Control Crosswalk (CAIQ-style)

A control-by-control responses sheet for vendor security assessments, organized by the CSA Cloud Controls Matrix (CCM) domains and answerable against SOC 2, ISO 27001, and NIST. Companion to the architecture document and security overview.

Status — Available shipped today · Built implemented + tested, not operationally deployed · Planned committed, not built · No not implemented today.

Read this first. The product shipped today is a **single-party desktop workbench** with **remote LLM inference** (your prompts and in-scope context are sent to the LLM provider you configure). Many enterprise/hosted controls below are therefore *Built* or *Planned*, not *Available*. Answers are honest about that distinction.

#	Domain	Control question	Response	Status	Evidence
GRC-01	Governance	Is there a documented security/architecture model?	Yes — enterprise architecture & security doc, a formal invariant set, append-only ADRs.	Available	Arch; `specs/`
GRC-02	Governance	Third-party certifications (SOC 2 / ISO 27001)?	No certification today. SOC 2 Type II is highest-priority committed; ISO 27001 not yet on the roadmap.	Planned	Arch §12
A&A-01	Audit & Assurance	Is the security model independently verified?	Machine-checked (42 Quint models + adversarial teeth tests) in CI. No third-party pen test/audit yet.	Available Planned	Arch §13
IAM-01	Identity & Access	Is SSO (OIDC/SAML) supported?	OIDC + SAML verifiers built and tested (OIDC per-commit vs Keycloak; SAML sidecar, single-use replay defense). Live IdP interop planned.	Built	Arch §6
IAM-02	Identity & Access	Automated provisioning (SCIM)?	Inbound SCIM provisioning/de-provisioning built; outbound sync planned.	Built	Arch §6
IAM-03	Identity & Access	RBAC with least privilege?	Role assignments + ABAC evaluator; execution has no ambient authority (`INV-11`). Admin console planned.	Built	Arch §5–6
IAM-04	Identity & Access	Is MFA enforced?	Not implemented today; org-level enforcement roadmap.	No	Arch §6

#	Domain	Control question	Response	Status	Evidence
IAM-05	Identity & Access	Are access decisions fail-closed?	Yes — uncertainty/absence denies (`INV-20`), machine-checked.	Available	Arch §5
DSP-01	Data Security	How is data classified and stored?	Records / append-only events / content (by handle) / projections; local SQLite + git-backed content store.	Available	Arch §4
DSP-02	Data Security	Does data leave the customer environment?	Yes, to the LLM provider — prompts + in-scope context sent for inference in plaintext today. Otherwise local; federation opt-in.	Available (disclosed)	Arch §2,§4
DSP-03	Data Security	Is data isolated between tenants/projects?	By authority/scope (`INV-1`); handles convey no access (`INV-10`). Hosted multi-tenant ops planned.	Model Hosted Planned	Arch §2,§5
DSP-04	Data Security	Retention & deletion capability?	Revocation (future-only, `INV-18`) + content erasure (tombstone, modeled + reducer). Bulk/admin UI planned.	Available	Arch §4
DSP-05	Data Security	DPA and subprocessor list?	Planned. With BYO-credentials, the LLM provider is the customer's own subprocessor.	Planned	Arch §12
CEK-01	Crypto & Keys	Is data encrypted at rest?	AES-256-GCM (AEAD via `ring`); envelope encryption with KMS-wrapped key, verified live vs Azure Key Vault for server deployments.	Built	Arch §8
CEK-02	Crypto & Keys	Is data encrypted in transit?	Cert-pinned TLS; relay routes opaque bytes; cross-party messages signed (P-256 ECDSA) and verified.	Available	Arch §8
CEK-03	Crypto & Keys	How are keys managed?	Envelope DEK/KEK; KEK in Azure Key Vault via a `KeyWrap` seam. Live KMS needs a service principal.	Built	Arch §8
CEK-04	Crypto & Keys	Confidential computing /	SEV-SNP quote verifier built + tested vs real Milan vectors.	Built Planned	Arch §3,§8

#	Domain	Control question	Response	Status	Evidence
		attestation?	Live confidential-VM hosting + confidential inference planned.		
LOG-01	Logging	Audit log of security-relevant actions?	Per-actor append-only `{actor, action, target}` (references only), position-ordered, filterable.	Available	Arch §9
LOG-02	Logging	Can logs export to our SIEM?	Yes — `HttpAuditSink` POSTs JSON to a customer collector (Splunk/Datadog/webhook) over rustls.	Available	Arch §9
LOG-03	Logging	Are logs tamper-evident?	Append-only semantically (immutable event log); cryptographic tamper-evidence not yet shipped.	Planned	Arch §9
LOG-04	Logging	Production monitoring/alerting?	Not implemented today.	No	Arch §9
SEF-01	Incident Mgmt	Incident-response plan / breach notification?	Not implemented today; to be established before a hosted offering.	No	Arch §9
BCR-01	Business Continuity	SLA / DR / backup posture?	Single-machine desktop today (customer controls backups). Hosted SLA + status page planned.	Planned	Arch §3,§9
CCC-01	Change Control	How are changes controlled and verified?	Trunk-based with a green-bar CI gate on every change (fmt, clippy-deny, full tests, model checks, coverage gate). Method changes edit-authored + audited (`INV-24`).	Available	Arch §11
TVM-01	Threat & Vuln	Dependency CVE scanning?	Not implemented (`Cargo.lock` pinned; no `cargo audit`/Dependabot in CI yet).	No	Arch §11
TVM-02	Threat & Vuln	SAST / secret scanning?	`cargo clippy -D warnings` per-PR; dedicated SAST + secret scanning not implemented.	Partial	Arch §11
TVM-03	Threat & Vuln	Documented threat model?	Yes — STRIDE + OWASP LLM Top 10 (2025) + MITRE ATLAS, with mitigations and status.	Available	Arch §7

#	Domain	Control question	Response	Status	Evidence
STA-01	Supply Chain	Is there an SBOM?	Not implemented (CycloneDX/SPDX not yet produced).	No	Arch §11
STA-02	Supply Chain	Build provenance attested (SLSA)?	Reproducible build + image measurement digest pipeline built; formal SLSA attestation not implemented.	Built No	Arch §11
STA-03	Supply Chain	Are released binaries signed/notarized?	Not implemented — desktop builds are currently unsigned.	No	Arch §11
AIS-01	App Security	How is the LLM agent prevented from over-reach?	No ambient authority (`INV-11`); kernel OS-sandbox bounds tool/file/network; method read-only (`INV-24`); per-project network isolation is opt-in (egress open by default, no per-host allowlist yet).	Available (Linux/macOS)	Arch §7
AI-01	AI Governance	Is AI risk governed (NIST AI RMF)?	Mapped to Govern/Map/Measure/Manage. No model bias/eval program today.	Built Partial	Arch §10
AI-02	AI Governance	Is the model-provider data flow documented?	Yes — prompts + in-scope context reach the configured LLM provider in plaintext today; provider named in the trust boundary. Confidential inference planned.	Available (disclosed)	Arch §2,§4,§10
IPY-01	Interoperability	Can a customer export/leave with their data?	Event-sourced, locally stored, content addressable. Formal export/portability tooling planned.	Partial / Planned	Arch §4

Security contact: jack@gaugewright.com · Reviewed against spec rev 2026-06. This sheet states current truth honestly, including gaps; a "Planned" answer with intent is preferred to a gap papered over.