established?	YES	Incident Response Plan defines response timelines by severity level. Regulatory notification timelines documented (GDPR 72-hour, CCPA). Automatic IP blocking and account lockout provide immediate automated response.
SEF-02.2	Are policies and procedures reviewed and updated at least annually?	YES	ISMS Policy defines an annual review cadence. Incident Response Plan is version-controlled and updated based on lessons learned from incidents.
SEF-03.1	Is a security incident response plan established and documented?	YES	Incident Response Plan (FIMIL-IRP-001) is formally documented with severity levels, response phases, communication templates, regulatory notification procedures, and post-incident review process.
SEF-04.1	Is the security incident response plan tested and updated at planned intervals?	PARTIAL	Incident Response Plan is documented and updated as needed. Automated incident response (IP blocking, account lockout) is operationally validated. However, no formal tabletop exercise or IR simulation has been conducted.
SEF-05.1	Are information security incident metrics established and monitored?	YES	Security monitoring tracks brute force attempts, credential stuffing, failed login rates, and alert counts. Incident model tracks resolution times. Admin security dashboard surfaces incident metrics.
SEF-06.1	Are processes supporting business processes to triage security events defined?	YES	Security alert system classifies events by severity (critical/high/medium/low). Alert types include brute_force, credential_stuffing, impossible_travel, api_anomaly, suspicious_ip, and account_takeover. Admin dashboard enables triage with acknowledge/resolve workflow.
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined?	YES	Incident Response Plan includes breach notification procedures with GDPR 72-hour and CCPA timelines. Customer notification via announcement system. Regulatory contact procedures documented in Compliance Register.
SEF-07.2	Are security breaches reported as per applicable SLAs, laws, and regulations?	YES	Incident Response Plan documents notification timelines aligned with GDPR (72-hour), CCPA, and customer SLA requirements. Compliance Register tracks regulatory notification obligations.
SEF-08.1	Are points of contact maintained for applicable regulatory and legal authorities?	YES	Incident Response Plan includes CISA/CIRCIA federal incident reporting procedures with specific contact points. Compliance Register tracks regulatory obligations. GDPR and CCPA notification contacts documented. Regulatory notification timelines established (GDPR 72-hour, CCPA, CIRCIA).

STA — Supply Chain Management, Transparency & Accountability

11/15 controls satisfied

ID	Question	Answer	Explanation
STA-01.1	Are policies and procedures implementing the shared security responsibility model established?	YES	Vendor Risk Management Policy (FIMIL-VRM-001) documents shared responsibility model with DigitalOcean. Security whitepaper at /security communicates customer responsibilities. DPA defines data processing responsibilities.
STA-01.2	Are the policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence. Vendor Risk Management Policy defines review cadence by tier (annual for Tier 1, biannual for Tier 2).
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain?	YES	Vendor Risk Management Policy establishes three-tier vendor classification with documented shared responsibility for each. DPAs executed with all vendors. Exit strategies documented for critical vendors.
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability?	YES	Security whitepaper at /security communicates security architecture and customer responsibilities. Terms of Service and DPA define data handling responsibilities. SLA published at /legal/sla.
STA-04.1	Is the shared ownership and applicability of all CCM controls delineated?	PARTIAL	Vendor Risk Management Policy documents shared responsibility with DigitalOcean. Physical controls marked as cloud provider responsibility. However, a formal CCM-specific control ownership matrix has not been produced.
STA-05.1	Is SSRM documentation for all cloud services reviewed and validated?	PARTIAL	Vendor assessments documented for all critical vendors (DigitalOcean, GitHub, Stripe, Cloudflare, Resend, PostHog). Vendor Risk Management Policy defines review cadence. However, review schedule not yet exercised (policies just established).
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented?	YES	Fimil implements all customer-side responsibilities: application security, authentication, authorization, encryption, logging, monitoring, incident response, and data governance. Cloud provider handles physical infrastructure and host-level security.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	YES	Vendor Risk Management Policy documents all vendors with three-tier classification: Tier 1 (DigitalOcean, GitHub, Stripe), Tier 2 (Cloudflare, Resend), Tier 3 (PostHog). DPA status tracked for each vendor.
STA-08.1	Are risk factors associated with all organizations in the supply chain reviewed?	YES	Individual vendor risk assessments documented for all six vendors. Risk ratings assigned by tier. Exit strategies documented for critical vendors. SOC 2 report collection tracked.
STA-09.1	Do service agreements incorporate mutually agreed upon security provisions?	YES	DPAs executed with all critical and significant vendors as of 2026-03-14. Vendor Risk Management Policy defines security requirements by tier. Customer-facing DPA at /legal/dpa defines mutual data protection obligations.
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	YES	Vendor Risk Management Policy defines review cadence by tier: annual for Tier 1 (critical), biannual for Tier 2 (significant). ISMS Policy mandates annual policy review.
STA-11.1	Is there a process for conducting internal assessments at least annually?	YES	CSA STAR Level 1 self-assessment completed. Statement of Applicability maps ISO 27001 controls with implementation status. Compliance Register tracks regulatory compliance. ISMS Policy defines annual review cadence. Automated quarterly access reviews via Fimil-Ops endpoints. Continuous monitoring plan (FIMIL-CONMON-001) provides ongoing assessment.
STA-12.1	Are policies requiring all supply chain CSPs to comply with security requirements implemented?	YES	Vendor Risk Management Policy defines security requirements by vendor tier. DPAs include security obligations. Docker images scanned with Trivy, signed with Cosign via Sigstore, include SPDX SBOMs, and have GitHub Actions build provenance attestation. Dependabot monitors supply chain dependencies. Scanner containers sandboxed with --network=none and cap_drop ALL.
STA-13.1	Are supply chain partner IT governance policies reviewed periodically?	PARTIAL	Vendor Risk Management Policy defines review cadence for vendor assessments. SOC 2 report collection tracked. However, review schedule not yet exercised and no automated vendor monitoring in place.
STA-14.1	Is a process to conduct periodic security assessments for supply chain organizations defined?	PARTIAL	Vendor Risk Management Policy defines assessment procedures by tier with documented review cadences. However, periodic assessments have not yet been executed; the initial vendor assessments were just established.

TVM — Threat & Vulnerability Management

11/12 controls satisfied

ID	Question	Answer	Explanation
TVM-01.1	Are policies and procedures established to identify, report, and prioritize vulnerability remediation?	YES	Core platform function. EPSS enrichment provides exploit probability scores. Priority scoring (0-100) combines severity, age, reachability, and EPSS. Auto-triage rules classify findings. Risk Assessment documents vulnerability treatment plans.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence for all policies. Vulnerability management capabilities evolve continuously as the platform is itself a security product.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established?	YES	Scanner containers sandboxed with --network=none, --cap-drop ALL, no-new-privileges, read-only mounts, and resource limits. Falco DaemonSet provides runtime malware detection with 7 custom rules. People Security Policy documents endpoint antivirus requirements.
TVM-02.2	Are asset management and malware protection policies reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence. Falco rules and container security configurations are version-controlled in Helm charts.
TVM-03.1	Are processes to enable scheduled and emergency responses to vulnerability identification?	YES	Patch management SLA (FIMIL-PM-001) defines remediation timelines: Critical 24h, High 7d, Medium 30d. Trivy scanning in CI/CD blocks critical vulnerabilities from deployment (emergency gate). Dependabot provides automated dependency update PRs. Change Management Policy defines Emergency change type for urgent security patches.
TVM-04.1	Are processes to update detection tools and threat signatures on weekly basis?	YES	Platform uses latest-tagged scanner images (Semgrep, Trivy, Grype, etc.) which include up-to-date vulnerability databases and detection signatures. EPSS data refreshed from FIRST.org with 24-hour Redis cache TTL.
TVM-05.1	Are processes to identify updates for applications using third-party libraries defined?	YES	Dependabot configured across all repositories for automated dependency updates with pull request generation. Trivy and Grype scan for known vulnerabilities in dependencies. OSV-Scanner provides Google OSV database coverage. Patch management SLA (FIMIL-PM-001) defines remediation timelines: Critical 24h, High 7d, Medium 30d.
TVM-06.1	Are processes for periodic, independent, third-party penetration testing defined?	NO	No penetration testing program exists. No independent third-party security assessment has been conducted. This is the top identified gap in the compliance assessment (ISO A.5.35).
TVM-07.1	Are processes for vulnerability detection on managed assets at least monthly defined?	YES	Trivy image scanning runs on every deployment via CI/CD. The platform provides continuous vulnerability scanning. Falco runtime monitoring runs continuously. Vulnerability detection occurs on every code push, not just monthly.
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model?	YES	Priority scoring (0-100) combines severity (60%), age (20%), reachability (15%), and EPSS (5%). Reachability analysis distinguishes direct from transitive dependencies. Auto-triage rules classify findings based on risk patterns.
TVM-09.1	Is a process defined to track and report vulnerability identification and remediation?	YES	Finding status tracking (open, confirmed, false_positive, accepted, fixed) with audit trail. Scan comparison shows new, fixed, and unchanged findings between scans. PR scanning identifies regressions. Weekly digest notifications summarize vulnerability status.
TVM-10.1	Are metrics for vulnerability identification and remediation established?	YES	Scanner health metrics track success/failure rates and execution times. Finding status transitions tracked over time. Scan comparison provides new/fixed/unchanged counts. Priority scoring provides quantified risk metrics. Weekly digest reports aggregate vulnerability trends.

UEM — Universal Endpoint Management

1/15 controls satisfied

ID	Question	Answer	Explanation
UEM-01.1	Are policies and procedures established for all endpoints?	PARTIAL	People Security Policy (FIMIL-PPL-001) documents endpoint security requirements: full-disk encryption, host firewall, screen lock after 5 minutes, and antivirus. However, no MDM enforcement or automated compliance verification. Currently sole founder implementing manually.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated annually?	YES	ISMS Policy defines an annual review cadence for all policies including the People Security Policy which covers endpoint management.
UEM-02.1	Is there a defined list of approved services, applications, and acceptable sources?	PARTIAL	Acceptable Use Policy and People Security Policy document permitted usage. Vendor Risk Management Policy tracks approved services. However, no formal approved application list or software whitelist for endpoints.
UEM-03.1	Is a process defined to validate endpoint device compatibility?	PARTIAL	People Security Policy specifies endpoint requirements (encryption, firewall, screen lock). However, no MDM or automated device compliance checking is implemented. Validation is manual.
UEM-04.1	Is an inventory of all endpoints used and maintained?	PARTIAL	Formal asset register (FIMIL-AM-001) with 26-row inventory covers infrastructure and application assets. Currently sole founder with known devices. However, no MDM-managed endpoint inventory with automated device discovery and compliance tracking.
UEM-05.1	Are processes to enforce policies and controls for all endpoints defined?	PARTIAL	People Security Policy defines endpoint security requirements. Technical enforcement exists for server-side endpoints (container hardening, network policies). However, no MDM for user endpoint policy enforcement.
UEM-06.1	Are all relevant interactive-use endpoints configured to require automatic lock screen?	PARTIAL	People Security Policy requires screen lock after 5 minutes of inactivity. Currently implemented manually by the sole founder. No MDM enforcement to verify or enforce the setting.
UEM-07.1	Are changes to endpoint operating systems managed through change management?	PARTIAL	Change Management Policy governs infrastructure changes. Server-side containers use immutable images with version tags. However, user endpoint OS changes are not managed through formal change management (no MDM).
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints?	PARTIAL	People Security Policy requires full-disk encryption (BitLocker/LUKS). Technical controls protect server-side data (Fernet encryption, sealed secrets). However, no DLP tooling on user endpoints and no MDM verification.
UEM-09.1	Are anti-malware detection and prevention technology services configured?	PARTIAL	People Security Policy documents endpoint antivirus requirements. Falco provides runtime malware detection for server-side containers. However, no centrally managed anti-malware for user endpoints (no MDM).
UEM-10.1	Are software firewalls configured on managed endpoints?	PARTIAL	People Security Policy requires host firewall enabled on all endpoints. Kubernetes network policies protect server-side endpoints. However, user endpoint firewall configuration is manual without MDM enforcement.
UEM-11.1	Are managed endpoints configured with data loss prevention technologies?	NO	No DLP tooling is deployed on user endpoints. Server-side controls prevent data leakage (tenant isolation, rate limiting, network-isolated scanners), but no endpoint DLP is configured.
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	NO	No MDM solution is deployed, so no remote geolocation capability exists for mobile endpoints. Currently sole founder; MDM to be evaluated as team grows.
UEM-13.1	Are processes to enable remote company data deletion on managed devices defined?	PARTIAL	People Security Policy documents remote wipe requirements. Server-side capabilities exist for access revocation (user deactivation, token revocation, session invalidation). However, no MDM for actual device-level remote wipe.
UEM-14.1	Are processes to maintain proper security of third-party endpoints defined?	PARTIAL	People Security Policy documents BYOD and third-party device security requirements. Vendor Risk Management Policy covers third-party security. However, no technical enforcement for third-party endpoints.