IMS · SHARED ASSESSMENTS SIG-LITE SCAFFOLD

Security Questionnaire Pre-fill

v1 scaffold · pre-filled with IMS architecture as of 2026-04-25

PURPOSE

Procurement-grade pre-fill of the Shared Assessments SIG-Lite security questionnaire, attached as a procurement artefact for institutional buyers.

SCOPE

IMS marketing surface (ims.quintarthai.com / quintarthai.com/ims) and IMS console (quintarthai.com/tracker), operated by Quintessentia Network Inc. (Canada).

METHODOLOGY VERSION

IMS methodology v1 — see /ims/methodology.html

TOTAL QUESTIONS

80 across 20 domains

STATUS LEGEND

ANSWERED = grounded in IMS architecture today, defensible in audit · PARTIAL = partially true today, full answer pending milestone · PLANNED = on roadmap, honest 'no' today · ORG-SPEC = requires Quintessentia officer to fill in (HR / finance / legal) · N/A = not applicable

Status breakdown:

- ANSWERED 40 questions (50%)
- PARTIAL 18 questions (22%)
- PLANNED 12 questions (15%)
- ORG-SPEC 9 questions (11%)
- N/A 1 questions (1%)

How to use this scaffold:

1. Read the ANSWERED rows — these are the security commitments IMS makes today, verifiable in production by inspecting the live system or its public artefacts.
2. Read the PARTIAL and PLANNED rows — these are the explicit gaps. They are NOT marked as fulfilled; do not let any vendor mark them as such without evidence.
3. The ORG-SPEC rows must be completed by a Quintessentia officer before this scaffold is delivered to a procurement counterparty as a final artefact.
4. Versioning: this is scaffold v1. Each material change increments the version and is announced at /ims/changelog.html.

DOMAIN A

Risk Assessment & Risk Treatment

A.1.1 PARTIAL

Does the organisation have a documented information-security risk-assessment methodology?

Internal threat-model doc exists for IMS architecture; formal documented methodology will be produced as part of SOC 2 Type I scoping in Q3 2026.

A.1.2 PLANNED

Is risk assessment performed at least annually?

Founder-level review monthly today; formal annual cycle begins with SOC 2 engagement.

A.1.3 ORG-SPEC

Are identified risks tracked to closure with named owners?

Risk register maintained internally by Quintessentia officers.

DOMAIN B

Information Security Policy

B.1.1 PARTIAL

Does an information-security policy exist, approved by management, and reviewed at least annually?

Internal security posture documented at /ims/methodology and /ims/privacy. Formal approved policy doc on roadmap with SOC 2 engagement.

B.1.2 ORG-SPEC

Is the policy communicated to all staff and contractors?

Quintessentia internal — small team; formal acknowledgement workflow on roadmap.

B.1.3 PLANNED

Are exceptions to the policy formally approved and tracked?

Will be tracked with policy formalisation.

DOMAIN C

Organisation of Information Security

C.1.1 ORG-SPEC

Is a named individual accountable for information security?

Quintessentia internal — named officer to be confirmed in MSA.

C.1.2 PARTIAL

Are security roles and responsibilities documented?

Engineering responsibilities documented in /ims/methodology; formal RACI matrix on roadmap.

C.1.3 PARTIAL

Does the organisation participate in industry security forums?

Founder follows OWASP, CISA, and humanitarian InfoSec working groups; active membership pending bandwidth.

DOMAIN D

Asset Management

D.1.1 ANSWERED

Is there a complete inventory of information assets?

All production assets enumerated in internal infrastructure manifest. Source registry published live at /ims/sources.html.

D.1.2 ANSWERED

Are assets classified by sensitivity?

Public · Internal · Restricted · High classification used; default for IMS data is Public (open-source signals only).

D.1.3 ORG-SPEC

Are asset owners assigned?

Founder/officer-level assignment today; expanded as the team grows.

DOMAIN E

Human Resources Security

E.1.1 PLANNED

Are background checks performed on personnel with access to customer data?

Founder-only access today; background-check policy to be in place before first hire.

E.1.2 ORG-SPEC

Do staff sign confidentiality / non-disclosure agreements?

Quintessentia internal HR policy.

E.1.3 PLANNED

Is security training provided to all personnel at onboarding and at least annually?

Training programme will be in place before first hire; founder maintains personal CPE through OWASP and CISA briefings.

E.1.4 PLANNED

Is there a documented offboarding process that revokes access immediately?

Documented offboarding policy will be in place before first hire.

DOMAIN F

Physical & Environmental Security

F.1.1 N/A

Are physical premises protected by access controls (badges, locks, CCTV)?

IMS production infrastructure runs in a Tier-3+ data centre operated by Hostinger International (Lithuania, EU). Quintessentia has no on-premises servers; all engineering happens on encrypted endpoints.

F.1.2 ORG-SPEC

Is there documented physical-security policy for office locations?

Quintessentia officer — small home-office today; relevant policy will be drafted before any office is established.

F.1.3 ANSWERED

Is environmental monitoring (fire, water, temperature) in place at the data centre?

Hostinger-operated facility — Tier-3+ certified; specifics on Hostinger's data centre certifications available on request.

DOMAIN G

Communications & Operations Management

G.1.1 — ANSWERED

Are change-management procedures documented and followed?

Every change to the IMS marketing surface and tracker production code is logged in /root/PROJECT_LOG.md with timestamp, scope, backup pointer, and verification — published publicly at /ims/changelog.html.

G.1.2 — PARTIAL

Is segregation of duties enforced for production deployments?

Founder is currently the sole production deployer; segregation enforced architecturally (config-via-script, hooks log each change, instant rollback via .bak files).

G.1.3 — ANSWERED

Are backups taken regularly and restoration tested?

Postgres pg_dump nightly at 02:00 UTC, 30-day retention, stored at /var/backups/postgres/ on an encrypted volume.

G.1.4 — ANSWERED

Is system capacity monitored?

Live status at /ims/status.html exposes ingest lag, throughput, and source-feed counts pulled directly from production telemetry.

G.1.5 — PARTIAL

Are all systems patched to current security-update levels?

Ubuntu 22.04 LTS · unattended-upgrades enabled for security-only · monthly manual review of outstanding updates.

DOMAIN H

Access Control

H.1.1 ANSWERED

Is access to systems granted based on least privilege?

Production access limited to founder via SSH key-only authentication; no password-based login; root-only operations; no shared credentials.

H.1.2 ANSWERED

Are user accounts uniquely identifiable?

All user accounts in the IMS console use unique identifiers; audit-log rows attribute every privileged action.

H.1.3 ANSWERED

Are passwords required to meet complexity standards?

IMS console enforces NIST SP 800-63B-aligned password rules; SSO via SAML on the founding-cohort roadmap.

H.1.4 PARTIAL

Is multi-factor authentication required for privileged access?

Founder uses SSH key auth (effectively MFA via key + passphrase) for production; TOTP/WebAuthn supported for IMS console users; mandatory MFA enforcement policy on roadmap.

H.1.5 ORG-SPEC

Are access reviews conducted at least quarterly?

Founder-level review weekly; formal quarterly review cycle starts with SOC 2 engagement.

DOMAIN I

Information Systems Acquisition, Development, Maintenance

I.1.1 ANSWERED

Are secure-coding practices followed (OWASP Top 10 awareness)?

OWASP Top 10 actively considered for every endpoint; CSP, CSRF protection via SameSite cookies, parametrised queries, input validation. Methodology published at /ims/methodology.

I.1.2 ANSWERED

Is the source-code repository protected with access control and audit?

Private Git repository; access via SSH key only; commit history is the audit trail.

I.1.3 PARTIAL

Are dependencies vetted and monitored for known vulnerabilities?

Python `requirements.txt` and Node `package.json` reviewed at each release; automated CVE scanning via GitHub Dependabot on roadmap.

I.1.4 PARTIAL

Are changes to production code reviewed before deployment?

Single-founder review today; formal peer review begins when team grows beyond one engineer.

I.1.5 ANSWERED

Is there a separate environment for development / staging / production?

Production at quintarthai.com; staging at staging.quintarthai.com (same VPS, separate nginx vhost); local development on encrypted founder workstation.

DOMAIN J

Information Security Incident Management

J.1.1 PARTIAL

Is there a documented incident-response plan?

Founder maintains an internal incident-response runbook; formal multi-stakeholder IR plan to be finalised with SOC 2 engagement.

J.1.2 PARTIAL

Are security incidents categorised by severity?

Internal severity tiers used; published rubric will accompany the SOC 2 engagement.

J.1.3 ANSWERED

Is there a defined breach-notification timeline aligned with GDPR (72 hours)?

DPA template at /ims/dpa.html commits to 72-hour breach notification per GDPR Art. 33.

J.1.4 PARTIAL

Are post-incident reviews conducted?

Internal post-mortem practice for any production incident; written post-mortem documents on roadmap.

J.1.5 ANSWERED

Is a security contact published?

security@quintarthai.com published in /.well-known/security.txt at quintarthai.com.

DOMAIN K

Business Continuity Management

K.1.1 PLANNED

Is a business-continuity plan documented?

BCP scoping starts with SOC 2 engagement Q3 2026.

K.1.2 PARTIAL

Is a disaster-recovery plan documented?

Production data is recoverable from nightly Postgres pg_dump backups; full DR runbook on roadmap.

K.1.3 PARTIAL

Are recovery-time objectives (RTO) and recovery-point objectives (RPO) defined?

Internal targets: RTO 4h, RPO 24h based on backup cadence. Customer-specific RTO/RPO available on contract.

K.1.4 PLANNED

Are continuity tests performed regularly?

Quarterly restore test on roadmap with SOC 2 engagement.

DOMAIN L
Compliance

L.1.1 ANSWERED
Does the organisation comply with applicable data-protection regulations (GDPR, CCPA, PIPEDA)?
Privacy posture documented at /ims/privacy.html, designed against GDPR, CCPA, and PIPEDA. Quintessentia is incorporated in Canada (PIPEDA jurisdiction); EU residency offered on contract.

L.1.2 PLANNED
Are independent security audits performed annually?
SOC 2 Type I targeted Q3 2026 will be the first independent audit.

L.1.3 ANSWERED
Is intellectual-property compliance maintained for all third-party software?
Open-source dependencies tracked; licence audit performed at each release.

L.1.4 ANSWERED
Are records retained per legal/contractual requirements?
Retention schedule per /ims/privacy.html: lead form 24 months · access logs 30 days · analytics events 90 days.

DOMAIN M

End-User Device Security

M.1.1 ANSWERED

Are end-user devices encrypted at rest?

All Quintessentia engineering endpoints use full-disk encryption (FileVault / BitLocker / LUKS).

M.1.2 ORG-SPEC

Is endpoint anti-malware deployed?

Endpoint posture per Quintessentia HR policy.

M.1.3 PLANNED

Are endpoints centrally managed (MDM)?

MDM deployment when team grows beyond founder.

M.1.4 ANSWERED

Are removable media restricted?

Production keys never leave encrypted endpoints; no use of USB/removable media for production data.

DOMAIN N

Network Security

N.1.1 ANSWERED

Are firewalls deployed at network perimeters?

Hostinger network-edge filtering plus host-level iptables on the production VPS. Default INPUT policy: DROP. Only TCP 22 (SSH), 80 (HTTP redirect), 443 (HTTPS), and UDP 443 (HTTP/3) are allowed.

N.1.2 PARTIAL

Are intrusion-detection / prevention systems in place?

Application-level WAF rules in nginx (block_sqli, block_xss, block_traversal, block_agent, block_cmd_injection, block_crlf, block_ldap, block_ssrf, block_nosql); host-level fail2ban; network-level IDS on roadmap.

N.1.3 ANSWERED

Is internal network traffic encrypted?

Inter-service traffic on the VPS uses local Unix sockets where possible; remaining service-to-service traffic uses loopback only (127.0.0.1).

N.1.4 ANSWERED

Are public services rate-limited?

/ims-api/leads (5 req/min, burst 10), /ims-api/track (60 req/min, burst 20), tracker API (existing limits). Verifiable from /etc/nginx config.

N.1.5 ANSWERED

Is HTTPS enforced site-wide with strong ciphers?

TLS 1.2 (AES-256-GCM-SHA384) and TLS 1.3 (TLS_AES_256_GCM_SHA384). HSTS preload. HTTP/2 + HTTP/3 enabl

DOMAIN O
Privacy

O.1.1 ANSWERED
Is a Privacy Policy published and current?
Published at /ims/privacy.html, updated 2026-04-25 (versioned with date).

O.1.2 ANSWERED
Are sub-processors disclosed?
Hostinger International Ltd. (hosting · EU); Let's Encrypt (TLS issuance, no PII shared). Listed in /ims/privacy.html and DPA template.

O.1.3 ANSWERED
Is a Data Processing Agreement available?
DPA template published at /ims/dpa.html (Module 2 Controller-to-Processor SCCs incorporated).

O.1.4 ANSWERED
Are data subjects' rights (access, deletion, portability) honoured?
All GDPR Art. 15-22 rights honoured per /ims/privacy.html. Response within 30 days. Contact privacy@quintarthai.com.

O.1.5 ANSWERED
Is data minimisation practiced?
Marketing site collects only what's required for response (name, email, org, role, use case). No cookies, no fingerprinting, no third-party tags.

O.1.6 ANSWERED
Are children's data protections in place?
Service is not directed at children under 16. We do not knowingly collect their data. Stated in /ims/privacy.html §9.

DOMAIN P

Threat & Vulnerability Management

P.1.1 PARTIAL

Are vulnerability scans performed on infrastructure?

Manual reviews using openvas/nuclei; automated scheduled scans on roadmap.

P.1.2 ANSWERED

Is a responsible-disclosure programme in place?

Coordinated disclosure invited via /.well-known/security.txt at quintarthai.com.

P.1.3 PLANNED

Are penetration tests performed annually?

First pen test scheduled to coincide with SOC 2 Type I scoping.

DOMAIN Q

Server Security

Q.1.1 — PARTIAL

Are servers hardened per a documented baseline?

Internal hardening checklist applied (key-only SSH, default-DROP firewall, minimal package set, automatic security updates). Formal CIS-benchmark-style documentation on roadmap.

Q.1.2 — ANSWERED

Is logging centralised and retained?

nginx access + error logs retained 30 days; ims-events analytics log retained 90 days; ims-leads log retained 24 months. Quarterly archival to off-site storage.

Q.1.3 — ANSWERED

Is time synchronisation enabled across all servers?

systemd-timesyncd active; UTC.

Q.1.4 — ANSWERED

Are admin actions logged with user attribution?

Every production change logged in /root/PROJECT_LOG.md with timestamp, scope, and operator. SSH session logs retained per system default.

DOMAIN R
Cloud Security

R.1.1 — ANSWERED
Is the cloud provider compliant with industry standards (ISO 27001, SOC 2)?
Hostinger International Ltd. — ISO 27001 certified data centres (Lithuania).

R.1.2 — PARTIAL
Are cloud configurations reviewed against best practice?
Initial config follows hardening checklist; periodic review on roadmap.

R.1.3 — ANSWERED
Is data segregated by customer?
Logical isolation today; per-customer dedicated infrastructure available on Institutional tier on contract.

DOMAIN S

Application Security

S.1.1 ANSWERED

Is input validation applied to all user-supplied data?

All API endpoints validate input shape and size; nginx WAF rules block common injection patterns at the edge.

S.1.2 ANSWERED

Are output encoding controls applied to prevent XSS?

All dynamic HTML rendered through templates with auto-escaping; CSP `default-src 'self'` blocks any successful inline-script injection.

S.1.3 ANSWERED

Are SQL parametrisation / ORM safeguards in use?

All database queries parametrised via SQLAlchemy / asyncpg; no string concatenation.

S.1.4 ANSWERED

Are file uploads scanned and restricted?

Marketing surface accepts no file uploads. The IMS console accepts no file uploads from end users today (briefs are generated, not uploaded).

S.1.5 ANSWERED

Is session management secure (HttpOnly, Secure, SameSite=Strict)?

Session cookies use HttpOnly, Secure, SameSite=Lax. Marketing surface sets zero cookies.

DOMAIN T

Cybersecurity Incident Management (per SIG-Lite expansion)

T.1.1 PLANNED

Is an incident-response retainer in place with an external firm?

External IR retainer to be evaluated alongside SOC 2 engagement.

T.1.2 PLANNED

Are tabletop exercises performed?

Quarterly tabletop on roadmap.

T.1.3 ORG-SPEC

Is cyber-insurance carried?

Quintessentia internal — coverage being evaluated.

CLOSING NOTES

Limitations of this scaffold

- This is scaffold v1. Many ORG-SPEC and PLANNED items will move to ANSWERED through the Q3 2026 SOC 2 Type I engagement.
- 'PARTIAL' is honest reporting, not deflection. We mark a control PARTIAL when the architectural / operational basis is in place but documentation / formalisation is on the roadmap. Buyers should treat PARTIAL as 'evidence available, not yet packaged for audit'.
- Where this scaffold conflicts with a signed Master Services Agreement or Data Processing Agreement, the signed instrument prevails.
- To request the live source-feed registry, the engineering audit log, or any specific evidence cited above, email trust@quintarthai.com.
- This document carries a SHA-256 hash in its footer. Any modification to this PDF after distribution will break the hash.

Hash (full): eb5b252ac143593adb487cebb132ce3dc9f451ff1da7302a856f9e5155e4198f